ФЕДЕРАЛЬНОЕ АГЕНТСТВО

ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

ГОСТ Р МЭК 62443-2-1— 2015

СЕТИ КОММУНИКАЦИОННЫЕ ПРОМЫШЛЕННЫЕ

Защищенность (кибербезопасность) сети и системы

Часть 2-1

Составление программы обеспечения защищенности (кибербезопасности) системы управления и промышленной автоматики

IEC 62443-2-1:2010
Industrial communication networks — Network and system security — Part 2-1: Establishing an industrial automation and control system security program (IDT)

Издание официальное

Москва
Стандартинформ
2015

gost.e-ecolog.ru

Предисловие

1 ПОДГОТОВЛЕН Негосударственным образовательным частным учреждением «Новая инженерная школа» (НОЧУ «НИШ») на основе аутентичного перевода на русский язык указанного в пункте 4 международного стандарта, который выполнен Российской комиссией экспертов МЭК/ТК 65, и Федеральным государственным унитарным предприятием «Всероссийский научно-исследовательский институт стандартизации и сертификации в машиностроении» (ВНИИНМАШ)

2 ВНЕСЕН Техническим комитетом по стандартизации ТК 306 «Измерения и управление в промышленных процессах»

3 УТВЕРЖДЕН И ВВЕДЕН В ДЕЙСТВИЕ Приказом Федерального агентства по техническому регулированию и метрологии от 22 июня 2015 г. № 774-ст

4 Настоящий стандарт идентичен международному стандарту МЭК 62443-2-1:2010 «Промышленные коммуникационные сети. Защищенность (кабербезопасность) сети и системы. Часть 2-1. Составление программы обеспечения защищенности (кибербезопасности) системы управления и промышленной автоматики» (IEC 62443-2-1:2010, «Industrial communication networks — Network and system security — Part 2-1: Establishing an industrial automation and control system security program»).

Алфавитный указатель терминов, используемых в настоящем стандарте, приведен в дополнительном приложении ДА.

При применении настоящего стандарта рекомендуется использовать вместо ссылочных международных стандартов соответствующие им национальные стандарты Российской Федерации, сведения о которых приведены в дополнительном приложении ДБ

5 ВВЕДЕН ВПЕРВЫЕ

6 В настоящем стандарте часть его содержания может быть объектом патентных прав

*Правила применения настоящего стандарта установлены в ГОСТ Р 1.0—2012 (раздел 8). Информация об изменениях к настоящему стандарту публикуется в ежегодном (по состоянию на 1 января текущего года) информационном указателе «Национальные стандарты», а официальный текст изменений и поправок — в ежемесячном информационном указателе «Национальные стандарты». В случае пересмотра (замены) или отмены настоящего стандарта соответствующее уведомление будет опубликовано в ближайшем выпуске ежемесячного информационного указателя «Национальные стандарты». Соответствующая информация, уведомление и тексты размещаются также в информационной системе общего пользования — на официальном сайте Федерального агентства по техническому регулированию и метрологии в сети Интернет (*gost.e-ecolog.ru

© Стандартинформ, 2015

Настоящий стандарт не может быть полностью или частично воспроизведен, тиражирован и распространен в качестве официального издания без разрешения Федерального агентства по техническому регулированию и метрологии

Содержание

1 Область применения 1
2 Нормативные ссылки 2
3 Термины, определения и сокращения 2
3.1 Термины и определения 2
3.2 Сокращения 6
3.3 Структура 7
4 Элементы системы управления кибербезопасностью 7
4.1 Обзор 7
4.2 Категория «Анализ рисков» 9
4.3 Категория «Устранение риска при помощи системы управления кибербезопасностью» 11
4.4 Категория «Контроль и совершенствование системы управления кибербезопасностью» 27
Приложение А (справочное) Руководство по разработке элементов системы управления кибербезопасностью 29
Приложение В (справочное) Процесс разработки системы управления кибербезопасностью 112
Приложение С (справочное) Сопоставление требований настоящего стандарта с ИСО/МЭК 27001 120
Приложение ДА (справочное) Алфавитный перечень терминов 129
Приложение ДБ (справочное) Сведения о соответствии ссылочных международных стандартов национальным стандартам Российской Федерации 131
Библиография 132

0 Введение

0.1 Обзор

Кибербезопасность приобретает все большее значение для современных компаний. Многие организации, работающие в сфере информационных технологий, много лет занимаются вопросами кибербезопасности и за это время внедрили зарекомендовавшие себя системы управления кибербезопасностью (CSMS), которые приведены в стандартах Международной организации по стандартизации (ISO) и Международной электротехнической комиссии (МЭК) (см. ИСО/МЭК 17799 [23] и ИСО/МЭК 27001 [24]). Такие системы управления обеспечивают хорошо отлаженный метод защиты объектов организации от кибератак.

Организации, применяющие IACS (системы промышленной автоматики и контроля), начали применять готовые коммерческие технологии (COTS), разработанные для бизнес-систем, используемых в их повседневных процессах, в результате чего возрос риск кибератак, направленных на оборудование IACS. Как правило, такие системы в среде IACS по многим причинам не настолько робастны, как системы, специально спроектированные как IACS для подавления кибератак. Подобные недостатки могут привести к последствиям, которые отразятся на уровне охраны труда, промышленной безопасности и охраны окружающей среды (HSE).

Организации могут попытаться использовать существовавшие ранее решения в сфере информационных технологий и кибербезопасности бизнеса для обеспечения безопасности IACS, при этом не осознавая последствий своих действий. И хотя многие такие решения можно применять в отношении IACS, реализовывать их необходимо правильным способом, чтобы избежать неблагоприятных последствий.

0.2 Система управления кибербезопасностью для IACS

Система управления описывает компоненты, которые должны быть включены в систему управления, но при этом не определяет, каким образом она должна разрабатываться. В настоящем стандарте рассмотрены аспекты компонентов, включенных в CSMS для IACS, и приводятся указания по разработке CSMS для IACS.

Для решения сложной задачи в качестве общего проектного подхода проблема разбивается на мелкие компоненты, каждый из которых рассматривается в определенном порядке. Такой основательный подход позволяет изучить риски, связанные с кибербезопасностью для IACS. Однако частой ошибкой при этом является то, что работа одновременно осуществляется с одной системой. Обеспечение информационной безопасности представляет собой гораздо более сложную задачу, которая требует решений для всего набора IACS, включая политики, процедуры, практики и персонал, в работе которого применяются такие IACS. Возможно, для внедрения масштабной системы управления потребуется изменение культуры внутри организации.

Постановка вопроса кибербезопасности на уровне всей организации может выглядеть устрашающе. К сожалению, решить подобную задачу простым способом не представляется возможным. Это объясняется разумной причиной: не имеется комплекса практик безопасности, подходящих для всего и всех. Может быть, и реально достичь абсолютной безопасности, но навряд ли рекомендуется, ведь это чревато потерей функциональности, которая требуется для достижения этого почти идеального состояния. Безопасность на деле является балансом между риском и затратами. Все ситуации будут отличаться друг от друга. В некоторых случаях риск может быть скорее связан с факторами HSE, нежели чем с чисто экономическим воздействием. Реализация риска скорее закончится непоправимыми последствиями, чем небольшим финансовыми трудностями. Поэтому готовый набор обязательных практик в области обеспечения безопасности будет либо слишком жестким и, скорее всего, дорогостоящим, либо недостаточным для того, чтобы решить проблему риска.

0.3 Связь между настоящим стандартом и ИСО/МЭК 17799 и ИСО/МЭК 27001

ИСО/МЭК 17799 [23] и ИСО/МЭК 27001 [24] — это очень хорошие стандарты, в которых описана система управления кибербезопасностью для бизнес-систем и систем информационных технологий. Многие положения этих стандартов также применяются и в отношении IACS. В настоящем стандарте сделан акцент на необходимость соответствия практик управления кибербезопасностью IACS и практик управления кибербезопасностью бизнес-систем и систем информационных технологий. Экономический эффект появится когда, будет достигнуто соответствие между этими программами. Пользовате-

лям настоящего стандарта предлагается ознакомиться с ИСО/МЭК 17799 и ИСО/МЭК 27001, в которых представлена дополнительная информация. Настоящий стандарт разработан на основе указаний, приведенных в указанных стандартах ИСО/МЭК. В нем рассматриваются некоторые существенные различия между IACS и общими бизнес-системами и системами информационных технологий, а также раскрывается важная концепция, суть которой заключается в том, что риски кибербезопасности для IACS могут негативным образом отразиться на охране труда, промышленной безопасности и охране окружающей среды и должны быть объединены с прочими существующими практиками по управлению такими рисками.

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

СЕТИ КОММУНИКАЦИОННЫЕ ПРОМЫШЛЕННЫЕ

Защищенность (кибербезопасность) сети и системы

Часть 2-1

Составление программы обеспечения защищенности (кибербезопасности) системы управления и промышленной автоматики

Industrial communication networks. Network and system security. Part 2-1.
Establishing an industrial automation and control system security programme

Дата введения — 2016—01—01

1 Область применения

Настоящий стандарт определяет элементы, необходимые для встраивания системы управления кибербезопасностью (CSMS) в системы управления и промышленной автоматики (IACS). В настоящем стандарте также приведено руководство по разработке таких элементов. В настоящем стандарте широко трактуются определения и сфера применения компонентов IACS, описанных в IEC/TS 62443-1-1.

Элементы CSMS, приведенные в настоящем стандарте, в целом включают в себя политику, процедуру, практику и соответствующий персонал и служат описанием того, что включается или должно быть включено в окончательный вариант CSMS для организации.

Примечание 1 — В других стандартах серии МЭК 62443, а также в документах, приведенных в элементе «Библиография» настоящего стандарта, более подробно описаны специфические технологии и/или решения для систем кибербезопасности.

Руководство по разработке CSMS (см. приложение А) приведено в настоящем стандарте в качестве примера. В указанном руководстве отражена точка зрения разработчика относительно того, каким образом организация может разрабатывать элементы, но при этом руководство не является источником решений во всех возможных ситуациях. Пользователям настоящего стандарта следует ознакомиться с требованиями и применять указанное руководство при разработке CSMS, обладающих полной функциональностью. Политики и процедуры, описанные в настоящем стандарте, должны составляться разрабатываться с учетом особых требований каждой организации.

Примечание 2 — Могут возникнуть ситуации, когда в работе находится ранее существовавшая CSMS и добавляется часть IACS, либо могут быть организации, которые ранее никогда официально не создавали CSMS. В настоящем стандарте не могут быть предусмотрены все случаи, когда организации придется устанавливать CSMS для среды IACS, поэтому настоящий стандарт не является источником решений для всех возможных ситуаций.

Издание официальное

2 Нормативные ссылки

Документ, ссылка на который приведена ниже, обязателен при применении настоящего стандарта. Для датированных ссылок применяют только указанное издание. Для недатированных ссылок применяют последнее издание ссылочного документа (включая любые изменения).

IEC/TS 62443-1-1[1)] Промышленные коммуникационные сети. Защищенность сети и системы. Часть 1-1. Терминология, концептуальные положения и модели (IEC/TS 62443-1-12, Industrial communication networks — Network and system security — Part 1-1: Terminology, concepts and models)

3 Термины, определения и сокращения

3.1 Термины и определения

В настоящем стандарте применены термины и определения, указанные в IEC/TS 62443-1-1, а также следующие термины с соответствующими определениями:

3.1.1 **учетная запись доступа** (access account): Функция управления доступом, дающая пользователю право доступа к определенной совокупности данных или функций конкретного оборудования.

Примечание — Учетные данные доступа зачастую привязаны к идентификаторам (ID) и паролям пользователей. ID и пароли пользователей могут быть закреплены за пользователем или группой пользователей, к примеру, рабочим персоналом пульта управления, выполняющим сходный набор рабочих задач.

3.1.2 **административные порядки** (administrative practices): Сформулированные и документированные методики/процедуры, которым отдельно взятые сотрудники обязаны следовать во всех случаях.

Примечание — Данные порядки обычно рассматриваются в контексте наемного труда в организации. В среде систем промышленной автоматики и контроля (IACS) он косвенно связан с охраной труда, техникой безопасности и охраной окружающей среды (HSE).

3.1.3 **имущественный объект** (asset): Физический или логический объект, который принадлежит организации или относится к ней иным способом, представляя для нее ощущаемую или реальную ценность.

[IEC/TS 62443-1-1, пункт 3.2.6]

Примечание — В данном конкретном случае имущественным объектом является любой объект, подлежащий защите, связанный с системой управления кибербезопасностью (CSMS).

3.1.4 **аутентификация** (authentication): Мера безопасности, запроектированная на установление правомерности передачи самого сообщения или его источника, а также средство проверки авторизационных данных индивидуального пользователя для получения определенных категорий информации.

[IEC/TS 62443-1-1, пункт 3.2.13]

3.1.5 **система управления горелкой** (burner management system): Система для безопасного запуска, контроля работы и отключения систем розжига, относящихся к котлам, факельным установкам, инсинераторам, газовым турбинам, термическим окислителям и другому оборудованию с огневым подводом теплоты.

3.1.6 **план непрерывности бизнеса** (business continuity plan): Документ, устанавливающий процедуры восстановления после существенного сбоя и возобновления бизнес-процессов.

Примечание 1 — Этот термин собирательный и относится также к другим аспектам восстановления после чрезвычайных происшествий, к примеру, управлению в чрезвычайных обстоятельствах, человеческим ресурсам и взаимодействию со средствами массовой информации (СМИ) или прессой.

Примечание 2 — План непрерывности бизнеса устанавливает также процедуры для поддержания на устойчивом уровне важных бизнес-процессов в ходе восстановления после существенного сбоя.

3.1.7 **планирование непрерывности бизнеса** (business continuity planning): Деятельность по разработке плана непрерывности бизнеса.

[1)] Настоящий стандарт разработан на основе AN SI/ISA 99.02.01:2009 и в полном объеме заменяет его для использования в любой стране мира. При этом понимается, что второе издание IEC/TS 62443-1-1 является международным стандартом, а не технической спецификацией (TS), т. к. в него были включены некоторые нормативные требования, в отношении которых возможно достижение соответствия.

3.1.8 **управление изменениями** (change management): Деятельность по контролю и документированию любых изменений в системе для обеспечения надлежащего функционирования управляемого оборудования.

3.1.9 **совместимость между стандартами** (compliance): Соответствие стандарта требованиям, сформулированным в другом стандарте.

Заимствовано из [ИСО/МЭК 10746-2, пункт 15.1]

Примечание — Данный термин характеризует зависимость между двумя нормативами — А и В, которая действует тогда, когда норматив А предъявляет требования, которым полностью соответствует норматив В (В совместим с А).

3.1.10 **соответствие стандарту** (conformance): Зависимость между объектом внедрения стандарта и самим стандартом, при которой каждое положение, верное в стандарте, должно быть верно для объекта его внедрения.

Заимствовано из [ИСО/МЭК 10746-2, пункт 15.1]

Примечание — Данное соответствие действует, когда конкретные требования, указанные в нормативе (требования соответствия), соблюдены в объекте его внедрения. Оценка соответствия — это действия по выявлению этого соответствия.

3.1.11 **последствие** (consequence): Результат, вытекающий из определенного инцидента.

3.1.12 **важнейший** (critical): Крайне важные устройство, компьютерная система, процесс и т. п., нарушение безопасности которых в результате того или иного инцидента может серьезно отразиться на финансовом состоянии, а также здоровье, условиях труда сотрудников организации и экологической безопасности.

3.1.13 **система управления кибербезопасностью** (cyber security management system): Программа, разработанная организацией для поддержания кибербезопасности всех имущественных объектов данной организации на заданном уровне конфиденциальности, целостности и доступности, независимо от того, относятся ли данные объекты к бизнес-процессам или системам IACS организации.

3.1.14 **аппаратные требования** (device requirements): Характеристика контрмеры, которой должны соответствовать устройства в пределах определенной зоны для достижения требуемого уровня целевой безопасности.

3.1.15 **консультант безопасности** (gatekeeper): Доверенное лицо, с которым консультируется высшее руководство с целью назначения приоритетов проблемам, которые ему необходимо решить, над остальными проблемами, с которыми другие справятся лучше.

3.1.16 **охрана труда, техника безопасности и охрана окружающей среды** (здоровье, условия труда и экологическая безопасность) (health, safety and environment): Обеспечение охраны здоровья и безопасности сотрудников и местного населения, а также высокой экологичности рабочих процессов.

3.1.17 **человеко-машинный интерфейс** (human-machine interface; HMI): Совокупность средств, с помощью которых люди (пользователи) взаимодействуют с конкретной машиной, устройством, компьютерной программой или другим сложным инструментом (системой).

Примечание — Во многих случаях такие средства включают в себя видеоэкраны или компьютерные терминалы, кнопки, звуковую обратную связь, мигающие сигналы и др. Человеко-машинный интерфейс представляет собой:

- средство ввода информации, посредством которого пользователи управляют машиной;
- средство вывода информации, посредством которого машина доносит информацию до пользователей.

3.1.18 **инцидент** (incident): Событие, которое не является частью запланированной работы системы или сервиса и приводит или может привести к сбою или снижению качества сервиса, предоставляемого системой.

3.1.19 **независимый аудит** (independent audit): Проверка организации (ее политики, методик, действий, оборудования, персонала и т. п.) независимой группой, которая не связана с данной организацией.

Примечание — Такой аудит может требоваться для публичных компаний.

3.1.20 **информационная техника** (information technology): Объекты имущества организации, относящиеся к вычислительной технике, которая реализует нефизические объекты, к примеру, программные приложения, вычислительные программы и файлы данных о сотрудниках.

Примечание 1 — В настоящем стандарте термин «информационная техника», употребляемый в этом значении, приводится без сокращений.

Примечание 2 — Другой случай употребления термина «информационная техника» (IT) относится к внутренней организационной структуре компании (к примеру, отделу информационных технологий), или единицам оборудования, которые обычно обслуживает этот отдел (то есть управляющим компьютерам, серверам и сетевой инфраструктуре). В настоящем стандарте термин «информационная техника», употребляемый в этом значении, представлен в виде аббревиатуры IT.

3.1.21 **неподдерживаемая система** (legacy system): Система промышленной автоматики и контроля, расположенная на производственном объекте, которая может быть недоступна в качестве коммерчески доступного продукта (COTS).

Примечание — Неподдерживаемая система могла когда-то быть готовым коммерческим объектом, но в данный момент может быть недоступна и/или не обслуживаться.

3.1.22 **вероятность возникновения** (likelihood): Количественная оценка возможности того, что действие, событие или инцидент произойдут.

3.1.23 **локальный пользователь** (local user): Пользователь, находящийся в пределах периметра рассматриваемой зоны безопасности.

Примечание — Примером локального пользователя является лицо, находящееся непосредственно на производственном участке или в пульте управления.

3.1.24 **система управления производством** (manufacturing execution system): Система планирования и отслеживания процессов производства, используемая для анализа и сообщения о доступности и состоянии ресурсов, планирования и обновления распоряжений, сбора подробных данных о ходе производства, таких как расход материалов, использование трудовых ресурсов, параметры управления, состояние заказов и оборудования, и другой важнейшей информации.

Примечание 1 — Данная система запрашивает спецификации материалов, технологические маршруты и прочие данные из главной системы планирования ресурсов предприятия и обычно используется для отслеживания и создания отчетов в режиме реального времени о процессах в производственных помещениях, при этом полученные данные поступают обратно в главную систему планирования.

Примечание 2 — Для дополнительных сведений см. МЭК 62264-1.

3.1.25 **MAC-адрес** (MAC-address): Аппаратный адрес, который позволяет дифференцировать одно устройство сети от другого.

3.1.26 **оператор (operator):** Специальный пользователь, который обычно отвечает за корректную работу управляемого оборудования.

3.1.27 **управление патчами** (patch management): Важная составляющая управления системами, включающая в себя получение, испытание и установку множественных патчей (кодовых изменений) на администрируемую компьютерную систему.

Примечание — Задачи в рамках управления патчами включают в себя обеспечение актуальной информацией о доступных патчах, подбор подходящих патчей для конкретных систем, обеспечение корректной установки патчей, испытание систем после установки патчей с документированием всех выполненных действий, к примеру, специальной настройки конфигураций, которую необходимо выполнить удаленно через гетерогенные среды в соответствии с передовым практическим опытом.

3.1.28 **инженер по организации производства** (process engineer): Лицо, которое обычно отвечает за технические аспекты промышленного управления и использует IACS и прочие средства для мониторинга работы и управления промышленной автоматикой на объекте.

3.1.29 **система управления производственными данными** (process information management system): Группа систем, которые предоставляют вспомогательную информацию для упрощения работы с объектом.

3.1.30 **программируемый логический контроллер** (programmable logic controller; PLC): Программируемое микропроцессорное устройство, которое используется в промышленности для управления сборочными линиями и монтажными механизмами, расположенными в производственном помещении, и многими другими видами механического, электрического и электронного оборудования производственного объекта.

Примечание — PLC обычно программируется в соответствии с [14] и рассчитан на использование в режиме реального времени в жестких условиях производства. PLC связаны с датчиками и исполнительными механизмами и характеризуются количеством и типом предоставляемых портов ввода/вывода, а также частотой сканирования портов ввода/вывода.

3.1.31 **управление безопасностью процесса** (process safety management): Регулирование, направленное на предотвращение чрезвычайных происшествий в химических и биотехнологических системах путем решения вопросов, которые связаны с рациональным использованием и техническим проектированием.

3.1.32 **удаленный доступ** (remote access): Связь с объектами или системами, находящимися в пределах определенного периметра, или их использование, осуществляемые из любой точки, которая находится за пределами этого периметра.

3.1.33 **удаленный пользователь** (remote user): Пользователь, который находится за пределами периметра рассматриваемой зоны безопасности.

Пример — Примерами удаленных пользователей могут быть лица, находящиеся в офисе того же здания, лица, устанавливающие связь по корпоративной глобальной вычислительной сети (WAN), и лица, устанавливающие связь по открытым инфраструктурным сетям.

3.1.34 **оценка рисков** (risk assessment): Процесс выявления и измерения рисков, затрагивающих деятельность организации (включая ее миссию, функции, имидж или репутацию), ее имущественные объекты или отдельных представителей, путем определения вероятностей возникновения таких рисков, конечного ущерба, а также назначения дополнительных контрмер для смягчения этого ущерба.

Примечание — Термин синонимичен понятию «анализ риска» и включает в себя анализ угроз и уязвимостей.

3.1.35 **смягчение риска** (risk mitigation): Действия по уменьшению вероятности и/или выраженности события.

3.1.36 **границы допустимости риска** (risk tolerance): Риск, который организация готова принять.

3.1.37 **самостоятельная оценка** (self-assessment): Проверка организации (то есть ее политики, методик, действий, оборудования и персонала) группой, являющейся частью организации.

Примечание — Такая группа может иметь непосредственное отношение к бизнес-процессу организации, либо представлять другое ее подразделение, но быть подробнейшим образом информирована о рисках, связанных с данным бизнес-процессом.

3.1.38 **методика «шести сигм»** (Six Sigma®): Ориентированная на процесс методика, которая рассчитана на повышение эффективности бизнеса путем совершенствования конкретных аспектов стратегических бизнес-процессов.

3.1.39 **социальная инженерия** (social engineering): Практика заполучения конфиденциальной информации путем психологического воздействия на легальных пользователей.

3.1.40 **заинтересованное лицо** (stakeholder): Отдельный человек или группа, заинтересованные в достижении результатов, на которые нацелена организация, и сохранении жизнеспособности продуктов и услуг организации.

Примечание — Заинтересованные лица воздействуют на программы, продукты и услуги. В данном конкретном случае заинтересованным кругом лиц являются сотрудники организации, которые отвечают за обеспечение и мониторинг кибербезопасности. Данные сотрудники включают в себя руководителя программы кибербезопасности, а также команду специалистов разного профиля из всех отделов, которых касается программа кибербезопасности.

3.1.41 **системный администратор** (system administrator): Лицо (лица), отвечающие за управление безопасностью компьютерной системы.

Примечание — Такое управление может включать в себя обслуживание операционной системы, управление сетью, администрирование учетных данных и управление патчами, с учетом текущих изменений.

3.1.42 **требования к системе** (system requirements): Характеристики требуемого уровня целевой безопасности

3.1.43 **отслеживаемый удаленный доступ** (ushered access)/**отслеживание удаленного доступа** (shadowing): Процесс отслеживания действий удаленного пользователя в сети.

3.1.44 **оценка уязвимости** (vulnerability assessment): Формальное описание и анализ уязвимости системы.

3.2 Сокращения

В данном подразделе приведены обозначения и сокращения, используемые в настоящем стандарте:

ANSI — Американский национальный институт стандартов (American National Standards Institute);

CFR — Свод федеральных нормативных актов (США) (U.S. Code of Federal Regulations);

ChemITC — Центр по информационным технологиям в области химии Американского химического совета (Chemical Information Technology Center of the American Chemistry Council);

COTS — коммерчески доступные продукты (Commercial off the shelf);

CPU — центральное процессорное устройство (Central processing unit);

CSCSP — программа кибербезопасности химического сектора (Chemical Sector Cyber Security Program);

CSMS — система управления кибербезопасностью (Cyber security management system);

CSVA — оценка уязвимости кибербезопасности (Cyber security vulnerability assessment);

DCS — распределенная система управления (Distributed control system);

DMZ — демилитаризованная зона (Demilitarized zone);

DoS, DDoS — отказ в обслуживании, распределенная атака типа «отказ в обслуживании» (Denial of service, Distributed denial of service);

FDN — сеть полевых устройств (Field device network);

FTP — протокол передачи файлов (File transfer protocol);

HMI — человеко-машинный интерфейс (Human machine interface);

HSE — относящийся к охране труда, технике безопасности и охране окружающей среды (здоровью, условиям труда и экологической безопасности) (Health, safety and environmental);

HVAC — отопление, вентиляция и кондиционирование воздуха (Heating, ventilation, and air-conditioning);

IACS — система(ы) промышленной автоматики и контроля [Industrial automation and control system(s)];

ID — идентификатор (Identification);

IEC — Международная электротехническая комиссия (МЭК) (International Electrotechnical Commission);

IEEE — Институт инженеров по электротехнике и электронике (The Institute of Electrical and Electronics Engineers);

IP — интернет-протокол (Internet protocol);

ISA — Международное общество автоматизации (International Society of Automation);

ISO — Международная организация по стандартизации (ИСО) (International Organization for Standardization);

IT — информационная техника (Information technology);

KPI — ключевой показатель(ли) эффективности [Key performance indicator(s)];

LAN — локальная вычислительная сеть (Local area network);

MAC — управление доступом к среде (Media access control);

MES — система управления производством Manufacturing execution system;

NERC — Североамериканский совет по надежности электроснабжения (действует в США и Канаде) [North American Electric Reliability Council (applies to U.S. and Canada)];

NIST — Национальный институт стандартов и технологий (США) (U.S. National Institute of Standards and Technology);

OS — операционная система (Operating system);

PC — персональный компьютер (Personal computer);

PCN — сеть управления процессами (Process control network);

PCSRF — форум NIST по определению требований к безопасности управления процессами (NIST Process Control Security Requirements Forum);

PIM — управление информацией о процессах (Process information management);

PIN — персональный идентификационный номер (Personal identification number);

PLC — программируемый логический контроллер (Programmable logic controller);

PSM — управление безопасностью процессов (Process safety management);

RAID — избыточный массив независимых дисков (Redundant array of independent disks);

RCN — сеть регулирующего контроля (Regulatory control network);

SANS — Институт системного администрирования, аудита, сетевых технологий и безопасности (SysAdmin, Audit, Networking, and Security Institute);

SCADA — диспетчерский контроль и сбор данных (Supervisory control and data acquisition);

SI — Международная система единиц (International System of Units);

SIS — автоматизированная система(ы) безопасности [Safety instrumented system(s)];

SoA — положение о применимости (Statement of applicability);

SOC — стандартный режим эксплуатации (Standard operating condition);

SOP — типовая инструкция (Standard operating procedure);

SP — специальная публикация [Special Publication (by NIST)];

SSL — уровень защищенных сокетов (Secure socket layer);

TCP — протокол управления передачей (Transmission control protocol);

TR — технический отчет (Technical report);

VLAN — виртуальная локальная вычислительная сеть (Virtual local area network);

VPN — виртуальная частная сеть (Virtual private network);

WAN — глобальная вычислительная сеть (Wide area network).

3.3 Структура

Элементами CSMS являются:
- назначение элемента;
- базовое описание элемента;
- обоснование того, почему включается данный элемент;
- требования к такому элементу.

Для описания каждого элемента и соответствующих требований используется табличное представление. Требования пронумерованы в соответствии с подпунктами (но сами при этом не являются подпунктами) таким образом, чтобы на требования можно было ссылаться по отдельности и избирательно.

4 Элементы системы управления кибербезопасностью

4.1 Обзор

В настоящем подразделе описаны элементы, составляющие CSMS для IACS. Эти элементы являются тем, что включается и должно быть включено в CSMS в целях обеспечения защиты IACS от кибератак.

Элементы представлены в трех основных категориях:
- анализ рисков;
- устранение риска при помощи CSMS;
- контроль и усовершенствование CSMS.

Каждая из указанных категорий подразделяется на группы элементов и/или элементы. На рисунке 1 показана связь между категориями, группами элементов и элементами.

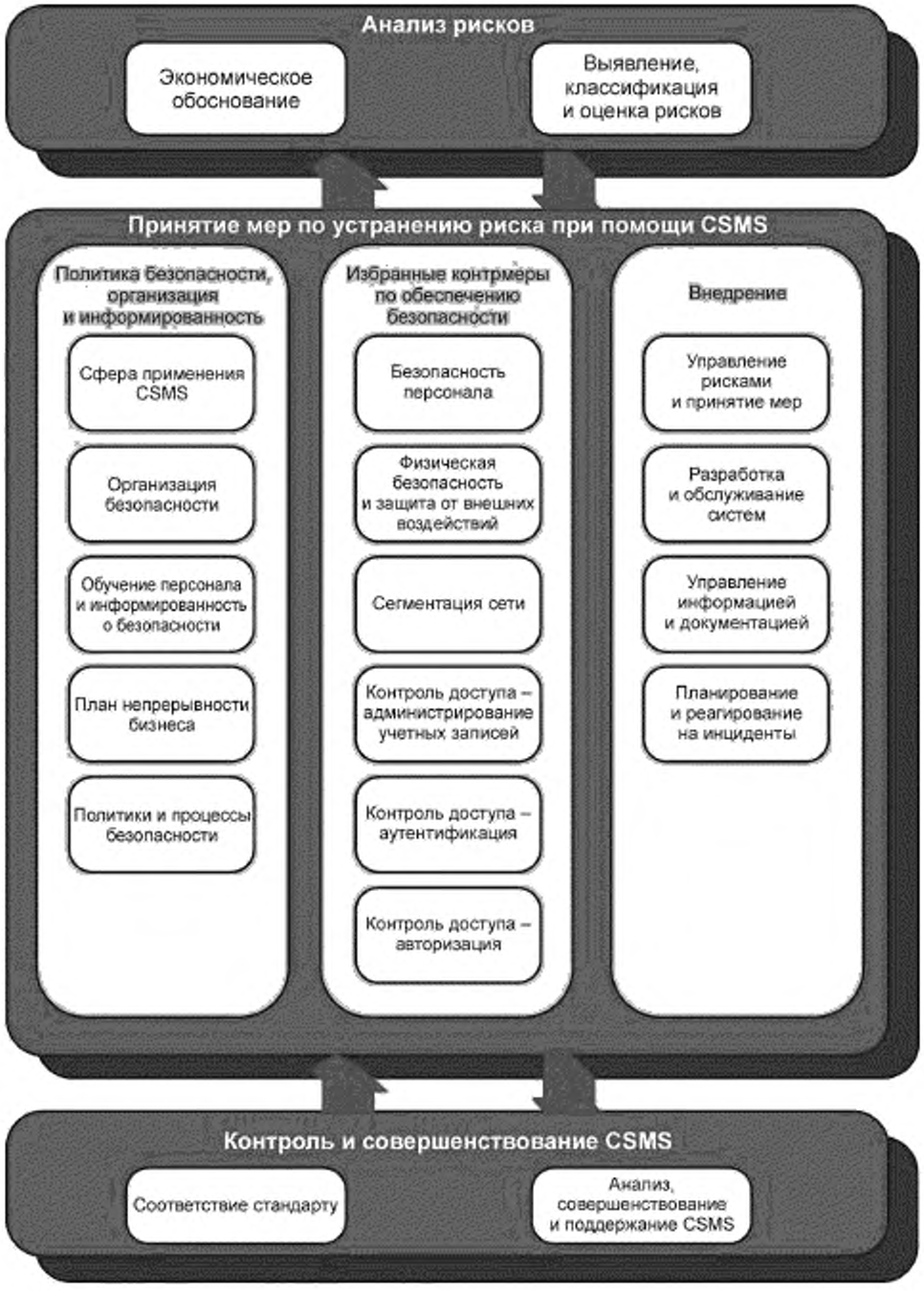


Рисунок 1 — Графическое изображение элементов системы управления кибербезопасностью

В каждом элементе в настоящем разделе показаны цель элемента, базовое описание элемента, обоснование включения данного элемента и соответствующие требования к элементу.

В приложении А приведена та же самая структура вместе с категориями, группами элементов и элементами. Но в нем описано, каким образом необходимо разрабатывать элементы CSMS. Пользователям необходимо ознакомиться с приложением А, чтобы понять особые требования и вопросы, возникающие при разработке CSMS для IACS. Руководство, приведенное в приложении А, должно составляться в зависимости от особых требований каждой организации.

В настоящем стандарте определены элементы, требуемые для CSMS. Настоящий стандарт не предназначен для того, чтобы описывать конкретный последовательный процесс определения и устранения риска, включающего такие элементы. Поэтому организации следует создавать такой процесс в соответствии со своей культурой, устройством и действующим состоянием работ по обеспечению кибербезопасности. В целях облегчения работы организации по применению настоящего стандарта в А.3.4.2 (приложение А) приведен пример процесса по выявлению и устранению риска. Кроме того, в приложении В приведены рекомендации по эффективному управлению работой в отношении всех элементов, описанных в настоящем стандарте.

Несмотря на то, что CSMS является превосходным инструментом для управления рисками в крупной компании, она также может применяться и в отношении небольших организаций. В больших компаниях CSMS может быть организована на более формальном уровне и поэтому может применяться в различных ситуациях и странах. Когда речь идет о небольшой организации, необходимо принимать аналогичные меры CSMS, но уже с меньшей долей формальности. В разделе 4 и приложении А описаны действия, предприняв которые пользователи смогут лучше понять элементы и работу в рамках CSMS.

4.2 Категория «Анализ рисков»

4.2.1 Описание категории

Первой главной категорией CSMS является «Анализ рисков». В категории описан большой объем исходной информации, из которой составляются многие другие элементы CSMS. На рисунке 2 показаны два элемента, являющиеся частью категории:

- экономическое обоснование;
- выявление, классификация и оценка рисков.

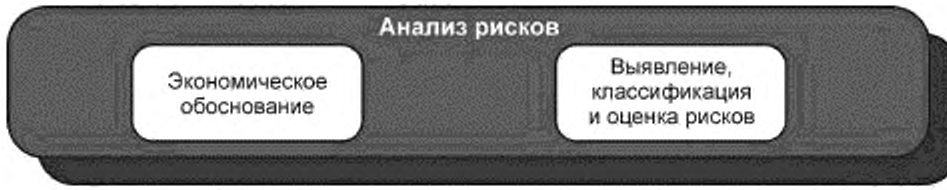


Рисунок 2 — Графическое представление категории «Анализ рисков»

4.2.2 Элемент «Экономическое обоснование»

Цель:

Идентифицировать и документально описать уникальные потребности организации для устранения рисков кибератак в отношении IACS.

Описание:

Экономическое обоснование зависит от характера и масштаба последствий в финансовой сфере и в сфере охраны труда, промышленной безопасности и охраны окружающей среды, а также прочих потенциальных последствий, возникающих в результате инцидентов в отношении IACS.

Обоснование:

Разработка экономического обоснования играет важную роль для того, чтобы организация смогла убедить руководство выделить необходимое финансирование для реализации программы по обеспечению кибербезопасности IACS.

Требования:

Таблица 1 — Экономическое обоснование: Требования

Описание работ	Требование
4.2.2.1 Разработка экономического обоснования	Организация должна разработать укрупненное экономическое обоснование в качестве основы для своей работы по управлению кибербезопасностью IACS, в котором бы рассматривался такой аспект, как уникальная зависимость организации от IACS

4.2.3 Элемент «Выявление, классификация и оценка рисков»

Цель:

Определить комплекс кибер-рисков IACS, которые угрожают организации, и оценить вероятность и уровень серьезности таких рисков.

Описание:

Организации отстаивают свою способность выполнять миссию путем систематического определения, выставления приоритетов и анализа потенциальных угроз, уязвимостей и последствий, применяя проверенные методы. Первая группа требований включает в себя действия, предпринимаемые организацией для составления как укрупненного, так и детального анализа рисков, в том числе оценку уязвимости, в стандартном хронологическом порядке. К таким требованиям, связанным с подготовкой укрупненного и детального анализа рисков, относятся требования 4.2.3.1, 4.2.3.2 и 4.2.3.8. Требования 4.2.3.10—4.2.3.14 представляют собой общие требования, применяемые к процессу оценки рисков в целом. Процесс принятия мер, основанных на такой оценке, представлен в 4.3.4.2.

Обоснование:

Поскольку целью инвестирования в обеспечение кибербезопасности является снижение уровня риска, она обуславливается пониманием уровня риска и возможностей его снижения.

Требования:

Таблица 2 — Выявление, классификация и оценка рисков: Требования

Описание работ	Требование
4.2.3.1 Выбор метода оценки рисков	Организация должна выбирать определенный подход и метод анализа рисков, которые определяют и расставляют в порядке приоритета риски, связанные с угрозами безопасности, уязвимостями и последствиями для материальных объектов IACS
4.2.3.2 Предоставление исходной информации для выполнения оценки рисков	Организация должна предоставить лицам, участвующим в оценке рисков, соответствующую информацию, включая обучение методике, до начала оценки рисков
4.2.3.3 Выполнение укрупненного анализа рисков	Укрупненный анализ рисков должен проводиться для понимания последствий для финансовой сферы и сферы HSE в случае появления угрозы для доступности, целостности или конфиденциальности IACS
4.2.3.4 Определение IACS	Организация должна определить различные IACS, собрать данные об устройствах, с тем, чтобы можно было описать характер риска и встроить устройства по группам в логические системы
4.2.3.5 Разработка простых сетевых схем	Организация должна разработать простые сетевые схемы для каждой логически интегрированной системы с указанием главных устройств, типов сетей и расположения оборудования
4.2.3.6 Расстановка приоритетов систем	Организация должна разработать критерии и назначить класс приоритета для снижения риска каждой логической группы управления
4.2.3.7 Выполнение детального анализа уязвимостей	Организация должна выполнить детальный анализ уязвимостей своих отдельных логических IACS, область охвата которого зависит от результатов укрупненного анализа рисков и приоритета предмета IACS в отношении таких рисков

Окончание таблицы 2

Описание работ	Требование
4.2.3.8 Выбор метода проведения детального анализа рисков	Методика оценки рисков, выбранная организацией, должна включать в себя методы определения приоритетов детальных уязвимостей, выявленных в ходе детального анализа
4.2.3.9 Выполнение детального анализа рисков	Организация должна провести детальный анализ рисков, включая уязвимости, выявленные в ходе детального анализа
4.2.3.10 Определение периодичности повторных анализов и критериев для начала их проведения	Организация должна определить периодичность проведения повторного анализа рисков и уязвимостей, а также критерии начала анализа, в зависимости от изменений технологии, организации или промышленной эксплуатации
4.2.3.11 Интегрирование результатов оценки физических рисков, рисков HSE и рисков, связанных с кибербезопасностью	Результаты оценки физических рисков, рисков HSE и рисков, связанных с кибербезопасностью, должны быть объединены для понимания общего риска для материальных объектов
4.2.3.12 Выполнение оценки рисков на протяжении жизненного цикла IACS	Оценка рисков должна проводиться на всех этапах жизненного цикла технологии, включая разработку, внедрение, изменения и снятие с эксплуатации
4.2.3.13 Документальное оформление выполненного анализа рисков	Методика оценки рисков и результаты оценки рисков должны быть оформлены документально
4.2.3.14 Ведение записей по анализу уязвимостей	Для всех объектов, составляющих IACS, необходимо вести актуальные записи по анализу уязвимостей

4.3 Категория «Устранение риска при помощи системы управления кибербезопасностью»

4.3.1 Описание категории

Вторая главная категория CSMS называется «Устранение риска при помощи CSMS». В этой категории содержится большой объем требований и информации из CSMS. Категория подразделяется на три группы элементов:

- политика, организация и понимание необходимости безопасности;
- избранные контрмеры по обеспечению безопасности;
- принятие мер.

4.3.2 Группа элементов «Политика, организация и понимание необходимости безопасности»

4.3.2.1 Описание группы элементов

В первой группе элементов описывается разработка базовых политик по обеспечению кибербезопасности, организации, ответственные за обеспечение информационной безопасности и понимание таких вопросов внутри самой организации. Графическое представление пяти элементов, включенных в группу элементов, показано на рисунке 3:

- сфера применения CSMS;
- организация безопасности;
- обучение персонала и понимание необходимости в обеспечении безопасности;
- план бизнес-непрерывности;
- политики и процессы безопасности.



Рисунок 3 — Графическое представление группы элементов «Политика безопасности, организация и информированность»

4.3.2.2 Элемент «Сфера применения CSMS»

Цель:

Определить, проанализировать и документально оформить системы, процессы и организации, на которые распространяется действие CSMS.

Описание:

Сфера применения включает в себя все аспекты IACS, точки интегрирования с бизнес-партнерами, заказчиками и поставщиками.

Обоснование:

Руководство должно понимать границы, в пределах которых CSMS применяется к организации, и определять направленность действия CSMS. Разработка предельно понятной области применения облегчит руководству работу по достижению целей в отношении CSMS.

Требования:

Таблица 3 — Сфера применения CSMS: Требования

Описание работ	Требование
4.3.2.2.1 Определение сферы применения CSMS	Организация должна разрабатывать формальный письменный документ с описанием сферы применения для программы обеспечения кибербезопасности
4.3.2.2.2 Определение составляющих сферы применения	Сфера применения должна объяснять стратегические цели, процесс и сроки для CSMS

4.3.2.3 Элемент «Организация безопасности»

Цель:

Организовать структурные единицы, ответственные за управление, проведение и оценку общей кибербезопасности объектов IACS, принадлежащих организации.

Описание:

Высшие руководители создают организацию, структуру или сеть людей, ответственных за контроль и направленность действий по управлению рисками кибербезопасности, связанными с IACS. Кроме того, они обеспечивают наличие персонала, необходимого для реализации и оценки программ кибербезопасности организации на протяжении жизненного цикла CSMS. Организация любого уровня может применять настоящий стандарт, включая компанию или иное предприятие, подразделение, завод или группу.

Обоснование:

Ответственность за реализацию программы безопасности начинается с верхнего уровня организации. Поскольку кибербезопасность IACS затрагивает несколько различных наборов профессиональ-

ных навыков, обладателей которых зачастую невозможно обнаружить в одном конкретном отделе или подразделении организации, необходимо, чтобы члены высшего руководства сформулировали подход к управлению безопасностью с четким пониманием ответственности, благодаря чему обеспечивается грамотное использование профессиональных навыков и трудовых ресурсов. Данный процесс может принимать различные формы в отдельной организации и в группе людей, работающих вместе над различными проблемами организации безопасности. Данный конкретный подход значительным образом зависит от существующей культуры организации.

Требования.

Таблица 4 — Организация безопасности: Требования

Описание работ	Требование
4.3.2.3.1 Получение поддержку высшего руководства	Организация должна получить поддержку высшего руководства для реализации программы кибербезопасности
4.3.2.3.2 Создание организации(й) по обеспечению безопасности	Необходимо создать или выбрать организацию, структуру или сеть заинтересованных лиц под контролем руководства, которые будут отвечать за обеспечение конкретной направленности и контроля за аспектами информационной безопасности IACS
4.3.2.3.3 Определение видов ответственности внутри организации	Необходимо четко определить виды ответственности внутри организации для выполнения работы по обеспечению информационной безопасности и принятию соответствующих мер по обеспечению физической безопасности
4.3.2.3.4 Определение состава группы заинтересованных лиц	Ключевая группа заинтересованных лиц по своему характеру должна быть многофункциональной и сочетать в себе профессиональные навыки ее участников, необходимые для обеспечения безопасности во всех аспектов IACS

4.3.2.4 Элемент «Обучение персонала и повышение информированности о необходимости безопасности»

Цель:

Предоставить всему персоналу (включая сотрудников, работников по контракту и сторонние организации) информацию, необходимую для определения, изучения, поиска решений и, в зависимости от обстоятельств, устранения уязвимостей и угроз для IACS, а также информацию о том, что в их собственной работе применяются эффективные контрмеры.

Описание:

Весь персонал должен пройти соответствующее техническое обучение по вопросам известных угроз и уязвимостей аппаратного/программного обеспечения и социальной инженерии.

Обоснование:

При работе с IACS вопросу кибербезопасности необходимо уделять такое же внимание, как и безопасности и эксплуатационной целостности, поскольку последствия могут быть настолько же тяжелыми. Осознание необходимости в обеспечении безопасности всеми членами персонала является важным инструментом для снижения рисков информационной безопасности. Информированные и бдительные сотрудники являются одной из наиболее важных линий защиты в обеспечении безопасности системы. Поэтому весь персонал должен осознавать важность обеспечения надежной работы системы.

Требования:

Таблица 5 — Обучение персонала и информированность: Требования

Описание работ	Требование
4.3.2.4.1 Разработка программы обучения	Организация должна разрабатывать и внедрять программу обучения по работе с системой информационной безопасности
4.3.2.4.2 Обеспечение обучения работе с процессом и оборудованием	Весь персонал (включая сотрудников, работников по контракту и сторонние организации) должен проходить первоначальное и периодическое обучение по вопросам работы с правильными процессами безопасности и правильному использованию объектов обработки информации

Окончание таблицы 5

Описание работ	Требование
4.3.2.4.3 Проведение обучения персонала технической поддержки	Весь персонал, отвечающий за управление рисками, разработку IACS, системное администрирование/обслуживание и прочие задачи, влияющие на CSMS, должен пройти обучение по вопросам целей в области безопасности и промышленным операциям, связанным с такими задачами
4.3.2.4.4 Проведение аттестации программы обучения	Аттестация программы обучения должна проходить на постоянной основе с тем, чтобы гарантировать, что персонал понимает программу безопасности и проходит надлежащее обучение
4.3.2.4.5 Периодический пересмотр программы обучения	По мере необходимости программа обучения пересматривается на предмет появления новых или изменяющихся угроз и уязвимостей
4.3.2.4.6 Регистрация результатов программы обучения	Необходимо регулярные ведение и проверка регистрируемых результатов обучения и сроков изменения программы

4.3.2.5 Элемент «План непрерывности бизнеса»

Цель:

Определить процедуры ведения и повторного установления важных бизнес-процедур в процессе восстановления после существенного сбоя.

Описание:

В плане бизнес-непрерывности должны рассматриваться цели восстановления различных систем и подсистем, используемых в работе, с учетом стандартных бизнес-потребностей, перечень потенциальных помех и процедуры восстановления для каждого типа, а также график проверки нескольких или всех процедур восстановления. Одной из основных целей восстановления должно быть сохранение максимальной доступности системы управления.

Обоснование:

Ни один комплекс защиты не может предотвратить все нарушения, возникающие в результате инцидентов, создающих угрозу для кибербезопасности. Детальный план бизнес-непрерывности гарантирует восстановление и использование информации IACS в максимально возможные быстрые сроки после наступления существенного сбоя.

Требования.

Таблица 6 — План непрерывности бизнеса: требования

Описание работ	Требование
4.3.2.5.1 Определение цели восстановления	Прежде чем приступить к разработке плана бизнес-непрерывности, организация должна определить цели в области восстановления для используемых систем, с учетом бизнес-потребностей
4.3.2.5.2 Определение влияния и последствия для каждой системы	Организация должна определить степень влияния существенного сбоя на каждую систему, а также последствия, связанные с потерей одной или более систем
4.3.2.5.3 Разработка и внедрение планов бизнес-непрерывности	Планы непрерывности должны разрабатываться и внедряться с тем, чтобы гарантировать возможность восстановления бизнес-процессов в соответствии с целями восстановления
4.3.2.5.4 Формирование группы по разработке бизнес-непрерывности	Должна быть создана группа по разработке бизнес-непрерывности, включая владельцев IACS и прочих лиц. В случае существенного сбоя эта группа должна определить приоритеты наиболее важных бизнес-систем и систем IACS для повторного установления операций
4.3.2.5.5 Определение и передача специфических должностных функций и обязанностей	План бизнес-непрерывности должен определять и передавать специфические должностные функции и ответственность для каждой части плана
4.3.2.5.6 Создание резервных процедур, обеспечивающих работу плана бизнес-непрерывности	Организация должна создавать процедуры резервирования и восстановления (см. 4.3.4.3.9) для поддержки плана бизнес-непрерывности

Окончание таблицы 6

Описание работ	Требование
4.3.2.5.7 Проверка и обновление плана бизнес-непрерывности	План бизнес-непрерывности должен проверяться на постоянной основе и обновляться по мере необходимости

4.3.2.6 Элемент «Политики и процедуры безопасности»

Цель:

Рассмотреть способы, которыми организация может пользоваться для определения безопасности, управлять своей программой безопасности, определять свое отношение к допустимости риска и пересматривать свои программы для введения дополнительных усовершенствований.

Описание:

Политики в области кибербезопасности для среды IACS должны разрабатываться на основе действующих политик высокого уровня, описанных рисков и уровней допустимости риска в соответствии с решением руководства. Процедуры кибербезопасности разрабатывают, исходя из политик в области информационной безопасности, и определяют способы реализации таких политик.

Обоснование:

Такие письменные политики и процедуры дают четкое представление для сотрудников, подрядчиков, сторонних организаций и аналогичных лиц о взгляде компании на вопрос информационной безопасности и ролях и обязанностях таких организаций и сотрудников в рамках обеспечения безопасности объектов компании.

Требования:

Таблица 7 — Политики и процедуры в области безопасности: требования

Описание работ	Требование
4.3.2.6.1 Разработка политики безопасности	Организация должна разработать политики обеспечения информационной безопасности высокого уровня для среды IACS, одобренные руководством
4.3.2.6.2 Разработка процедуры безопасности	Организация должна разработать и одобрить процедуры кибербезопасности, в основе которых лежат процедуры кибербезопасности, и предоставить указания по выполнению требований, изложенных в таких политиках
4.3.2.6.3 Сохранение соответствия систем управления рисками	Политики и процедуры кибербезопасности, направленные на защиту от рисков для IACS, должны соответствовать или являться продолжением политик, созданных в рамках других систем управления рисками
4.3.2.6.4 Определение требований к политике и процедурам информационной безопасности	Политики и процедуры кибербезопасности для среды IACS включают в себя требования о соответствии.
4.3.2.6.5 Определение уровня допустимости риска для организации	Организация должна определить и документально оформить свое понимание допустимости рисков в качестве основы для разработки политики и проведения работы по управлению рисками
4.3.2.6.6 Доведение политики и процедуры в области информационной безопасности до сведения персонала	Политики и процедуры кибербезопасности для среды IACS должны доводиться до сведения всего соответствующего персонала
4.3.2.6.7 Изучение и актуализация политики и процедуры в области информационной безопасности	Политики и процедуры кибербезопасности должны пересматриваться на постоянной основе, должна проводиться их аттестация, подтверждающая, что они являются актуальными, выполняются и поддерживаются в актуальном состоянии в соответствии с требованиями, что гарантирует их соответствие требованиям
4.3.2.6.8 Демонстрация поддержки руководства в реализации информационной безопасности	Высшее руководство должно продемонстрировать собственную ответственность за обеспечение информационной безопасности, утверждая политики в области информационной безопасности

4.3.3 Группа элементов «Избранные контрмеры по обеспечению безопасности»

4.3.3.1 Описание группы элементов

Вторая группа элементов в этой категории называется «Избранные контрмеры по обеспечению безопасности». Здесь описываются основные типы средств по управлению безопасностью, являющиеся частью хорошо продуманной CSMS. Документ не преследует своей целью описать весь процесс реализации каких-либо таких избранных контрмер. В нем рассмотрено много вопросов в отношении политики, процедур и практики применительно к таким конкретным контрмерам. На рисунке 4 показаны шесть элементов, составляющих группу элементов:

- безопасность персонала;
- физическая безопасность и защита от внешних воздействий;
- сегментация сети;
- контроль доступа — администрирование учетных записей;
- контроль доступа — аутентификация;
- контроль доступа — авторизация.

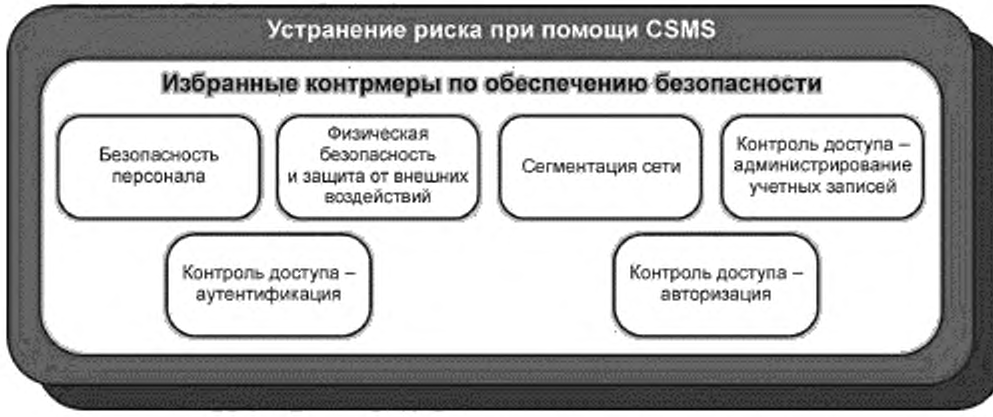


Рисунок 4 — Графическое представление группы элементов «Избранные контрмеры по обеспечению безопасности»

Такие конкретные меры были выбраны, поскольку из-за их масштабного влияния на политику и архитектуру очень важно учесть их до того, как начнется работа по созданию CSMS. Настоящий стандарт не преследует своей целью составление полного и достаточного списка контрмер, т. к. его полнота определяется в процессе анализа и управления рисками, описанном в настоящем стандарте.

4.3.3.2 Элемент «Безопасность персонала»

Цель:

Установить политики и процедуры, позволяющие определять, будет ли персонал поддерживать безопасность IACS на протяжении всего периода работы в организации.

Описание:

Безопасность персонала подразумевает изучение нового и действующего персонала с точки зрения их действий по обеспечению безопасности IACS для организации в будущем. В случае нового персонала элемент позволяет оценить его до прихода в организацию и убедиться в том, что его действия будут соответствовать будущим обязанностям в рамках обеспечения безопасности. Для действующего персонала элемент позволяет оценить, насколько такие сотрудники продолжают действовать в соответствии с их текущими обязанностями в рамках обеспечения безопасности.

Обоснование:

Во многих организациях требования к безопасности персонала исходят из соображений инсайдерских угроз и возможных инцидентов, вызванных невнимательным отношением к деталям или по вине персонала, не подходящего для выполнения такой работы, поскольку у таких сотрудников не имеется соответствующего образования или они используют вещества, затуманивающие сознание. Внедрение политик в области безопасности персонала может помочь снизить риск появления подобных проблем.

Требования:

Таблица 8 — Безопасность персонала: требования

Описание работ	Требование
4.3.3.2.1 Установление политики в области безопасности персонала	Должна быть установлена политика в области безопасности персонала, четко определяющая намерение организации обеспечивать безопасность в целом и обязанности персонала в этом отношении. (Персонал включает в себя сотрудников, работников по контракту и сторонние организации.)
4.3.3.2.2 Проведение первоначального отбор персонала	Кроме случаев, когда налагаются запреты государственных органов, весь персонал, имеющий доступ к IACS (физический и кибердоступ), включая новый принятый персонал и перемещения внутри организации на связанные с секретностью позиции, должен проходить отбор, включая подтверждение личности и проверки по другим имеющимся данным, в ходе подачи заявлений о приеме на работу
4.3.3.2.3 Регулярное выполнение проверки персонала	Персонал также должен проходить постоянные проверки на предмет изменений, которые могут указывать на конфликт интересов или сложности, связанные с надлежащим выполнением должностных обязанностей
4.3.3.2.4 Учет обязанностей в сфере обеспечения безопасности	Политика безопасности персонала должна затрагивать обязанности в сфере безопасности, начиная с приема на работу и заканчивая прекращением трудовых отношений, что особенно важно для позиций, связанных с секретностью
4.3.3.2.5 Документальное оформление и доведение до сведения сотрудников ожидания и обязанности	Ожидания и обязанности в отношении безопасности должны быть четко изложены в соответствующих документах и на регулярной основе доводиться до сведения персонала
4.3.3.2.6 Составление четкого перечня условий найма	В условиях найма должны быть четко изложены ответственность персонала за информационную безопасность. Действие таких обязательств продлевается на разумный период времени после прекращения трудовых отношений
4.3.3.2.7 Распределение обязанностей в целях обеспечения возможности проведения соответствующих проверок и сохранения баланса	Обязанности должны быть разделены между сотрудниками, что позволит проводить соответствующие проверки и сохранять баланс, исключая такие ситуации, когда в руках одного сотрудника сосредоточен весь контроль над действиями, изменяющими функциональную эксплуатацию IACS

4.3.3.3 Элемент «Физическая безопасность и защита от внешних воздействий»

Цель:

Создать безопасную среду для защиты объектов IACS. Объектом называется физический или логический объект, который принадлежит организации или охраняется ею, представляя для нее ощущаемую или реальную ценность (см. IEC/TS 62443-1-1, 3.2.6). Активами IACS являются объекты, входящие в состав IACS, в физическом и киберисполнении, или объекты, которые могут влиять на эксплуатацию IACS. Физическая безопасность гарантирует, что все объекты, особенно такие, которые связаны с IACS организации, защищены физически от неавторизованного доступа, утраты, повреждения, неверного применения и т. п. Защита от внешних воздействий гарантирует, что объекты организации защищены от условий среды, способных привести такие объекты в состояние непригодности или повреждению информации, содержащейся в них.

Описание:

Меры по обеспечению физической безопасности и защиты от внешних воздействий должны быть разработаны таким образом, чтобы они дополняли меры по обеспечению информационной безопасности, принятые для защиты объектов, являющихся частью IACS, и были согласованы с физической безопасностью остальных объектов завода. При разработке программы физической безопасности объектов в сферу применения важно включать все системы, а не просто ограничиваться традиционными объектами, располагающимися в компьютерных залах. Необходимо применять практический инженерный подход для уравнивания рисков в ходе разработки процедур обеспечения физической безопасности.

Физическая сегментация является ключевой контрмерой, предназначенной для разделения устройств на зоны безопасности, в отношении которых применяются определенные практики безопасности, позволяющие достигнуть нужного уровня безопасности.

Обоснование:

Физические объекты являются средством для достижения цели, а также самой целью. В современных системах управления физическими объектами обеспечивается работа киберсистемы. Таким образом, объект ценен сам по себе, но также имеет ценность, будучи неотъемлемой частью системы управления. Поскольку и объект, и система управления нужны друг для друга, оба компонента должны быть защищены, чтобы обеспечить сохранность системы. Важнейшим условием безопасности является принятие соответствующих контрмер, соизмеримых с уровнем риска. Несмотря на то, что физическая сегментация представляет собой важную контрмеру для обеспечения безопасности, применяемую в сочетании с другими способами защиты для снижения риска, который может быть связан с IACS, может не потребоваться, чтобы риски в отношении безопасности не выходили за принятые рамки.

Требования:

Таблица 9 — Физическая безопасность и защита информации от внешних воздействий: требования

Описание работ	Требование
4.3.3.3.1 Установление дополнительных политик в области физической защиты и информационной безопасности	Должны быть установлены политики и процедуры безопасности, направленные на обеспечение и физической безопасности, и защиты от внешних воздействий в рамках защиты объектов
4.3.3.3.2 Установление периметра(ов) физической безопасности	Для обеспечения барьеров для неавторизованного доступа и защиты объектов должен быть установлен один или несколько периметров физической безопасности
4.3.3.3.3 Обеспечение средствами контроля входа	На каждом барьере или границе необходимо предусмотреть соответствующие средства контроля входа
4.3.3.3.4 Защита объектов от внешних воздействий	Объекты должны быть защищены против повреждения условиями среды в результате таких угроз, как пожар, вода, дым, пыль, радиация, коррозия и удар
4.3.3.3.5 Требование от сотрудников выполнения процедур безопасности	От сотрудников требуется выполнение и принудительное исполнение установленных процедур в рамках обеспечения физической безопасности
4.3.3.3.6 Защита соединения	Все линии связи под контролем организации должны быть надлежащим образом защищены от несанкционированного вмешательства или повреждения
4.3.3.3.7 Поддержка оборудования в надлежащем состоянии	Все оборудование, включая вспомогательное оборудование для защиты от внешних воздействий, должно поддерживаться в надлежащем состоянии в целях обеспечения правильной работы
4.3.3.3.8 Установление процедуры контроля и оповещения	Должны быть установлены процедуры контроля и оповещения в случаях появления угрозы для физической безопасности или защиты от внешних воздействий
4.3.3.3.9 Установление процедур добавления, удаления и ликвидации объектов	Должны быть установлены и проверены процедуры в отношении добавления, удаления или ликвидации всех объектов
4.3.3.3.10 Установление процедур промежуточной защиты важнейших объектов	Должны быть установлены процедуры, обеспечивающие защиту важнейших компонентов во время нарушения операций, например, из-за пожара, попадания воды, нарушения защиты, вмешательства, стихийного бедствия или любой другой аварийной ситуации

4.3.3.4 Элемент «Сегментация сети»

Цель:

Объединить в группы и разделить отдельные ключевые устройства IACS по зонам с обычными уровнями безопасности для управления рисками безопасности и достигнуть требуемого уровня безопасности для каждой зоны.

Описание:

Сегментация сети является ключевой контрмерой, предназначенной для разделения устройств на зоны безопасности, в которых для достижения требуемого уровня безопасности реализуются определенные практики обеспечения безопасности. Зона может представлять из себя изолированный независимый сегмент сети или сегмент сети, отделенный от сети организации при помощи барьерного устройства. IACS должны разрабатываться таким образом, который бы позволял фильтровать/предотвращать попадание несущественных пакетов данных в устройства IACS.

Для сетей TCP/IP наиболее распространенными барьерными устройствами являются брендмауэры, маршрутизаторы и коммутаторы 3 уровня. Для сетей, не относящихся к типу TCP/IP, барьерными устройствами могут быть отдельные шлюзы или встроенные в сеть интерфейсные модули устройства IACS.

Обоснование:

Важнейшим условием обеспечения безопасности является применение контрмер, соизмеримых с уровнем риска. Несмотря на то, что сетевая сегментация представляет собой важную контрмеру для обеспечения безопасности, применяемую в сочетании с другими способами защиты для снижения риска, который может быть связан с IACS, может и не потребоваться, чтобы риски в отношении безопасности были небольшими.

Требования.

Таблица 10 — Сегментация сети: требования

Описание работ	Требование
4.3.3.4.1 Разработка архитектуры сегментации сети	Для устройств IACS должна быть разработана стратегия применения контрмер, с использованием зон безопасности, с учетом уровня рисков для IACS
4.3.3.4.2 Применение изоляции или сегментации для IACS с высоким уровнем риска	IACS, подверженные высокому уровню риска, должны быть изолированы или иметь в составе барьерное устройство, отделяющее их от прочих зон с отличными уровнями безопасности или рисков
4.3.3.4.3 Блокировка несущественных передач данных при помощи барьерных устройств	Барьерные устройства блокируют все несущественные передачи информации внутри и снаружи зоны безопасности, в которой находится важнейшее оборудование управления

4.3.3.5 Элемент «Контроль доступа — Администрирование доступа»

Цель:

Гарантировать на постоянной основе, что только установленные субъекты имеют учетные записи, гарантирующие допуск, и что такие учетные записи предусматривают соответствующие привилегии доступа.

Описание:

Контроль доступа — это способ контроля того, кто и какие субъекты могут получать доступ к объектам и системам, а также какие виды доступа разрешаются. Контроль доступа характеризуется тремя ключевыми аспектами: администрирование учетных записей, аутентификация и авторизация. Сочетание всех трех аспектов позволяет разработать надежную стратегию контроля доступа.

Администрирование учетных записей — это способ, связанный с предоставлением и отменой полномочий по доступу, а также обслуживанием разрешений и привилегий, предоставленных таким учетным записям для доступа к конкретным ресурсам и функциям на физических объектах, в сетях или системах. Учетные записи должны зависеть от функции или роли[1)] и могут определяться для отдельных лиц, групп лиц, действующих в качестве команды, или для устройств, выполняющих какую-либо функцию.

Обоснование:

Неверное использование данных и систем может привести к серьезным последствиям, включая нанесение вреда человеческой жизни, окружающей среде, финансовым потерям и ущербу для корпоративной репутации. Такие риски возрастают, когда сотрудники, подрядчики или временный персонал получает нецелесообразный доступ к данным и системам.

[1)] Термин «ролевая модель управления доступом» см. МЭК 62443-1-1 (подпункт 3.2.92).

Требования:

Таблица 11 — Контроль доступа — Администрирование доступа: требования

Описание работ	Требование
4.3.3.5.1 Реализация политики обеспечения авторизации для учетных записей доступа	Привилегии доступа, предоставленные учетным записям, должны устанавливаться в соответствии с политикой организации в области авторизации (см. 4.3.3.7.1)
4.3.3.5.2 Идентификация отдельных лиц	Для всех средств контроля информационной безопасности выбор учетных записей доступа для отдельных лиц в отличие от учетных записей для команды определяется с учетом угроз, рисков и уязвимостей. В этом случае учитываются риски HSE отдельных средств контроля, снижение рисков с использованием современных средств обеспечения физической безопасности, требования к ответственности и административным/эксплуатационным потребностям
4.3.3.5.3 Авторизация доступа к учетной записей	Предоставление, изменение или прекращение доступа производится под контролем соответствующего руководителя
4.3.3.5.4 Регистрация учетных записи	Должна вестись регистрация всех учетных записей доступа, включая подробные данные о лице(ах) и устройствах, авторизованных для использования учетной записи, их разрешения и руководителя, предоставляющего разрешения
4.3.3.5.5 Приостановление или удаление учетных записей	Учетные записи доступа временно приостанавливаются или удаляются, когда в них больше нет необходимости (например, при изменении должности)
4.3.3.5.6 Проверка разрешений учетных записей	Все установленные учетные записи доступа должны постоянно проверяться, чтобы гарантировать, что лицо(а) и устройства имеют только минимально требуемые разрешения
4.3.3.5.7 Изменение паролей по умолчанию	Пароли по умолчанию для учетных записей доступа должны быть изменены до введения IACS в эксплуатацию
4.3.3.5.8 Проверка администрирования учетных записей	Должны выполняться периодические проверки на предмет соответствия требованиям политики в области администрирования учетных записей

4.3.3.6 Элемент «Контроль доступа — Аутентификация»

Цель:

Точно определить пользователей сети, хостов, приложений, сервисов и ресурсов для автоматизированных операций, чтобы предоставить им права и обязанности, связанные с учетными записями, созданными в рамках администрирования учетных записей.

Описание:

Контроль доступа — это способ контроля, кто и какие субъекты могут получать доступ к объектам и системам, а также какие виды доступа разрешаются. Контроль доступа характеризуется тремя ключевыми аспектами: администрирование учетных записей, аутентификация и авторизация. Сочетание всех трех аспектов позволяет разработать надежную стратегию контроля доступа.

Имеется несколько типов стратегии аутентификации, каждый из которых характеризуется различной степенью строгости. Способы строгой аутентификации — это способы, позволяющие довольно точно идентифицировать пользователя. Способы слабой аутентификации можно легко обойти, чтобы получить несанкционированный доступ к данным. Физическое расположение пользователя может существенным образом влиять на уровень риска, связанного с получением доступа к IACS.

Обоснование:

Требования к аутентификации отличаются большей строгостью применительно к пользователям, занимающимся администрированием/конфигурированием, и дистанционным пользователям, чем к прочим пользователям. Это объясняется тем, что пользователи, занимающиеся администрированием/конфигурированием, обладают более широким кругом привилегий и их действия потенциально оказывают большее влияние в сравнении с другими пользователями. Дистанционные пользователи, как правило, не проходят проверку современными средствами контроля физического доступа. Автомати-

ческое блокирование учетных записей из-за неверной регистрации или периодов неактивности повышает уровень строгости аутентификации, но при этом в среде IACS учитывается с большой степенью осторожности, т. к. неудачная попытка аутентификации действительного пользователя может привести к последствиям для HSE, если пользователь не сможет выполнять задачи в критической ситуации. В среде IACS делается большой упор на сочетание мер физической аутентификации и электронной аутентификации.

Требования:

Таблица 12 — Контроль доступа — Аутентификация: требования

Описание работ	Требование
4.3.3.6.1 Разработка стратегии аутентификации	Компании должны разработать стратегии или подход к аутентификации, позволяющий определять метод(ы) аутентификации для их последующего применения
4.3.3.6.2 Выполнение аутентификации всех пользователей до использования системы	Все пользователи должны проходить аутентификацию перед использованием запрашиваемого приложения, кроме случаев, когда предусмотрены компенсирующие комбинации технологий контроля входа и административных практик
4.3.3.6.3 Составление требований к способам строгой аутентификации для системного администрирования и конфигурирования приложений	Практики строгой аутентификации (например, с требованием ввести надежный пароль) должны применяться ко всем учетным записям для системных администраторов и для конфигурации приложений
4.3.3.6.4 Регистрация и проверка всех попыток доступа к важнейшим системам	В журналах регистрации должна вестись запись всех попыток доступа к важнейшим системам, такие журналы должны проверяться на предмет удачных и неудачных попыток доступа
4.3.3.6.5 Выполнение аутентификации всех удаленных пользователей на соответствующем уровне	Организация может реализовывать схему аутентификации с соответствующим уровнем строгости для точного определения дистанционного интерактивного пользователя
4.3.3.6.6 Разработка политики удаленного входа в систему и соединений	Организация должна разработать политику, регулирующую дистанционный вход в систему одним пользователем и/или через дистанционное соединение (например, межзадачные соединения) с системами управления, в которой бы определялись соответствующие отклики системы на неудачные попытки входа и истечение периодов неактивности
4.3.3.6.7 Блокировка учетной записи доступа после неудачных попыток удаленного входа	После определенного числа неудачных попыток входа дистанционным пользователем система должна деактивировать учетную запись на определенный срок
4.3.3.6.8 Требование повторной аутентификации по истечении периода неактивности удаленной системы	По истечении определенного срока неактивности дистанционный пользователь должен пройти повторную аутентификацию до получения повторного доступа к системе
4.3.3.6.9 Применение аутентификации для межзадачных соединений	В системах должны реализовываться соответствующие схемы аутентификации для межзадачных соединений между приложениями и устройствами

4.3.3.7 Элемент «Контроль доступа — Авторизация»

Цель:

Предоставить привилегии доступа к ресурсам после успешной аутентификации пользователя и идентификации его связанной учетной записи доступа. Предоставленные привилегии определяются конфигурацией учетной записи, заданной на этапе администрирования в бизнес-процессе.

Описание:

Контроль доступа — это способ контроля позволяющий определять, кто и какие субъекты могут получать доступ к объектам и системам, а также какие виды доступа разрешаются. Контроль доступа характеризуется тремя ключевыми аспектами: администрирование учетных записей, аутентификация

и авторизация. Сочетание всех трех аспектов позволяет разработать надежную стратегию контроля доступа.

При авторизации используются средства контроля, предназначенные для защиты информации и объектов от намеренного и случайного нарушения, изменения или раскрытия. Особый упор делается на меры, гарантирующие, что аутентифицированные агенты имеют доступ к требуемым информационным объектам. Как и в случае с аутентификацией, авторизация зависит от местоположения пользователя.

Обоснование:

При работе со средой IACS важно убедиться в том, что к необходимой информации и системам получают доступ соответствующие сотрудники, для которых не создаются препятствия для исполнения их должностных обязанностей из-за отсутствия авторизации. В приложении предусматривается авторизация для выполнения определенных должностных функций. При разработке стратегии авторизации необходимо учитывать последствия для системы безопасности.

Требования:

Таблица 13 — Контроль доступа — Авторизация: требования

Описание работ	Требование
4.3.3.7.1 Определение политики безопасности авторизации	В политике безопасности авторизации должны быть установлены правила, определяющие привилегии, подтвержденные для учетных записей доступа для персонала с различными должностными функциями, такая политика должна быть оформлена документально и применяться в отношении всего персонала после процедуры аутентификации
4.3.3.7.2 Установление соответствующих способов логической и физической защиты для получения доступа к устройствам IACS	Разрешение на получение доступа к устройствам IACS должно быть логическим (правилам, по которым предоставляется или отклоняется доступ для известных пользователей в зависимости от их должностных функций), физическим (замки, камеры и прочие средства контроля, ограничивающие доступ к активному пульту управления) или и тем, и другим
4.3.3.7.3 Осуществление контроля доступа к информации или системам через учетные записи доступа, определяемые должностными функциями	Учетные записи доступа должны определяться должностными функциями для управления доступом к соответствующей информации или системам для такой должностной функции пользователя. В ходе определения должностных функций необходимо учитывать последствия для сферы безопасности
4.3.3.7.4 Применение множественных способов авторизации для важнейших IACS	В средах, для которых требуется особый контроль, необходимо применять множественные способы авторизации для ограничения доступа к IACS

4.3.4 Группа элементов «Исполнение»

4.3.4.1 Описание группы элементов

Третьей группой элементов в этой категории является «Исполнение». Этот элемент внутри группы затрагивает вопросы, связанные с внедрением CSMS. На рисунке 5 показано графическое представление четырех элементов в группе элементов:

- управление рисками и принятие мер;
- разработка и обслуживание систем;
- управление информацией и документацией;
- планирование и реагирование на инциденты.



Рисунок 5 — Графическое представление группы элементов «Исполнение»

4.3.4.2 Элемент «Управление рисками и принятие мер»

Цель:

Уменьшить риск и поддерживать его на приемлемом уровне в IACS с учетом допустимости риска для организации.

Описание:

Управление рисками и принятие мер затрагивает такие вопросы, как выбор, разработка и принятие контрмер в соответствии с рисками. Такие контрмеры могут учитывать использование продуктов, которые обладают большими возможностями обеспечения безопасности, средства ручного и процедурного контроля безопасности и средства контроля с использованием технологий, позволяющих предотвращать или уменьшать риск возникновения инцидентов.

Обоснование:

Элемент «Управление рисками и принятие мер» используется для того, чтобы обратить результаты классификации/идентификации рисков и оценочный компонент настоящего стандарта в эффективные и определенные действия. Несмотря на то, что риск невозможно устранить полностью, им можно управлять таким способом, который позволяет соблюдать равновесие между стоимостью упразднения риска и потенциальной стоимостью инцидента.

Требования:

Таблица 14 — Управление рисками и принятие мер: требования

Описание работ	Требование
4.3.4.2.1 Осуществление непрерывного управления риском IACS	Организация принимает схему управления рисками, которая включает в себя отбор и внедрение устройств IACS и контрмеры по сведению риска до приемлемого уровня на протяжении жизненного цикла объекта
4.3.4.2.2 Применение обычного комплекса контрмер	В организации необходимо определить и применять общий комплекс контрмер (технических и административных), направленных на физические риски и риски для информационной безопасности при идентификации определенного риска

4.3.4.3 Элемент «Разработка и обслуживание систем»

Цель:

Обеспечить поддержание требуемого уровня допустимости риска для организации, т. к. ее объекты IACS формируются как через обслуживание существующих систем, так и через разработку и поставку новых систем.

Описание:

Этот элемент затрагивает вопрос проектирования информационной безопасности в системах, начиная с ранних этапов разработки. Также он включает в себя реализацию таких политик и процедур информационной безопасности, которые изменяются системой на протяжении ее жизненного цикла.

Обоснование:

Организации пришли к выводу, что обслуживание CSMS является более сложной задачей в сравнении с их созданием. По этой причине процедуры, которые целенаправленно ориентированы на обеспечение информационной безопасности в рамках естественного развития систем IACS, имеют особо большое значение.

Требования.

Таблица 15 — Разработка и обслуживание систем: требования

Описание работ	Требование
4.3.4.3.1 Определение и проверка функций и возможностей безопасности	Функции и возможности каждого нового компонента IACS должны определяться заранее, разрабатываться и достигаться в процессе поставки, и проверяться вместе с другими компонентами, с тем, чтобы вся система отвечала требованиям необходимого профиля безопасности
4.3.4.3.2 Разработка и внедрение системы управления изменениями	Должна быть разработана и внедрена система управления изменениями для среды IACS. Процесс управления изменениями следует за процедурой разделения должностных обязанностей, которая позволяет избежать конфликта интересов
4.3.4.3.3 Выполнение оценки всех рисков, приводящих к изменению IACS	Планируемые изменения в IACS должны изучаться с использованием четко определенных критериев на предмет их потенциального влияния на риски HSE и риски для информационной безопасности лицами, обладающими техническими знаниями о промышленной эксплуатации и системе IACS
4.3.4.3.4 Составление требований к политикам безопасности для разработки систем или введения изменений в процессы обслуживания	Требования к безопасности новой системы, устанавливаемой в среде IACS в существующей зоне, должны соответствовать политикам и процедурам безопасности, требуемым для такой зоны/среды. Аналогичным образом, обновления и изменения должны отвечать требованиям безопасности для такой зоны
4.3.4.3.5 Интегрирование процедуры управления изменениями в системе управления информационной безопасностью и безопасностью процессов (PSM)	Процедуры управления изменениями системы информационной безопасности должны быть интегрированы с существующими процедурами PSM
4.3.4.3.6 Проверка и продолжение реализации политики и процедуры	Операции и политики/процедуры управления изменениями должны пересматриваться и поддерживаться в актуальном состоянии для обеспечения того, чтобы изменения относительно безопасности не приводили бы к увеличению рисков для безопасности или бизнес-непрерывности
4.3.4.3.7 Установление и документальное оформление процедуры патч-менеджмента	Должна быть установлена, документально оформлена и выполнена процедура патч-менеджмента
4.3.4.3.8 Установление и документальное оформление процедуры управления антивирусной безопасностью/защитой от вредоносных программ	Должна быть установлена, документально оформлена и выполнена процедура управления антивирусной безопасностью/защитой от вредоносных программ
4.3.4.3.9 Установление процедуры резервирования и восстановления систем	Должна быть создана, использована и подтверждена соответствующими проверками процедура резервирования и восстановления систем и защиты резервных копий

4.3.4.4 Элемент «Управление информацией и документами»

Цель:

Классифицировать, управлять, обеспечить сохранность и предоставить авторизованному персоналу информацию, связанную с IACS и CSMS, в соответствующие сроки.

Описание:

Организации должны внедрять комплексные политики управления информацией и документацией для информационных объектов в рамках IACS и CSMS. Необходимо уделять большое внимание вопросу защиты такой информации и гарантии сохранения соответствующих версий. Системы классификации информации, позволяющие достигать нужных уровней защиты информационных объектов, являются ключевым условием для выполнения этой цели.

Обоснование:

Большая часть информации о IACS может храниться в электронном или бумажном виде за пределами IACS и быть не защищенными средствами контроля авторизации IACS. Несанкционированный доступ и использование этой информации представляют собой угрозу для безопасности IACS. Для такой информации необходимо предусмотреть надлежащий контроль и управление.

Требования.

Таблица 16 — Управление информацией и документами: требования

Описание работ	Требование
4.3.4.4.1 Разработка процессов управления на протяжении жизненного цикла для информации IACS	Для информации IACS должен быть разработан и поддерживаться процесс управления документацией в течение жизненного цикла
4.3.4.4.2 Определение уровней классификации информации	Должны быть определены уровни классификации информации (например, конфиденциальная информация, информация ограниченного доступа, для широкого пользования) для доступа и управления, включая обмен, копирование, передачу и распространение, соответствующие требуемому уровню защиты
4.3.4.4.3 Классификация всех информационных объектов CSMS	Все логические объекты в рамках CSMS (т. е. информация о проектировании системы, оценки уязвимости, сетевые схемы и программы для промышленной эксплуатации) должны быть классифицированы с указанием требуемого уровня защиты, сопоставимого с последствием несанкционированного раскрытия или изменения
4.3.4.4.4 Обеспечение надлежащего контроля записей	Должны разрабатываться политики и процедуры, детально описывающие процессы сохранения, физической защиты и защиты целостности, уничтожения и ликвидации всех объектов в зависимости от их классификации, включая письменные и электронные записи, оборудование и прочие средства, содержащие данные, с учетом юридических или правовых требований
4.3.4.4.5 Обеспечение возможности извлечения многолетних записей	Должны быть приняты соответствующие меры, обеспечивающие возможность извлечения многолетних записей (т. е. преобразование данных в новый формат или сохранение старого оборудования, которое может быть использовано для считывания данных)
4.3.4.4.6 Ведение классификации информации	Информация, для которой требуется особый контроль или обработка, должна периодически проверяться и подтверждаться на предмет того, что все еще есть необходимость в специальной обработке
4.3.4.4.7 Проверка процесса управления информацией и документацией	Должны выполняться периодические проверки на предмет соответствия информации и политики управления документацией

4.3.4.5 Элемент «Планирование и реагирование на инциденты»

Цель:

Определить, каким образом организация будет выявлять инциденты в системе кибербезопасности и реагировать на них.

Описание:

При разработке программы планирования и реагирования на инциденты необходимо включать в нее все системы, не ограничиваясь исключительно традиционным оборудованием компьютерного зала. Часть плана реагирования на инциденты должна быть посвящена процедурам реагирования ор-

ганизации на инциденты, включая способы оповещения и документирования, расследования, восстановления и последующий контроль выполнения мероприятий.

Обоснование:

Обнаружение инцидентов на ранней стадии и соответствующее реагирование на них может уменьшить последствия события. Планирование и реагирование на инцидент предоставляет организации возможность планирования инцидентов в системе безопасности и реагирования на них в соответствии с установленными компанией процедурами. Вне зависимости от степени защиты системы всегда существует вероятность нежелательного проникновения, которое может подвергнуть систему риску. В технологиях существуют уязвимые места, а число и сложность внешних угроз продолжает увеличиваться, создавая необходимость в разработке эффективных стратегий планирования и реагирования. Опыт фактических инцидентов был зафиксирован, поскольку он имеет решающее значение для оценки и совершенствования CSMS.

Требования:

Таблица 17 — Требования к планированию и реагированию на инциденты

Описание работ	Требование
4.3.4.5.1 Реализация плана реагирования на инциденты	Организация должна реализовать план реагирования на инциденты, в котором указан ответственный персонал и мероприятия, осуществляемые назначенными лицами
4.3.4.5.2 Передача плана реагирования на инциденты	План реагирования на инциденты должен передаваться всем соответствующим организациям
4.3.4.5.3 Создание процедуры уведомления о необычных действиях и событиях	Организация должна создавать процедуру уведомления о необычных действиях или событиях, которые фактически могут являться инцидентами в системе информационной безопасности
4.3.4.5.4 Проведение обучения персонала по процедуре уведомления об инцидентах в системе информационной безопасности	Персоналу должны быть разъяснены их обязанности по уведомлению об инцидентах в системе информационной безопасности и методы уведомления об этих инцидентах
4.3.4.5.5 Своевременное сообщение об инцидентах в системе информационной безопасности	Организация должна своевременно сообщать об инцидентах в системе информационной безопасности
4.3.4.5.6 Обнаружение и реагирование на инциденты	При обнаружении инцидента организация должна незамедлительно отреагировать на него в соответствии с принятыми процедурами
4.3.4.5.7 Обнаружение неудачных и удачных попыток нарушения информационной безопасности	В организации должны существовать процедуры обнаружения неудачных и удачных попыток нарушения информационной безопасности
4.3.4.5.8 Фиксация информации об инцидентах	Информация об обнаруженном инциденте должна быть зафиксирована с указанием инцидента, процедуры реагирования, выводов и любых действий, предпринятых для изменения CSMS после инцидента
4.3.4.5.9 Сообщение информации об инциденте	Зафиксированная информация об инциденте должна быть своевременно передана всем соответствующим организациям (т. е. руководству, подразделениям, занимающимся информационными технологиями, безопасностью технологического процесса, автоматизацией, безопасностью автоматического управления и производством)
4.3.4.5.10 Решение и исправление обнаруженных проблем	В организации должна существовать методика решения обнаруженных проблем и обеспечения их исправления
4.3.4.5.11 Проведение учения	Для проверки программы реагирования в рабочем порядке должны быть проведены учения

4.4 Категория «Контроль и совершенствование системы управления кибербезопасностью»

4.4.1 Описание категории

Третья основная категория CSMS называется «Контроль и совершенствование CSMS». Данная категория включает в себя обеспечение использования CSMS, а также контроль эффективности CSMS. На рисунке 6 графически показаны два элемента категории:

- соответствие стандарту;
- анализ, совершенствование и поддержание CSMS.

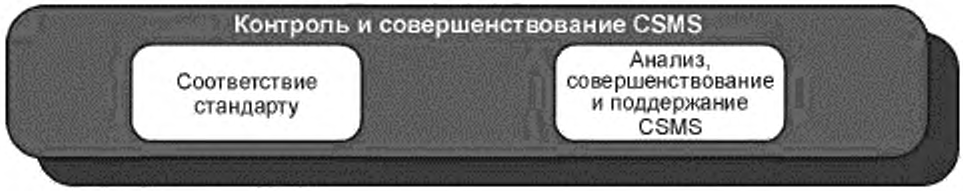


Рисунок 6 — Графическое изображение категории «Контроль и совершенствование CSMS»

4.4.2 Элемент «Выполнение норм и требований»

Цель:

Обеспечение соответствия CSMS, разработанной для организации.

Описание:

Соответствие CSMS означает, что организация придерживается официальной политики, своевременно выполняет процедуры и составляет отчеты для последующего анализа.

Обоснование:

Вне зависимости от качества CSMS при неиспользовании системы она не увеличивает эффективность организации и не способствует смягчению рисков.

Требования.

Таблица 18 — Требования к выполнению норм

Описание работ	Требование
4.4.2.1 Определение методики процесса аудита	В программе аудита должна быть указана методика проведения аудита
4.4.2.2 Проведение периодических аудитов IACS	Подтверждение соответствия IACS CSMS. CSMS должна включать периодические аудиты системы IACS для подтверждения того, что политика и процедуры безопасности выполняются в надлежащем порядке, и для выполнения целей по безопасности для конкретной зоны
4.4.2.3 Определение показателей соответствия	Организация должна определить показатели эффективности и критерии успешности, которые используются для контроля соответствия CSMS. Результаты всех периодических аудитов должны быть выражены, как степень выполнения этих показателей, для отражения эффективности и тенденций безопасности
4.4.2.4 Создание документального контрольного журнала	Должен быть указан перечень документации и отчетов, требуемых для создания контрольного журнала
4.4.2.5 Определение штрафных санкций за несоответствие	Организация должна определить, что означает несоответствие CSMS, и установить соответствующие штрафные санкции
4.4.2.6 Обеспечение компетентности аудиторов	Должна быть указана требуемая компетентность для аудита конкретных систем, входящих в область аудита. Также должен быть определен уровень независимости в рамках управления

4.4.3 Элемент «Анализ, совершенствование и поддержание системы управления кибербезопасностью»

Цель:

Обеспечение выполнения целей CSMS во времени.

Описание:

Анализ, совершенствование и поддержание CSMS обеспечивает непрерывный надзор над системой для контроля ее эффективного функционирования и управления изменениями, которые требуется вносить в систему, во времени.

Обоснование:

Анализ и мониторинг требуются для поддержания эффективности CSMS, поскольку система должна реагировать на изменения во внутренних и внешних угрозах, уязвимости и последствиях, а также на изменения в границах допустимости рисков, требованиях законодательства и развивающихся технических и нетехнических подходах к смягчению рисков.

Требования:

Таблица 19 — Требования к анализу, совершенствованию и поддержанию CSMS

Описание работ	Требование
4.4.3.1 Назначение организации для управления и внесения изменений в CSMS	Должна быть назначена организация для управления и координации совершенствования и внесения изменений в CSMS и использования установленного метода внесения и реализации изменений
4.4.3.2 Периодическое проведение оценки CSMS	Управляющая организация должна периодически оценивать всю систему CSMS для обеспечения достижения целей по безопасности
4.4.3.3 Определение триггерных факторов для оценки CSMS	Организация должна создать перечень триггерных факторов с установленными пороговыми значениями для последующего анализа соответствующих элементов CSMS и, возможно, внесения изменений. Эти триггерные факторы должны включать, как минимум, факты серьезных инцидентов в системе безопасности, изменения в законодательстве и нормативных документах, изменения в рисках и значительные изменения в IACS. Пороговые значения должны быть основаны на границах допустимости рисков для организации
4.4.3.4 Определение и проведение корректирующих и превентивных мероприятий	Организация должна определить и провести соответствующие корректирующие и превентивные мероприятия, чтобы модифицировать CSMS для выполнения целей по безопасности
4.4.3.5 Анализ границ допустимости рисков	Анализ границ допустимости рисков для организации проводится в случае значительных изменений в организации, технологии, целях деятельности, внутренней деятельности и внешних событиях, включая обнаруженные угрозы и изменения в социальной обстановке
4.4.3.6 Проведение мониторинга и оценки отраслевых стратегий, связанных с CSMS	Владельцы системы управления должны проводить мониторинг отрасли на предмет передовых практик, применяемых в CSMS для оценки и смягчения рисков, и оценивать их применимость
4.4.3.7 Проведение мониторинга и оценки действующего законодательства, относящегося к кибербезопасности	Организация должна ознакомиться с действующим законодательством и изменениями в законодательстве, относящимся к кибербезопасности
4.4.3.8 Запрос и сообщение о предложениях работников в сфере безопасности	Должен осуществляться активный поиск и доведение до высшего руководства предложений работников в сфере безопасности, касающихся недостатков и потенциала работы системы безопасности

Приложение А
(справочное)

Руководство по разработке элементов системы управления кибербезопасностью

А.1 Обзор

В настоящем приложении приведено справочное руководство для пользователей по разработке CSMS, удовлетворяющей требованиям, указанным в разделе 4 настоящего стандарта. Руководство, приведенное в настоящем приложении, описывает общую концепцию системы управления, что позволяет организациям, внедряющим CSMS, адаптировать ее к конкретным потребностям. Данное руководство необходимо считать отправной точкой или основой для разработки CSMS. Не все требования руководства могут быть применимыми, и в зависимости от применения организации может потребоваться более высокий уровень безопасности по сравнению с указанным. Как уже было указано в 4.1 настоящего стандарта, описанный процесс не является пошаговым.

Настоящее приложение разбито на категории, группы элементов и элементы, указанные в разделе 4 настоящего стандарта (см. рисунок А.1). Каждый элемент в настоящем приложении имеет следующую структуру:

- описание элемента: базовое описание темы;
- информация об элементе: в одном или нескольких подпунктах приведено подробное руководство по элементу. Их структура и содержание зависят от конкретных элементов;
- вспомогательные практические методы:
- основные методы: рекомендации для организаций по достижению базового уровня информационной безопасности. Эти методы являются строительными блоками требований по каждому элементу;
- дополнительные методы: инновационные методы обеспечения безопасности, используемые некоторыми организациями для дальнейшего повышения информационной безопасности;
- используемые ресурсы: источники дополнительной информации, а также опорные документы (в дополнение к настоящему стандарту).

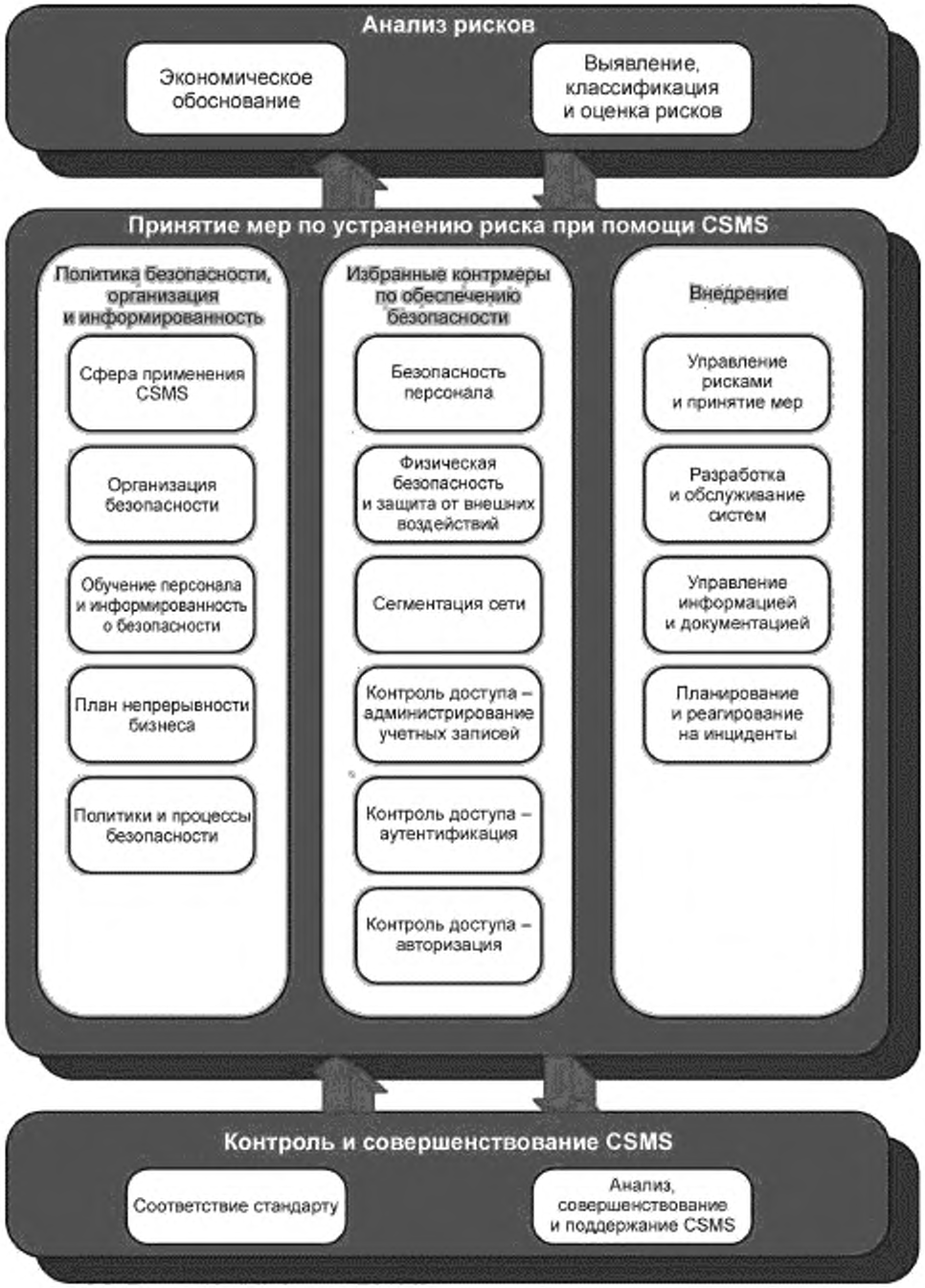


Рисунок А.1 — Графическое изображение элементов системы управления кибербезопасностью

А.2 Категория «Анализ рисков»

А.2.1 Описание категории

Первой основной категорией CSMS является анализ рисков. В этой категории рассматривается большая часть основной информации, которая входит во многие другие элементы CSMS. На рисунке А.2 показаны два элемента, являющиеся частью этой категории:

- экономическое обоснование;
- выявление, классификация и оценка рисков.

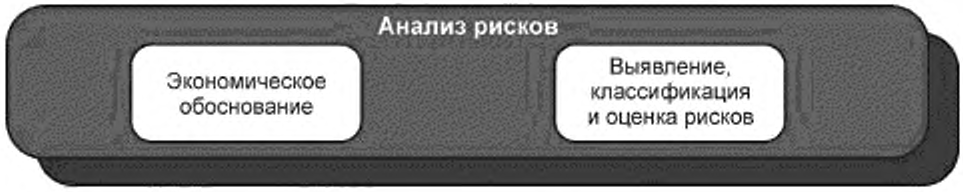


Рисунок А.2 — Графическое представление категории «Анализ рисков»

А.2.2 Элемент «Экономическое обоснование»

А.2.2.1 Описание элемента

Этот элемент устанавливает, что организация осведомлена и понимает важность информационной безопасности для информационной техники, используемой в IACS. Это понимание основано на понимании ролей, которые такая информационная техника играет в деятельности организации, рисках, связанных с этой деятельностью, и стоимости и других последствиях смягчения рисков для деятельности.

А.2.2.2 Риск информационной безопасности, экономическое обоснование и экономическая модель

Первым шагом реализации программы информационной безопасности для IACS является разработка убедительного экономического обоснования с учетом уникальных потребностей организации для смягчения риска информационной безопасности. Организация может взять экономическое обоснование для своей CSMS IACS и сопутствующих отдельных проектов из действующих политик, относящихся к безопасности, общему управлению рисками или выполнению требований нормативных документов. Другим организациям может потребоваться, чтобы экономическое обоснование имело форму официальной или неофициальной экономической модели для мероприятий по управлению кибербезопасностью, чтобы подтвердить, что стоимость смягчения риска информационной безопасности оправдывается финансовыми выгодами. Экономическое обоснование или экономическая модель для начальных действий по созданию CSMS будут зависеть от оценки рисков, обычно предварительной. После подтверждения рисков организация готова принимать соответствующие действия по их смягчению. Проведение более систематической и детальной оценки риска (как описано далее в настоящем стандарте) и отдельные решения в отношении контрмер сами по себе могут потребовать подготовки экономического обоснования, возможно, в форме экономической модели.

В экономическом обосновании отражаются бизнес-цели высшего руководства, которые основываются на опыте специалистов, имеющих дело с множеством аналогичных рисков. В настоящем подпункте рассмотрены ключевые компоненты окончательного экономического обоснования и ключевые ресурсы, помогающие определить эти компоненты. Экономическое обоснование может включать подтверждение предварительной или детальной оценки риска, других специальных аспектов всей CSMS, описанных в настоящем стандарте, или реализации контрмеры.

Опыт показывает, что реализация программы информационной безопасности без согласованного экономического обоснования часто приводит к потере ресурсов программы в пользу других потребностей бизнеса. Обычно такие другие потребности бизнеса имеют более очевидные бизнес-выгоды и простое обоснование.

А.2.2.3 Ключевые компоненты экономического обоснования

Существует четыре ключевых компонента экономического обоснования: приоритетные последствия для бизнеса, приоритетные угрозы, ожидаемое годовое влияние на бизнес и стоимость контрмер.

а) Приоритетные последствия для бизнеса

Перечень возможных последствий для бизнеса должен быть сужен до конкретных последствий для бизнеса, которые высшее руководство сочтет наиболее убедительными. Например, компания, производящая продукты питания и напитки, которая не использует токсичные или огнеопасные материалы и обычно перерабатывает свою продукцию при относительно низких температурах и давлении, может не беспокоиться о повреждении оборудования или влиянии на окружающую среду, но для нее более актуальным является потеря эксплуатационной готовности и снижение качества продукции. Понимание здесь основано на истории прошлых инцидентов, а также на знаниях о фактическом использовании IACS в деятельности и возможном влиянии на бизнес, которое могут оказать несанкционированные технические изменения. Также необходимо учитывать соблюдение нормативных документов;

b) Приоритетные угрозы

Перечень возможных угроз необходимо сузить по возможности до угроз, которые считаются убедительными. Например, компания, производящая еду и напитки, может не счесть терроризм убедительной угрозой, для нее будут более актуальными угрозы вирусов, «червей» и недовольства персонала. Понимание в данном случае базируется, в основном, на истории прошлых инцидентов;

c) Ожидаемое годовое влияние на бизнес

Наиболее важные пункты перечня приоритетных последствий для бизнеса должны быть тщательно изучены для получения оценки годового влияния на бизнес предпочтительно, но не обязательно, в финансовом плане. В примере с компанией, производящей продукты питания и напитки, компания пережила инцидент с вирусом в своей внутренней сети, который по оценке организации информационной безопасности привел к определенным финансовым затратам. Поскольку внутренняя сеть и сеть управления соединены между собой, можно предположить, что вирус, появившийся из сети управления, может оказать такое же влияние на бизнес.

Понимание здесь основывается, прежде всего, на историях прошлых инцидентов. Соблюдение установленных норм может повлечь за собой конкретные финансовые или деловые штрафы за несоблюдение;

d) Стоимость

Ожидаемая стоимость человеческой работы и технических контрмер должна быть подтверждена в экономическом обосновании.

Примечание — Для подготовки экономической модели требуется оценка влияния на бизнес в финансовом плане и сметы расходов на контрмеры, но успешное экономическое обоснование не всегда включает эту информацию.

Есть целый ряд информационных ресурсов, помогающих составить такое экономическое обоснование: внешние ресурсы в торговых организациях и внутренние ресурсы в соответствующих программах управления рисками или технологии и эксплуатации.

Внешние ресурсы в торговых организациях часто предоставляют ценную информацию о факторах, которые оказывают наиболее сильное влияние на их руководство, для поддержки их деятельности и о ресурсах в их организациях, которые зарекомендовали себя, как наиболее полезные. Для различных отраслей эти факторы могут быть разными, но может существовать сходство в функциях, которые могут выполнять другие специалисты управления рисками.

Внутренние ресурсы, связанные с соответствующей деятельностью по управлению рисками (а именно информационной безопасностью, охраной труда, техникой безопасности и охраной окружающей среды, физической безопасностью и непрерывностью бизнеса), могут оказать неизмеримую помощь на основе своего опыта соответствующих инцидентов в организации. Это информация полезна с точки зрения выделения приоритетных угроз и оценки влияния на бизнес. Эти ресурсы могут также дать представление о том, на работу с какими рисками ориентированы менеджеры, и, таким образом, о том, какие менеджеры могут оказаться наиболее подходящими или готовыми выступать в качестве лидеров.

Внутренние ресурсы, связанные с инженерно-эксплуатационными аспектами систем управления, могут обеспечить детальное понимание того, как системы управления фактически используются в организации. Как сети обычно разделяются? Какую конструкцию обычно имеют высокоопасные системы сгорания или автоматические системы безопасности? Какие контрмеры безопасности уже повсеместно используются? С учетом истории организации по слияниям и поглощениям, также важно понять, насколько репрезентативной является конкретная площадка по отношению ко всему предприятию, региону или всей организации.

Следует иметь в виду, что на ранней стадии промышленной эксплуатации, основной упор будет сделан на определении одного или двух приоритетных вопросов, которые оправдывают дальнейшие работы. При дальнейшей разработке программы информационной безопасности для IACS в перечне могут появиться другие элементы, и приоритеты могут сместиться по мере того как организация будет применять более строгие методы анализа рисков. Однако эти изменения не должны отвлекать от результата первоначальных действий, оправдывающего запуск программы.

A.2.2.4 Содержание предложений для экономического обоснования IACS

В каждой организации путь разработки эффективной программы информационной безопасности для IACS начинается с людей, которые выявляют риски, которые несет организация, и начинают четко формулировать эти риски внутри организации не только с технической точки зрения, но и с точки зрения бизнеса. Экономическое обоснование не является детальной оценкой рисков, это скорее предварительное описание рисков, достаточное для оправдания последующих запланированных шагов по построению CSMS. Обоснование может быть как детальным, так и кратким в зависимости от требований процесса принятия решений в конкретной организации.

Негативные последствия кибератак против IACS для бизнеса могут включать в себя:

- снижение производства или производственные потери на одной или нескольких площадках одновременно;
- травмы или смерть работников;
- травмы или смерть людей в обществе;
- повреждения оборудования;
- экологический ущерб;
- нарушение нормативных требований;

- загрязнение продукции;
- уголовную или гражданско-правовую ответственность;
- потерю служебной или конфиденциальной информации;
- потерю имиджа брэнда или доверия клиентов;
- экономические потери.

При определении приоритетности риска наступления этих последствий также важно учитывать потенциальный источник или угрозу, которая инициирует кибератаки, и вероятность наступления такого события. Киберугрозы могут возникнуть из источников внутри или вне организации. Угрозы могут быть результатом как преднамеренных, так и непреднамеренных действий, а также быть направленными на конкретные цели или ненаправленными. Инциденты в системе информационной безопасности могут быть результатом факторов угрозы различных типов, включая:

- любителей острых ощущений, любителей или аутсайдеров, которые обретают чувство власти, контроля, собственной значимости и удовольствия посредством успешного проникновения в компьютерные сети или ненаправленных (вирусы и «черви») или направленных атак (взлом) с целью кражи или уничтожения информации или нарушения деятельности организации;
- недовольных работников и подрядчиков, которые повреждают системы или крадут информацию из чувства мести или для получения прибыли;
- благонамеренных сотрудников, которые случайно допустили ошибку при внесении изменений в контроллер или работающее оборудование;
- работников, которые нарушают политики качества, безопасности или процедуры удовлетворения других насущных потребностей (например, производственные цели);
- террористов, как правило движимых политическими убеждениями, для которых кибератаки имеют потенциал недорогих, низкорискованных, но мощных атак, в особенности, когда они связаны с координированными физическими атаками;
- профессиональных воров (в том числе организованную преступность), которые осуществляют кражу информации для продажи;
- враждебные государства или группы, которые используют Интернет как военное оружие для кибервойны, чтобы повредить системы командования, управления и коммуникаций противника.

Документально подтвержденные случаи дают представление о том, каким образом и как часто один из таких факторов угрозы становятся причиной негативных последствий для бизнеса. Быстрое внедрение новых сетевых технологий привело к разработке новых инструментов, позволяющих осуществлять кибератаки. В отсутствие признанной общедоступной системы уведомления об инцидентах в ближайшем будущем будет крайне сложно определить количественную вероятность какого-либо конкретного типа произошедшего события. Вероятность будет необходимо оценивать качественно на основе собственной внутренней истории инцидентов в организации, а также на основе нескольких случаев, документация о которых является общедоступной. Ниже представлено несколько примеров таких случаев.

Пример 1 — В январе 2003 года с одного компьютера на другой по всему Интернету и в частных сетях быстро распространялся вирус «SQL Slammer Worm». Он проник в компьютерную сеть атомной электростанции «Davis-Besse»в Огайо и отключил систему мониторинга почти на пять часов, несмотря на убежденность персонала станции в том, что сеть защищена брандмауэром. Это произошло из-за незащищенного соединения между станцией и корпоративными сетями. Вирус «SQL Slammer Worm» атаковал критически важную сеть диспетчерского управления и сбора данных одной из энергетических компаний после перемещения из корпоративной сети в локальную сеть центра управлении. Другая энергетическая компания потеряла сеть ретрансляции кадров, используемую для связи, а некоторые нефтехимические предприятия потеряли HMI и архивы данных. Колл-центр 911 был переведен в автономный режим, были задержаны авиаперелеты, а также выведены из строя банкоматы.

Пример 2 — В течение нескольких месяцев в 2001 году была проведена серия кибератак на компьютеризированную систему очистки сточных вод недовольным подрядчиком в Квинсленде, Австралия. Одна из этих атак вызвала утечку миллионов галлонов неочищенных сточных вод в местную реку и парк. Было проведено 46 вторжений, пока преступника не арестовали.

Пример 3 — В сентябре 2001 года подросток предположительно взломал компьютерный сервер в порту Хьюстона, выбрав своей целью женщину-пользователя чата после спора с ней. Было заявлено, что подросток намеревался отключить компьютер женщины от Интернета, бомбардируя его огромным количеством бесполезных данных, и ему нужно было использовать ряд других серверов, чтобы сделать это. Во время атаки компьютерные системы планирования в восьмом по величине порту мира подверглись бомбардировке тысячами электронных сообщений. Веб-служба порта, содержащая важные данные для командиров судов, швартовочных компаний и вспомогательных фирм, отвечающих за оказание помощи судам при входе и выходе из гавани, стала недоступной.

Организация «CERT» (группа реагирования на нарушения компьютерной безопасности) осуществляла мониторинг и отслеживание количества атак на подключенные к Интернету системы с 1988 года. Ни один из инцидентов

не относился к системам управления. В 2004 году она прекратила отслеживание количества атак, так как распространенность автоматизированных средств нападения привела к тому, что атаки стали настолько распространенными, что количество инцидентов содержало мало информации в отношении оценки масштабов и последствий атак. На рисунке А.3 представлен график данных по инцидентам, демонстрирующий резкое их увеличение за последние 15 лет.

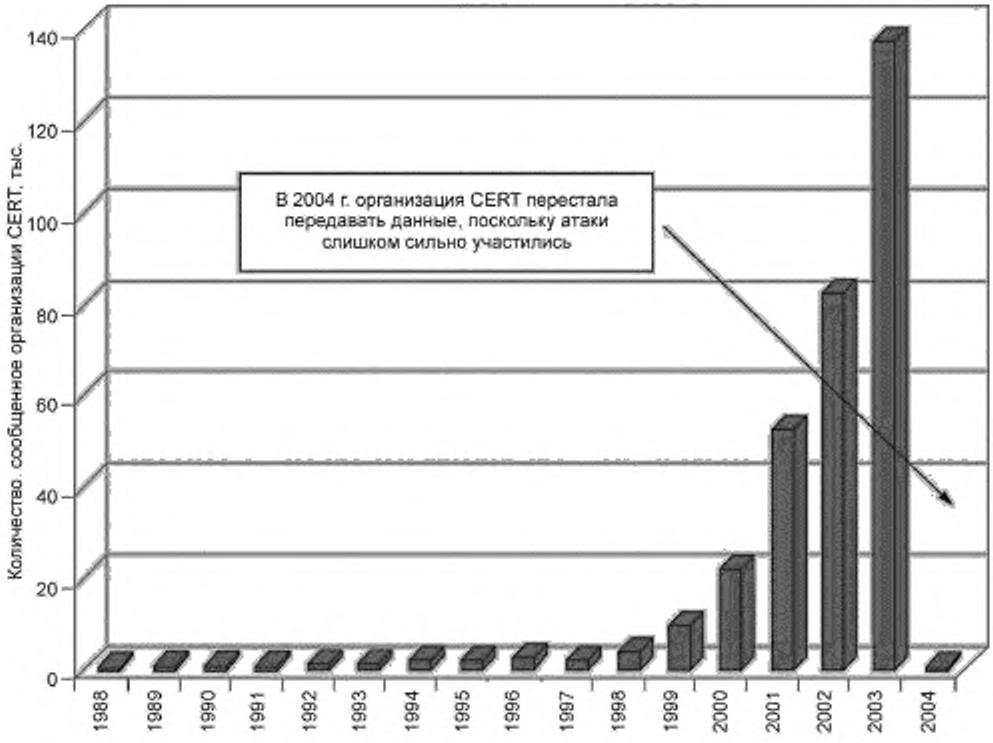


Рисунок А.3 — Подтвержденные атаки на компьютерные системы за период до 2004 г. (источник: CERT)

А.2.2.5 Дополнительные методы

А.2.2.5.1 Базовые методы

К базовым методам относятся следующие действия:

a) выявление и документирование бизнес-целей, важнейших бизнес-процессов и важнейших IT-процессов. Включает IACS и взаимодействие с партнерами цепочки создания стоимости, где конфиденциальная информация передается, хранится или обрабатывается;

b) выявление зависимости бизнеса от IT-систем. Классифицирует зависимость бизнеса, как низкую, среднюю и высокую, или по иной системе ранжирования;

c) определение различных сценариев повреждения от потери конфиденциальности, целостности и доступности информации, включающие в себя:

- манипулирование IACS и последствия таких действий для тех предприятий, которые используют такие системы;

- охрану труда, технику безопасности и охрану окружающей среды, работоспособность и надежность ведущих элементов IACS;

- риски, связанные с цепочкой создания стоимости и другими сторонними партнерами. Эти риски часто включают в себя потерю или изменение конфиденциальной информации. Примером является перехват информации, связанной с поставками продукции, включая тип материалов, количество, логистические маршруты, способ транспортировки и тому подобное;

d) проведение анализа влияния безопасности IACS на бизнес;

e) проведение анализа влияния на бизнес цепочки создания стоимости или других сторонних бизнес-партнеров;

f) определение профиля границ допустимости рисков для организации с точки зрения:
1) безопасности персонала (серьезные травмы или гибель людей);
2) финансовых потерь или последствий, включая штрафы за невыполнение норм;
3) экологических/нормативных последствий;
4) ущерба для имиджа компании;
5) влияния на инвестиционное сообщество;
6) потери клиентской базы или доверия;
7) влияния на инфраструктуру.

Примечание — Границы допустимости риска варьируются в зависимости от бизнеса, т. е. границы допустимости риска для организации являются ее болевым порогом. Границы допустимости риска могут быть очень низкими (например, когда серьезные травмы являются неприемлемыми и при их возникновении проблема должна разрешаться незамедлительно), когда речь идет о производственной безопасности на предприятии, или могут быть очень высокими (например, с точки зрения производственных потерь), если организация имеет несколько производственных площадок для товарной продукции. Финансовые последствия для одного бизнеса могут быть неактуальными для других предприятий. Организации с несколькими предприятиями должны учитывать взаимное влияние одного предприятия на другое при определении границ допустимости риска.

Менеджеры по информационной безопасности обычно знакомы с границами допустимости рисков для организации для некоторых, но не всех из перечисленных последствий. Другие менеджеры, несущие ответственность за управление рисками, связанными с последствиями для охраны труда, техники безопасности и охраны окружающей среды, знакомы с границами допустимости рисков в этих областях. Общий профиль границ допустимости рисков должен определяться путем объединения информации из этих источников, а также из среды IACS.

A.2.2.5.2 Дополнительные методы

Следующие действия относятся к дополнительным методам:

a) выявление и документирование бизнес-целей, важнейших бизнес-процессов и важнейших IT-процессов. Этот процесс целесообразно осуществлять с помощью поперечного разреза организации, на котором показаны функциональные области, а также подразделения компании. Данными вопросами занимается группа специалистов под руководством топ-менеджера, который отвечает за организацию IT, или команды лидеров, которая включает в себя высшее руководство всей организации. Эта группа оценивает риск, связанный с IACS;

b) проведение анализа влияния на бизнес, который описывает проблемы и последствия бездействия и выгоды от действий. По возможности эти действия следует оценивать количественно с точки зрения финансовых последствий (т. е. снижения продаж или штрафов), рыночных воздействий (то есть потери доверия или имиджа), а также влияния с точки зрения охраны труда, техники безопасности и охраны окружающей среды (то есть выбросов в окружающую среду, повреждения оборудования и гибели людей). Следует принимать во внимание, особенно при рассмотрении последствий для имиджа, что инцидент в одном конкретном подразделении может повлиять на организацию в целом;

c) документирование и утверждение (на соответствующем уровне руководства) рисков за пределами CSMS.

A.2.2.6 Используемые ресурсы

Этот элемент частично основан на материалах, приведенных в [24], [26], [27], [30], [42].

A.2.3 Элемент «Выявление, классификация и оценка рисков»

A.2.3.1 Описание элемента

Организации защищают способность выполнять свою миссию путем систематического выявления, определения приоритетности и анализа потенциальных угроз безопасности, уязвимости и последствий использования принятых методик. Риск формально определяется, как ожидание убытков, выражаемое как вероятность того, что конкретная опасность будет включать в себя конкретную уязвимость с конкретными последствиями (см. IEC/TS 62443-1-1). Как описано в элементе «Управление рисками и принятие мер» (см. A.3.4.2), организация определяет свои границы допустимости риска с точки зрения характеристик угроз, уязвимости и выявляемых ею возможных последствий.

Затем организация реализует решение в отношении границ допустимости рисков, принимая установленные меры для уменьшения вероятности угрозы безопасности путем снижения уязвимости и/или уменьшения последствий в случае, если угроза безопасности реализуется.

A.2.3.2 Риск информационной безопасности для системы промышленной автоматики и контроля

Подход к управлению рисками, изложенный в A.2.2, в основном, применяется для всех типов рисков информационной безопасности, а также для других видов рисков. В настоящем подпункте описаны уникальные аспекты анализа рисков информационной безопасности для IACS.

Несмотря на то, что в различных отраслях определенные виды воздействия на бизнес являются более актуальными, а определенные типы угроз — более вероятными, все отрасли, которые используют IACS, должны учитывать, что они вступают в новую рискованную среду. Одновременно с внедрением в IACS коммерческих операционных IT-систем и сетевых технологий и подключением пользователями их взаимосвязанных частных сетей к сетям IACS, также значительно увеличилось число угроз. Существуют риски, связанные с традиционной информацией (электронной или бумажной), классическими IT-системами и приложениями, IACS, деловыми партнерами, совместными предприятиями, сторонними партнерами и т. д.

Риски для традиционных информационных имущественных объектов ориентированы на конфиденциальность, целостность и доступность информации. Риски в IACS отличаются, так как системы управления больше ориентированы на факторы охраны труда, техники безопасности и охраны окружающей среды и эксплуатационную надежность, помимо традиционной защиты конфиденциальности, целостности и доступности информации. В IACS приоритеты обычно изменены с акцентом на доступность, целостность и конфиденциальность (именно в таком порядке). Это означает, что оценка риска информационной безопасности для IACS должна быть согласована с физической безопасностью и охраной труда, техникой безопасности и охраной окружающей среды, когда это целесообразно. Некоторые организации полностью объединяют работу по оценке рисков во всех этих областях. Риски с использованием аутсорсинга, сторонних подрядчиков и других партнеров в цепочке создания производственной стоимости включают в себя конфиденциальную информацию, которая передается, хранится и обрабатывается. Объединение этих бизнес-партнеров в деятельности организации потенциально предоставляет непреднамеренный доступ к системам компании.

Практически во всех этих случаях производственные операции, относящиеся к безопасности, и технологии, разработанные для классических IT-приложений, не применялись для IACS частично из-за невежества, а частично в связи с действительно существующими ограничениями, которых не существует в классических IT-приложениях. Целью настоящего стандарта является решение обоих вопросов.

A.2.3.3 Процесс оценки рисков

A.2.3.3.1 Общие положения

Обзор рисков требуется для подготовки экономического обоснования для CSMS. Более детально приоритеты, рассматриваемые этой системой, определяются на основании методики систематического рассмотрения рисков на более высоком уровне детализации по сравнению с уровнем оценки для составления начального экономического обоснования.

A.2.3.3.2 Оценка рисков и уязвимости

В общей литературе термины «оценка уязвимости» и «оценка рисков» иногда используются как синонимы. Эти два вида анализа можно разграничить в соответствии с определениями «оценка уязвимости» и «оценка риска» в настоящем стандарте. Напомним, что «уязвимость» определяется как недостаток или слабость в конструкции, реализации или эксплуатации и управлении системой, которые могут быть использованы для нарушения целостности системы или политики безопасности (см. IEC/TS 62443-1-1). Например, наблюдение о том, что пароли в центре управления редко меняются, является примером уязвимости, которая будет рассматриваться в оценке уязвимости. С этой уязвимостью может быть связано несколько рисков, например:

- низкая вероятность того, что пароль станет хорошо известен на предприятии с течением времени и работник, не прошедший обучение для работы в системе управления, использует пароль, чтобы решить проблему, что приведет к производственным потерям на несколько часов из-за ошибки ввода;
- низкая вероятность того, что недовольный бывший сотрудник успешно взломает корпоративный брандмауэр для получения удаленного доступа к сети системы управления, войдет в систему HMI и намеренно совершит действия, которые могут привести к производственным потерям на несколько дней.

Так как эти термины используются в настоящем стандарте, результатом оценки рисков является набор рисков, а результатом оценки уязвимости — набор уязвимостей, которые еще не были проанализированы с точки зрения рисков, которые они создают. Таким образом, оценка уязвимости является основой для оценки рисков. Следует иметь в виду, что некоторые существующие методики под названием «методы оценки уязвимости» включают концепции рисков, а другие нет.

При обращении к приведенному выше примеру с паролем диспетчерской становится ясно, что существуют также риски, связанные с периодическим изменением пароля системы управления, например, низкая вероятность того, что оператор не сможет запомнить новый пароль в чрезвычайной ситуации и не сможет войти в систему, чтобы разрешить ситуацию, что приведет к дополнительному серьезному экологическому ущербу. Компромисс между риском, снижаемым путем применения контрмеры, и риском, возникающим при применении контрмеры, как в данном случае, рассматривается в элементе «Управление рисками и принятие мер» настоящего стандарта (см. A.3.4.2).

A.2.3.3.3 Предварительная и детальная оценка рисков

Оценка рисков может осуществляться на нескольких уровнях. Настоящий стандарт устанавливает необходимость проведения оценки рисков на двух уровнях детализации — предварительную и детальную оценку рисков.

При предварительной оценке рисков рассматривается влияние общих типов уязвимостей информационной безопасности и вероятность того, что угроза может включать в себя эти уязвимости, но не учитывать конкретные случаи этих уязвимостей или связанные с ними контрмеры, которые уже были приняты. Таким образом, примеры рисков, выявляемых при предварительной оценке рисков, включают в себя:

- среднюю вероятность того, что произойдет вредоносное заражение, которое вызовет перегрузку сети управления и, следовательно, отсутствие информации о статусе производственного процесса в диспетчерской, что потенциально может привести к аварийному отключению и связанным с ним расходам;
- низкую вероятность того, что подрядчик с криминальными связями и с физическим доступом к сетевым средствам системы несанкционированно подключится к этим средствам и успешно изменит команды управления таким образом, чтобы объект был поврежден.

Предварительная оценка необходима, т. к. опыт показывает, если организации начинают с подробного рассмотрения уязвимостей, они упускают общую картину рисков информационной безопасности и затрудняются определить, в каких местах следует сосредоточить свои усилия, направленные на информационную безопасность. Предварительное изучение рисков может помочь сосредоточить усилия при детальной оценке уязвимости. Предварительная оценка, как правило, охватывает все сети управления, принадлежащие организации, с возможным разделением их на группы с общими характеристиками. Для детального рассмотрения всей IACS ресурсов может быть недостаточно.

Детальная оценка рисков, указанная в настоящем стандарте, дополняется детальной оценкой уязвимости, которая включает в себя изучение такой информации, как существующие технические контрмеры, соблюдение процедур управления учетными записями, патчами и статусами открытых портов отдельных компьютеров в определенной сети, и характеристик подключения системы, например, разделения с помощью брандмауэра, и конфигурации. Таким образом, примерами результата детальной оценки рисков являются:

- прямое подключение инженерных рабочих станций к корпоративной сети и сети системы управления на южном объекте, минуя внутренний брандмауэр сети управления, влияющий на риск заражения сети управления вредоносным программным обеспечением (далее — ПО). В сочетании с отсутствием антивирусной защиты на 50 % компьютеров в сети управления южного объекта это приводит к средней вероятности перегрузки сети, вызванной вирусом, приводящей к отсутствию информации о статусе производственного процесса в диспетчерской и возможному аварийному отключению и связанным с ним расходам;
- все сетевые средства системы управления (например, адреса 192.168.3.x) и соединения с другими сетями физически защищены стенами, потолком или полом или расположены в закрытых помещениях, доступных для трех уполномоченных сетевых администраторов системы управления. Поэтому риск успешной попытки подключения к этим средствам является низким.

Результаты детальной оценки рисков подтверждают соответствующие результаты предварительной оценки в соответствии с указанными примерами. Тем не менее, во время детальной оценки рисков во многих случаях можно определить, что уровень риска ниже или выше, чем предполагалось в предварительной оценке. Детальная оценка рисков может также выявить риски, которые не учитывались в предварительной оценке. И, наконец, учитывая, что детальная оценка выявляет конкретные уязвимости, она обеспечивает направление деятельности организации в отношении рисков, которые считаются неприемлемыми.

A.2.3.3.4 Типы методик оценки рисков

A.2.3.3.4.1 Общие положения

Существуют различные методы оценки рисков, разработанные и продаваемые различными организациями. В общем случае, их можно классифицировать в соответствии с двумя факторами: как они характеризуют отдельные риски (качественно или количественно) и как они структурируют процесс выявления рисков (на основе сценариев или имущественных объектов).

A.2.3.3.4.2 Качественная и количественная характеристика

Качественная оценка рисков обычно опирается на информацию от опытных сотрудников и/или экспертов о вероятности и степени воздействия конкретных угроз на конкретные имущественные объекты. Кроме того, различные уровни вероятности и степени воздействия разделяются на общие классы, например, высокая, средняя и низкая вероятность или степень, а не на конкретные вероятности или экономические последствия. Качественная оценка рисков является предпочтительной, когда существует недостаток достоверной информации о вероятности конкретных угроз, влияющих на конкретные имущественные объекты, или об оценке общих последствий ущерба для конкретных имущественных объектов.

Количественная оценка риска обычно основывается на обширных массивах данных, которые фиксируют скорость причинения ущерба имущественным объектам на основе воздействия определенных комбинаций угроз и уязвимостей. Если эта информация доступна, она может обеспечить более точную оценку риска, чем методы качественной оценки рисков. В связи с недавним воздействием угроз информационной безопасности на IACS, относительно низкой частотой, с которой происходят инциденты, и быстро развивающимся характером угроз, еще не созданы обширные массивы данных, помогающих оценить угрозы информационной безопасности для IACS. На данном этапе качественная оценка рисков является предпочтительным методом для оценки этих рисков.

A.2.3.3.4.3 Оценка на основе сценариев и оценка на основе имущественных объектов

При проведении оценки рисков обычно следует сосредоточиться на одном из двух аспектов: сценариях, в соответствии с которыми угрозы используют уязвимости для воздействия на имущественные объекты, или на самих имущественных объектах. При подходе, основанном на сценариях, может быть использован опыт реальных инцидентов или ситуаций, практически приведших к инциденту. Однако данный подход может не выявить угрозы или уязвимости для критичных имущественных объектов, которые ранее не были под угрозой. При подходе, основанном на имущественных объектах, можно будет использовать знания о системах организации, методах работы и конкретных имущественных объектах, воздействие угроз на которые может привести к серьезным экономическим последствиям. Данный подход может не выявить типы угроз или уязвимостей, которые ставят эти имущественные объекты в опасность или сценарии, связанные с несколькими имущественными объектами. Какой бы общий подход ни использовался, рекомендуется включать какой-либо аспект второго подхода для обеспечения более тщательной оценки рисков.

Пример — Организация, которая определила имущественные объекты как устройства, приложения и данные, является примером организации, объединяющей методы, основанные на сценариях и на имущественных объектах. На следующем этапе организация рассматривает возможные сценарии, относящиеся к этим имущественным объектам, и определяет последствия, как указано ниже. Сценарии для приложений очень схожи с приведенными сценариями для устройств.

a) Сценарии для устройств

1) Неавторизованный пользователь, получающий локальный доступ к устройству IACS

Определить, что является следствием того, что кто-то подходит к устройству и выполняет задачи, разрешенные данным устройством;

2) Удаленный доступ к устройству IACS, полученный неавторизованным пользователем

Определить, что является следствием получения неавторизованным пользователем удаленного доступа к этому устройству и выполнения какой-либо из задач, разрешенных на этом устройстве;

3) Устройство IACS отключено или уничтожено

Определить, что является следствием инцидента в системе информационной безопасности, который блокирует выполнение устройством всех или части его обычных функций;

b) Сценарии для данных

1) Кража данных IACS

Определить, что является следствием кражи такого массива данных:

- имеет ли массив данных высокую стоимость как объект интеллектуальной собственности;
- имеет ли массив бизнес-ценность для конкурентов;
- будет ли массив данных после обнародования являться порочащим для организации;
- является ли массив данных необходимым для соблюдения нормативных требований;
- являются ли данные предметом судебного приказа о хранении;

2) Повреждение данных IACS

Определить, каковы возможные последствия, если:

- массив данных будет перехвачен и изменен между источником и местом назначения;
- массив данных будет поврежден у источника;
- является ли массив данных необходимым для соблюдения нормативных требований;
- являются ли данные предметом судебного приказа о хранении;

3) Отказ в обслуживании данных IACS

Определить, каковы последствия того, что пользователю будет отказано в доступе к массиву данных IACS.

Примечание — Группа может осуществить основанную на сценариях оценку рисков, начав с описаний сценариев инцидентов, а затем определить последствия сценария, как показано в данном примере, или начать с создания списка нежелательных последствий, а затем действовать в обратном направлении для разработки возможных сценариев инцидента, которые могли бы привести к таким последствиям. Допускается также использовать комбинацию указанных подходов.

A.2.3.3.5 Выбор методики оценки рисков

Выбор правильной методики оценки рисков для организации очень субъективен и зависит от ряда вопросов. Многие из этих методик имеются на рынке. Некоторые предоставляются бесплатно, для других требуются лицензии на использование. Выбор методики оценки рисков наиболее применимой для организации, может быть сложной задачей. Общим для большинства методик является предположение о том, что риск представляет собой комбинацию вероятности события и последствий такого события.

Сложность заключается в количественной оценке вероятности возникновения, которая обычно выражается аналогично вероятности. Отраслевой опыт, связанный с технологической безопасностью и аварийностью, предоставляет большое число исторических количественных данных, на которых основываются значения вероятности.

Однако, определение соответствующих значений вероятности конкретного инцидента в системе информационной безопасности является непростым не только из-за отсутствия исторических данных, но и потому, что на основе прошлого опыта нельзя предсказать, что произойдет, когда уязвимость станет известна потенциальным нарушителям. Из-за этого осложнения многие компании и торговые ассоциации выбирают разработку своих собственных методик для устранения угроз и уязвимостей, имеющих особую важность для них, в соответствии с их корпоративной культурой. Также по этой причине в настоящем стандарте используется термин «вероятность возникновения», которая относится к оценке человеческих способностей и намерений, вместо ожидаемого термина «вероятность», который относится к возникновению природных явлений, свободных от человеческого вмешательства.

Использование некоторых методик позволяет провести предварительную оценку рисков. Использование других методик — детальную оценку рисков, давая возможность использовать результаты оценки уязвимости, а также методики могут служить непосредственно руководством для соответствующей детальной оценки уязвимости. Для организации эффективным является использование методики, позволяющей провести как предварительную, так и детальную оценку рисков.

Пример — Пример торговой ассоциации, помогающий решить задачу выбора правильной методики «Химический центр информационных технологий Американского химического совета» (ChemITC,)

опубликовал документ под названием «Доклад о методиках оценки уязвимости информационной безопасности, версия 2.0». [27] В нем рассматриваются различные элементы одиннадцати методик, которые сравниваются с набором критериев, имеющих значение для универсальных методик оценки рисков информационной безопасности для оценки коммерческих IT-систем, IACS и цепочек создания стоимости. В докладе предложены руководства по выбору методики. Часть руководства включена в следующие пункты с разрешения CSCSP.

a) шаг 1 — Фильтр

Первый шаг заключается в рассмотрении обзора выбранных методик. Целью этого шага является выявление интересующих методик на основе таких критериев, как простота использования, сложность, объем, потребность в ресурсах и тип методики [см. [27] (приложение IV)];

b) шаг 2 — Выбор

После определения методики следует выбрать методики, которые соответствуют потребностям организации [см. [27] (приложение II)]. В [27] (приложение II) определены конкретные критерии, которые были использованы для оценки методики. Критерии, перечисленные в нем, относятся к более обширному IT-пространству за пределами IACS. Вполне возможно, что необходимой является методика, учитывающая только подгруппу критериев, используемых в исследовании «ChemITC». Понимание разницы между потребностями организации и критериями оценки будет полезно при рассмотрении кратких обзоров различных методик. Затем следует ознакомиться с соответствующим кратким обзором для того, чтобы получить более подробную информацию для принятия обоснованного решения о выборе методики [см. [27] (приложение V)].

В кратком обзоре каждой методики рассматривается следующее:

- методика оценки уязвимости информационной безопасности;
- рецензенты;
- дата;
- веб-адрес;
- общие замечания;
- сильные стороны по сравнению с общими критериями оценки;
- пробелы по сравнению с общими критериями оценки;
- каким образом методика может быть использована;
- ограничения использования методики;
- предлагаемые изменения;

c) шаг 3 — Подтверждение решения (необязательно)

Если есть неопределенность или трудности в выборе методики, см. сводную таблицу технических критериев, приведенную в [27] (приложение II) по конкретной методике для подтверждения выбора организации(й). Сводная таблица технических критериев существует для каждой методики. Этот шаг является необязательным, т. к. он просто предоставляет еще более конкретные данные для оценки;

d) шаг 4 — Приобретение выбранной методики

После сужения круга методик до одной методики ее следует приобрести у поставщика. Веб-адреса, указанные в элементе настоящего стандарта «Библиография», являются хорошей отправной точкой.

A.2.3.3.6 Предварительная оценка рисков — выявление рисков

После того, как был определен набор ключевых заинтересованных сторон, прошедших обучение по основным свойствам IACS, они будут выполнять предварительную оценку рисков в соответствии с выбранной организацией методикой. В ходе процесса оценки уточняется характер отдельных рисков для организации, которые возникают в результате использования IACS. Это необходимо для окончательного выбора наиболее экономически эффективных контрмер, которые должны быть разработаны или применены, и для оправдания затрат на их применение. Поскольку эта задача является первым этапом оценки рисков, она не является детальной оценкой уязвимости или угроз. Она обычно включает в себя совещание по анализу рисков для сбора информации от всех заинтересованных сторон и использует предварительно определенные последствия для бизнеса, которые могут быть выявлены в экономическом обосновании.

Документом, являющимся результатом совещания по анализу рисков, является перечень сценариев, которые описывают, каким образом конкретная угроза может включать в себя конкретный тип уязвимости и нанести повреждения конкретным имущественным объектам, что приведет к выявленным негативным последствиям для бизнеса. На таком совещании также может быть точно определен уровень последствий и приоритетов по границам допустимости рисков.

Заинтересованные стороны, которые имеют опыт работы с IACS в коммерческих организациях, и лица, ответственные за управление соответствующими рисками, должны участвовать в работе по оценке рисков, чтобы использовать свои знания и опыт.

Для наиболее эффективного использования времени участников, проведению совещания по анализу рисков с участием всех заинтересованных сторон, как правило, необходимо посвятить полтора дня. Совещание по анализу рисков разбивается на две фазы: предоставление исходной информация и выявление рисков.

Независимо от того, какой метод оценки рисков используется в конечном итоге, важно обеспечить участников совещания по анализу рисков соответствующей исходной информацией перед тем, как приступать к выявлению

рисков. Обычно исходная информация включает в себя обзор экономического обоснования и устава, обзор архитектуры и функций IACS и обзор конкретных типов инцидентов, произошедших в организации, или обнародованных инцидентов, произошедших в других организациях.

Для успешного проведения совещания важно также, что участники понимали рабочие определения рисков и уязвимости. В противном случае, в ходе совещания, вероятно, будут определены уязвимости, но выявление рисков может пройти безуспешно. Например, ненадежная аутентификация в системе управления HMI является уязвимостью. Связанной с этой уязвимостью угрозой является риск того, что работник с недостаточным опытом может работать с HMI без присмотра и установить небезопасные параметры. Последствием может быть остановка производства в связи со срабатыванием устройств защиты. Распространенной ошибкой является то, что организация сначала определяет уязвимости информационной безопасности, а затем приступает к их снижению.

A.2.3.3.7 Предварительная оценка рисков — Классификация рисков

A.2.3.3.7.1 Общие положения

Перечень сценариев, являющихся результатом совещания по анализу рисков, описывает ряд различных рисков, вызываемых в организациях угрозами для IACS. Одной из обязанностей корпоративного управления является управление всеми рисками организации. Для облегчения этой работы риски должны быть выявлены и расположены по приоритетности. В настоящем подразделе описываются три шага по разработке принципов определения приоритетности отдельных рисков для оправдания соответствующих корректирующих действий.

A.2.3.3.7.2 Уравнение риска

Прежде чем описывать принципы определения приоритетности рисков и калибровки, важно понять основную концепцию анализа рисков (например, уравнение риска).

Вероятность произошедшего события учитывает как вероятность реализации угрозы, которая может привести к действию, так и вероятность того, что уязвимость, которая допускает действие, будет действительно использована угрозой. Например, вирус, повреждающий сети, должен сначала попасть в сеть, а затем победить антивирусную защиту сети. Если вероятность возникновения выражается аналогично вероятности, то:

$$\text{Вероятность}_{\text{наступления_события}} = \text{Вероятность}_{\text{реализации_угрозы}} \times \text{Вероятность}_{\text{используемой_уязвимости}} \quad (A.1)$$

Как упоминалось выше, риск включает вероятность и последствия, где последствием является негативное воздействие, которое испытывает организация из-за причинения конкретного ущерба имущественным объектам организации конкретной угрозой или уязвимостью.

$$\text{Риск} = \text{Вероятность}_{\text{наступления_события}} \times \text{Последствия} \quad (A.2)$$

A.2.3.3.7.3 Калибровка шкал вероятности и последствий

Системы управления рисками были разработаны в большинстве организаций для управления самыми разнообразными рисками. В некоторых случаях использование таких систем было предписано нормативными требованиями. Такие системы управления рисками используют одно уравнение риска для установления приоритетности рисков для организации по одинаковым типам угроз для различных имущественных объектов (например, информационная безопасность) или по различным угрозам для одинаковых имущественных объектов (то есть обеспечения непрерывности бизнеса, промышленной эксплуатационной безопасности, экологической безопасности и физической безопасности). В большинстве организаций в этих системах управления рисками уже разработаны шкалы вероятности и последствий.

Типичная шкала вероятности показана в таблице A.1. Эта шкала является только примером. Организация должна определить фактические значения для этой шкалы с учетом своего случая.

Таблица A.1 — Типичная шкала вероятности

Вероятность возникновения	
Категория	Описание
Высокая	Угроза/уязвимость, наступление которой вероятно в следующем году
Средняя	Угроза/уязвимость, наступление которой вероятно в течение следующих 10 лет
Низкая	Угроза/уязвимость, наступление которой ни разу не было зафиксировано и считается маловероятным

Большинству организаций трудно согласовать вероятность, и в настоящее время существует мало информации, которая может в этом помочь. Вполне очевидно, что различные мнения об этом факторе могут радикально изменить инвестиции в CSMS. Даже если не все смогут согласиться с окончательной оценкой вероятности, преимущество ее использования заключается в том, что предположения, используемые для стимулирования инвестиций в CSMS, понятны для всех. Поскольку вероятность возникновения является основным фактором риска, о

котором организация имеет наименьшее количество информации и который она не может контролировать, важно отслеживать улучшения в отраслевых показателях для уточнения этого фактора.

Для решения проблемы с согласованием некоторые организации используют следующие методы:

- использование 100 %-ной вероятности и, следовательно, рассмотрение только последствий или использование этого метода для некоторых видов последствий, таких как охрана труда, техника безопасности и охрана окружающей среды;
- согласование диапазона или категорий вероятности, а затем определение их приоритетности на основе диапазонов;
- попытка увеличения точности, используя отраслевые данные об атаках на IACS;
- попытка увеличения точности путем сбора внутренних данных об инцидентах;
- разделение вероятности возникновения на два фактора: вероятность того, что противник попытается провести атаку, и вероятность того, что атака будет успешной. Разделение этих факторов может помочь прояснить реальный источник разногласий. Если все согласятся, что попытка увенчается успехом, и аргумент в пользу низкого уровня риска основан на надежде, что попытка не будет предпринята, направленность дискуссии может измениться.

Последствия обычно измеряются по-разному для разных видов рисков. Типичная шкала последствий показана в таблице А.2. Этот пример иллюстрирует, как оценка риска информационной безопасности может учитывать безопасность технологического процесса и другие организационные риски. Как уже упоминалось, эта шкала является только примером и должна быть откалибрована для организации.

Важно проводить оценку последствий с высоким уровнем честности. Во время оценки следует выявить предположения, которые влияют на уровень последствий. Например, было бы разумно предположить, что были установлены все блокировки безопасности и системы отключения для минимизации влияния любого события, поскольку вероятность события в информационной системе в сочетании с несвязанной аварией, которая отключает системы безопасности, очень мала. Тем не менее, делая такое предположение, необходимо рассмотреть, существует ли риск преднамеренной кибератаки, использующей случайную неисправность систем безопасности, или физической скоординированной или информационной атаки, вызывающей такие неисправности. К другим возможным предположениям, на которые можно указать, относится предположение о том, что технологические режимы выполняются как при обычной работе, а также выполняются основные процедуры блокировки. Для предприятий важно четко оценить риск, учитывая сложность и состояние системы управления и соответствующих операций и зависимость работы объекта от этой системы.

Калибровка последствий обязательно осуществляется с учетом интересов и политики организации, осуществляющей оценку риска. Несмотря на то, что риск для IACS может быть очень сильно подвержен влиянию опасностей, связанных с производственной деятельностью, управляемой IACS, важно не путать риски для организации с рисками для общества.

В ходе производственной деятельности могут не использоваться какие-либо опасные материалы, но может производиться очень ценная и востребованная продукция, приносящая высокие доходы компании. Инцидент с безопасностью IACS, вызвавший нарушение производственной деятельности, в результате чего в течение нескольких дней производилась не соответствующая требованиям продукция, которая не может быть продана, может иметь очень серьезные финансовые последствия для компании. Для этой компании IACS имеет высокий уровень риска, несмотря на то, что для общества уровень риска может быть низким, поскольку отсутствует какое-либо влияние на здоровье, безопасность общества или окружающую среду. Аналогично эта же организация может считать, что уровень риска последствий нарушения производственной деятельности на промышленном предприятии, использующем вредные материалы, является высоким, даже если такое нарушение не влияет на производство, из-за внутренней политики и/или внешних норм, касающихся общественной безопасности.

Перед сбором группы для проверки производственных рисков следует составить четкие шкалы вероятности и последствий, которыми будет руководствоваться указанная группа.

Таблица А.2 — Типичная шкала последствий

Последствие									
Категория	Область риска								
	Планирование непрерывности бизнеса		Информационная безопасность			Безопасность производственной деятельности		Безопасность окружающей среды	Влияние на общество
	Остановка производства на одной площадке	Остановка производства на нескольких площадках	Затраты (млн долларов США)	Правовая	Доверие общества	Персонал на площадке	Люди за пределами площадки	Окружающая среда	Инфраструктура и услуги
A (высокая)	менее семи дней	менее одного дня	< 500	Тяжкое уголовное преступление	Потеря имиджа брэнда	Смерть	Смерть или серьезный инцидент в обществе	Предписание регионального или национального органа или долговременный существенный ущерб для большой территории	Влияние на различные отрасли или серьезное нарушение общественного обслуживания
B (средняя)	менее двух дней	< 1 ч	< 5	Малозначительное уголовное преступление	Потеря доверия клиентов	Потеря рабочего дня или серьезная травма	Жалобы или влияние на местное сообщество	Предписание местного органа	Возможное влияние на отрасль на уровне, превышающем уровень влияния одной компании. Возможное влияние на общественное обслуживание
C (низкая)	более одного дня	> 1 ч	> 5	Нет	Нет	Первая помощь или подтвежденная травма	Нет жалоб	Небольшое, выбросы ниже пределов, подлежащих сообщению	Небольшое или отсутствие влияния на отрасли, превыша-ющее влияние отдельной компании. Небольшое или отсутствие влияния на общественное обслуживание

А.2.3.3.7.4 Уровень риска

Результатом качественной оценки рисков является перечень имущественных объектов или сценариев с ранжированием общего уровня рисков. Обычно такой перечень оформляют в форме таблицы, аналогичной таблице А.3, в которой определены три уровня риска на основе трех уровней вероятности и последствий. Таким образом, каждому риску при оценке присваивается уровень риска. Указанная таблица является примером и требует дальнейшего анализа со стороны организации.

Таблица А.3 — Типичная таблица уровня риска

Вероятность возникновения	Категория последствий		
	А	А	А
Высокая	Высокий уровень риска	Высокий уровень риска	Средний уровень риска
Средняя	Высокий уровень риска	Средний уровень риска	Низкий уровень риска
Низкая	Средний уровень риска	Низкий уровень риска	Низкий уровень риска

Каждый уровень риска в каждом блоке (высокий, средний и низкий) соответствует конкретной комбинации вероятности и последствий. Организация вырабатывает политику определения границ допустимости рисков для каждого уровня риска, которая будет соответствовать конкретному уровню реакции компании. Фактический подход к снижению риска может быть связан с использованием определенных контрмер. Первоначальная версия приведенной таблицы должна быть составлена ответственным руководством компании до анализа рисков. Данный метод рекомендуется для обеспечения того, что оценка рисков даст результаты, непосредственно помогающие принимать решения и дающие организации основания для принятия мер.

Для получения дополнительной информации о выработке политики определения границ допустимости рисков, а также о том, каким образом политика определения границ допустимости рисков и результаты оценки рисков используются для управления рисками (см. А.3.4.2).

А.2.3.3.8 Детальная оценка рисков

А.2.3.3.8.1 Общие положения

Детальная оценка рисков ориентирована на отдельные сети и устройства IACS и учитывает детальную оценку технической уязвимости этих имущественных объектов и эффективность существующих контрмер. Не для всех организаций целесообразно проведение детальной оценки рисков сразу для всех имущественных объектов IACS. В этом случае организация соберет достаточно информации о своих IACS, позволяющей ей определить приоритетность этих систем и принять решение о том, какие системы должны быть проанализированы в первую очередь при детальной оценке уязвимости и рисков.

В ходе детальной оценки рисков выявляются риски и определяется их приоритетность. Риски выявляются для каждой IACS. После выявления рисков организация может определить приоритетность всех рисков, выявленных во всех системах, или рисков отдельно для каждой системы, либо определить приоритетность рисков, выявленных в подгруппах изученных IACS, например, всех IACS на конкретной площадке. Поскольку определение приоритетности в конечном итоге приводит к принятию решений о том, какие действия будут предприняты, а также решений об инвестициях для совершенствования информационной безопасности, объем приоритезации должен соответствовать объему бюджета и решениям полномочного органа организации для осуществления инвестиций. Например, если управление и финансирование всех IACS конкретной производственной линии выполняется как для группы, определение приоритетности выполняется совокупно для рисков этих IACS в целях облегчения принятия решений руководством.

А.2.3.3.8.2 Определение характеристик ключевых систем промышленной автоматики и контроля

Для выявления и приоритезации рисков IACS необходимо, чтобы организация определила местонахождение и выявила ключевые IACS и характеристики этих систем, которые создают риски. Без инвентаризации устройств и сетей IACS сложно оценить и определить приоритет мест, где требуется принятие мер по безопасности и где они будут оказывать наибольшее влияние.

Группа специалистов должна совместно с персоналом IACS выявить различные системы, используемые на площадке и управляющих удаленными объектами. Акцент должен быть сделан на системах, а не на устройствах, включая без ограничения системы управления, системы измерения и системы мониторинга, которые используют центральное устройство HMI. Необходимо учитывать как производственные зоны, так и инженерные зоны, например, электростанции и оборудование переработки отходов.

Как было указано выше, целью является определение основных устройств и типов устройств, которые используются и функционируют совместно для управления оборудованием. На этой стадии разработки программы безопасности нет необходимости в полной инвентаризации всех устройств IACS, поскольку инвентаризация потребует принятия субъективных решений о риске, который устройства управления привносят в производственную деятельность. Например, важно понимать:

- являются ли аналоговыми или цифровыми полевые приборы КИПиА и передача данных с полевых датчиков в контроллеры;
- соединены ли устройства/системы друг с другом и каковы типы используемых сетей;
- расположены ли устройства в охраняемой зоне, например, в здании и в огороженной зоне, или устройства расположены на расстоянии;
- подлежат ли устройства управления обязательному контролю;
- является ли потеря или неисправность устройства/системы значительной с точки зрения влияния на управляемое оборудование, а также с точки зрения бизнеса/финансовой точки зрения и с точки зрения охраны труда, техники безопасности и охраны окружающей среды.

Результаты идентификации устройств/систем должны показывать масштаб влияния на управляемое оборудование при потере устройствами управления производственной деятельностью, в которой они применяются, а также относительную уязвимость безопасности таких устройств (физическую, сетевую или иную). Этот тип информации может использоваться для понимания относительного риска для производственной деятельности. На данной стадии нет необходимости в проведении полной инвентаризации для определения точного числа каждого типа устройств.

А.2.3.3.8.3 Группирование устройств и систем и проведение инвентаризации

После выявления группой специалистов отдельных устройств/систем можно сгруппировать объекты в логические группы оборудования. В современных устройствах IACS эта совокупность оборудования функционирует как комплексная система управления различными действиями при производственной деятельности. Число логических систем управления в компании может варьироваться в широком диапазоне. В средних и крупных компаниях может существовать несколько сотен логических IACS, состоящих из тысяч отдельных устройств и систем низкого уровня.

Для средних и крупных организаций, решающих проблемы с кибербезопасностью в масштабе всей компании, может быть целесообразным составление перечня логических систем в базе данных с функцией поиска. Распределенные системы управления могут быть организованы по агрегатам, узлам, ячейкам или транспортным средствам в пределах локального или удаленного географического объекта. Системы SCADA могут быть организованы по центрам управления, удаленным объектам и соответствующему оборудованию управления. База данных будет более эффективной, если данные будут собираться в стандартном формате для облегчения сравнения одной системы с другой. На рисунке А.4 показан пример стандартного формата, который можно легко создать в форме сравнительной таблицы или базы данных. Он был включен, чтобы дать толчок к размышлениям о типе информации, который может использоваться позже при определении приоритетности систем и детальной оценке рисков.

Характеристика сети системы промышленной автоматики и контроля

Компания _____

Объект _____

Действующий агрегат _____

Контактное лицо по IT на объекте _____ Телефон _____

Контактное лицо по управлению технологическим процессом на площадке _____ Телефон _____

Последнее обновление _____

ПРОСИМ ОТВЕТИТЬ НА СЛЕДУЮЩИЕ ВОПРОСЫ:

_____ Подключены ли производственные системы и системы управления в настоящее время к LAN объекта или корпоративным сетям?

_____ Можно ли получить удаленный доступ к производственным системам и системам управления откуда-либо за пределами домена IACS?

Домен системы управления технологическим процессом

_____ Общее количество узлов, имеющих IP-адрес

_____ Количество узлов, имеющих IP-адрес, к которым может быть получен доступ откуда-либо за пределами домена системы управления

_____ Количество параллельных пользователей внутри домена IACS

_____ Количество параллельных пользователей внутри домена IACS, требующих доступа к внешним ресурсам

_____ Общее количество пользователей за пределами домена IACS, требующих доступа к ресурсам системы управления технологическим процессом

_____ Количество параллельных пользователей за пределами домена IACS, требующих доступа к ресурсам системы управления технологическим процессом

IP-адреса (отметьте нужное)

_____ протокол динамической конфигурации узла

_____ статические адреса

_____ используемые общедоступные адреса (т. е. x.x.x.x)

_____ используемые частные адреса (192.168.x.x)

Управляющие платформы

_____ Количество управляющих платформ

_____ Тип управляющих платформ (PLC, DCS, PC)

Поставщик управляющей платформы _____ _____

Модель управляющей платформы _____ _____

Операторская консоль и устройства HMI

_____ Количество операторских консолей

Поставщик операторской консоли _____ _____

Модель операторской консоли _____ _____

OS операторской консоли _____ _____

Узлы приложений (отметьте нужное)

_____ Управление технологическим процессом и сервер управления

_____ SCADA

_____ OPC-сервер

_____ Инженерная рабочая станция

_____ Пакетный сервер

_____ Прочее _____

Используемые сетевые барьеры безопасности

Тип (брандмауэры, маршрутизаторы, VLAN и т. д.) _____

Предполагаемая поддержка сетевой безопасности (отметьте нужное)

_____ Ресурсы объекта

_____ Внешняя (третья сторона)

Рисунок А.4 — Образец таблицы сбора данных о логических системах IACS, лист 1

Сеть объекта (ответьте да/нет)

_____ Существующие топологические схемы сети объекта имеются в наличии и актуальны?

_____ Расположены ли узлы системы управления технологическим процессом на изолированном сегменте LAN?

_____ Существует ли на объекте политика информационной безопасности?

_____ Аудит службы безопасности завершен

(если «Да»,то дата завершения _____)

_____ Использует ли объект двухфакторную аутентификацию?

_____ Оценка рисков службой безопасности завершена

(если «Да», то дата завершения _____)

Требования удаленного доступа (отметьте нужное)

_____ Через LAN объекта/корпоративную сеть

_____ Через модем с наборным вызовом

_____ Через Интернет

_____ Через локальный модем с наборным вызовом, напрямую привязанным к узлам производства и управления

Требования к локальному выходу (отметьте нужное)

_____ К приложениям и ресурсам объекта (системы управления документацией, системам качества, бизнес-системам)

_____ К корпоративным приложениям и ресурсам (системы управления документацией, системам качества, бизнес-системам)

_____ К Интернет-сайтам

Рисунок А.4, лист 2

Определение производственных устройств/систем автоматизированного управления необходимо проводить тщательно и уделять внимание не только устройствам, непосредственно осуществляющим управление. К системам или сетям относятся не только PLC или распределенные системы управления. На производственном объекте полного цикла IACS состоит из устройств, которые непосредственно используются для производства, проверки, управления или отгрузки продукции, и может включать, среди прочего, следующие компоненты:

- распределенные системы управления и соответствующие устройства;
- системы диспетчерского управления и сбора данных и соответствующие устройства;
- PLC и соответствующие устройства;
- станции HMI;
- автоматизированную систему безопасности и соответствующие устройства;
- цеховые (специальные) компьютеры;
- системы управления производственными данными и системы управления производством;
- промышленные системы автоматизированного моделирования процессов и методов управления;
- экспертные системы;
- системы проверки;
- системы транспортировки и отслеживания материала;
- анализаторы;
- системы измерения;
- системы пакетной обработки;
- системы мониторинга и/или управления электроснабжением;
- системы удаленной телеметрии;
- системы связи, используемые для связи с удаленными устройствами;
- системы стандартных условий эксплуатации и стандартной процедуры эксплуатации;
- системы управления документацией;
- компьютеры разработки программ;

- системы управления отоплением, вентиляцией и кондиционированием воздуха;
- сетевые коммуникационные шлюзы (т. е. коммутаторы, концентраторы и маршрутизаторы);
- сетевые защитные устройства (т. е. брандмауэры и системы обнаружения вторжений).

Следует рассмотреть все сетевые устройства на основе центральных процессоров, которые имеют решающее значение для поддержания производства. Целью этой стадии инвентаризации является обнаружение устройств, которые уязвимы для сетевых атак, для их включения в детальную оценку рисков.

Примечание — На данной стадии не следует принимать решение о том, какие устройства должны быть изолированы или отделены от локальной компьютерной сети. Лучше ошибиться, включив больше устройств, чем меньше. После проведения оценки рисков и получения лучшего представления об общей уязвимости группа оценки должна решить, необходимы ли на самом деле решения по смягчению рисков и где должны быть расположены различные устройства.

На рынке доступно несколько корпоративных инструментов инвентаризации, которые будут работать в сетях для выявления и документирования всех аппаратных средств, систем и программного обеспечения (ПО), существующего в сети. Применять этот тип приложения для идентификации IACS следует с осторожностью. Необходимо провести оценку того, как работают эти средства и какое влияние они могут оказать на подключенное оборудование управления, прежде чем использовать любое из них.

Оценка инструментов может включать в себя тестирование в аналогичных, автономных, непроизводственных условиях системы управления для обеспечения того, что инструмент не окажет негативное влияние на работу системы управления и не нарушит производство. Несмотря на то, что непроизводственные устройства могут не оказывать никакого влияния на производственные системы, они могут отправлять информацию, которая может вызывать (и в прошлом вызывала) сбои или неисправность систем управления. Воздействие может быть связано с характером информации и/или трафиком и нагрузкой на систему. Несмотря на то, что это влияние может быть приемлемым в информационных системах, оно неприемлемо в IACS.

A.2.3.3.8.4 Разработка простых сетевых схем

Простая сетевая схема позволяет группировать различные системы и устройства промышленной автоматизации и управления и объединять их в идентифицируемую логическую систему управления. Она должна включать в себя устройства, определенные в таблице сбора логических данных IACS, о чем говорилось в A.2.3.3.8.2. Схема должна отражать базовую архитектуру логической сети, например, способы сетевого взаимодействия, в сочетании с некоторыми физическими базовыми элементами сетевой архитектуры, например, расположение устройств.

Перед тем, как определить приоритеты IACS и выполнить детальный анализ рисков, важно обеспечить, чтобы у группы имелось четкое понимание сферы применения/границ системы, подвергаемой анализу. Сетевая схема выполняет роль инструмента для визуализации сети и помогает при проведении анализа риска. Это может быть очень простая блок-схема, на которой показаны устройства, системы и интерфейсные соединения, или более детальная схема, как например, схема, представленная на рисунке А.5. Применяя любой такой подход, можно добиться поставленных целей. Если определены зоны и каналы, они должны быть показаны на простой сетевой схеме. (Более подробные пояснения по разработке зон и каналов представлены в A.3.3.4.).

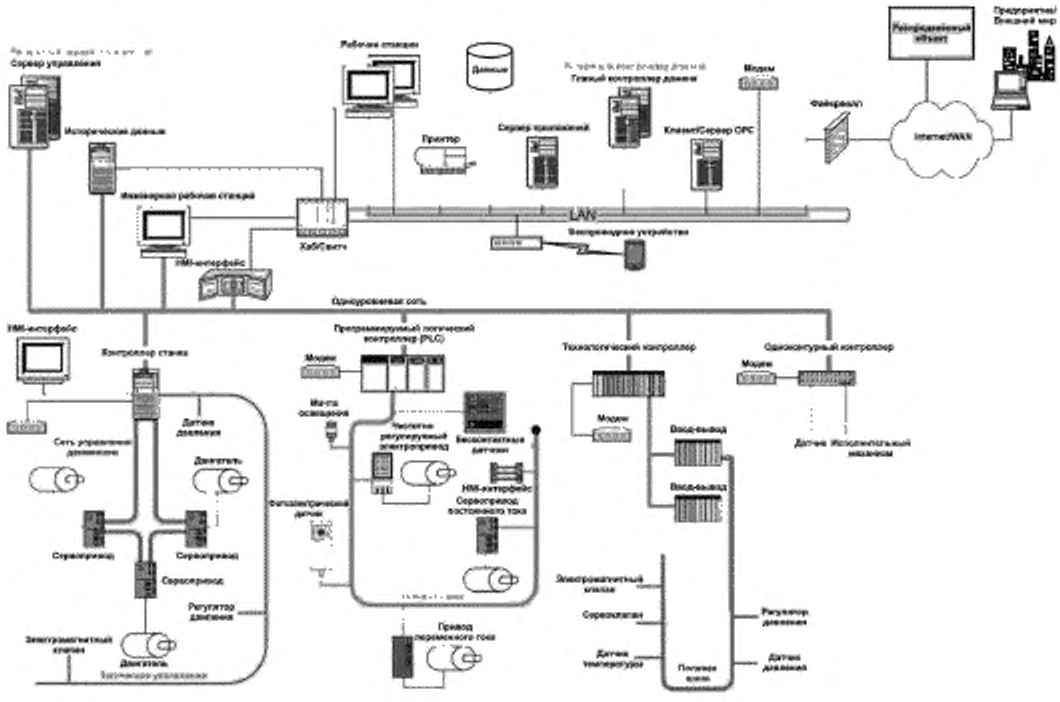


Рисунок А.5 — Пример схемы логической сети с высокой степенью детализации графическими средствами

Простые сетевые схемы являются начальной точкой и отображают состояние за конкретный момент времени. Опыт по проведению детального анализа уязвимостей подсказывает, что практически при каждой оценке обнаруживаются соединения, не идентифицированные при составлении первоначальных схем. Поэтому такие схемы не должны быть единственной основой для оценки возможности взаимодействия, когда не требуется проведение более детальной физической проверки. Они полезны для определения масштаба работ по оценке рисков и определения зон и каналов, описанных в IEC/TS 62443-1-1.

А.2.3.3.8.5 Предварительная оценка общего риска для каждой идентифицированной системы

После составления списка устройств, объектов и сетей IACS необходимо выполнить предварительную оценку относительного уровня риска, связанного с системами, чтобы можно было расставить их приоритеты для детальной оценки риска. Если детальная оценка риска должна быть проведена в отношении всех IACS или если в результате проведения укрупненного анализа риска получены достаточные данные для определения приоритетов отдельных IACS по типу риска, то этот шаг не потребуется.

Необходимо выполнить оценку каждой отдельной системы, чтобы понять последствия для финансовой сферы и HSE, определенные при укрупненном анализе риска, если такому риску подвергаются доступность, целостность или конфиденциальность системы. Также необходимо определить масштабность оценки.

Персонал, ознакомленный с работой IACS, должен проанализировать уровень предварительного отбора. Обычно персонал IACS и IT применяет знания в отношении используемых устройств и систем, в то время как эксплуатационный персонал владеет знаниями в отношении последствий инцидента, связанного с обеспечением безопасности. Чтобы выполнить оценку предварительного отбора, необходима совместная работа этих специалистов.

Группа разрабатывает укрупненную шкалу для количественной оценки общего риска, связанного с каждой системой. Шкала должна быть простой (высокий, средний и низкий уровень или от 1 до 10) и определять критерии для каждой отметки на шкале риска.

Группа принимает решение об уровне риска, связанного с каждой системой после изучения последствия для финансовой сферы и HSE в случае, если такому риску подвергаются доступность, целостность или конфиденциальность системы. Группа должна регистрировать проведение укрупненного анализа для логической системы в инвентарном списке, разработанном ранее. Благодаря определению уровней допустимости риска становится возможным определять приоритеты фактических объектов в среде IACS.

Результаты такой предварительной оценки являются важными входными данными для принятия решения о проведении детальной оценки уязвимости конкретной IACS. Планирование полной оценки уязвимости проводится, если:

- установлено, что IACS в данный момент соединена с корпоративной сетью или внешними сетями (например, Интернет, модемы). После проведения детальной оценки риска можно будет лучше понять уязвимости и соответствующую стратегию снижения рисков;
- установлено, что поддержка системы в данный момент осуществляется дистанционно;
- ожидается, что любой из двух вышеупомянутых критериев будет выполнен в ближайшем будущем. В таком случае оценку уязвимости необходимо провести до принятия действий, приводящих к созданию такой опасной ситуации.

А.2.3.3.8.6 Определение приоритетов систем

В А.2.3.3.8.5 предлагалось присваивать рейтинг уязвимости/риска для каждой идентифицированной логической системы IACS. Процесс расстановки вполне можно начинать с такой оценочной шкалы. Однако, принимая решение о том, с чего необходимо начинать детальный анализ, важно учитывать несколько дополнительных моментов, например:

- риск для компании (например, для финансовой сферы или HSE);
- области, в которых процесс оценки может быть наиболее успешным;
- стоимость потенциально необходимых контрмер;
- сравнение капитальных и некапитальных издержек;
- наличие квалифицированного вспомогательного персонала для работы с конкретной системой;
- географический регион;
- директивы или конфиденциальные данные торговой организации-участника;
- государственные или локальные политические требования;
- внешний или собственный вспомогательный персонал;
- поддержка сайта для проведения работы;
- история известных проблем с обеспечением информационной безопасности.

Не существует правильного или неправильного подхода. Значения будут отличаться для каждой компании. Важно применять одинаковые принципы определения приоритетов для всех площадок. Необходимо вести записи присвоенных приоритетов и соответствующих оснований.

А.2.3.3.8.7 Определение уязвимостей и приоритетов рисков

Следующим этапом в процессе оценки риска является собственно детальная оценка риска для приоритетных систем. В большинстве методик реализуется подход, при котором систему разбивают на мелкие компоненты и анализируют риски, связанные с такими мелкими компонентами, из которых формируется вся система.

При детальной оценке риска физические угрозы и угрозы для информационной безопасности, внутренние и внешние угрозы, а также аппаратное и ПО и данные необходимо рассматривать в качестве источников для возникновения уязвимостей.

Обязательным условием является то, что группа специалистов должна применять комплексный подход к оценке. В состав группы должен входить, как минимум, один руководитель по управлению работами на площадке, специалист по IACS, IT-специалист и специалист по сетям. К другим членам группы относятся специалисты в области физической безопасности, безопасности информационных систем, вопросов права, бизнеса (операционная деятельность, техобслуживание, инжиниринг и т. д.), человеческих ресурсов, HSE и поставщиков аппаратного обеспечения. Такие специалисты лучше всего справятся с задачей идентификации уязвимостей и последствий реализации рисков, относящихся к их компетенции.

Несмотря на то, что работа ведется в целях определения угроз и последствий, связанных с конкретной системой, с большой долей вероятности можно утверждать, что главной задачей является получение возможности сравнивать результаты оценки одной системы/площадки с другой внутри организации. Такая способность будет зависеть от того, насколько последовательно применяется методика. К проверенным методам относятся:

- использование ведущего лица для руководства работами на каждой площадке;
- использование небольшой группы специалистов, которые работали вместе над другими проектами, для управления работами по проведению анализа с учетом географических особенностей, хозяйственного подразделения и т. п. факторов;
- использование качественных учебных материалов с описанием процедур и упражнений для подготовки группы профессионалов, которые будут проводить оценку на каждой площадке;
- использование обычной формы или базы данных для регистрации результатов анализа;
- централизованный анализ всех результатов, позволяющий понять, насколько результаты реалистичны и сопоставимы с похожими системами.

При проведении анализа важно учитывать все аспекты IACS, включая непреднамеренные изменения в конфигурации системы, возникшие в результате проведения ремонтных работ, временного подсоединения поставщика к системе для ее наладки, или даже незначительные изменения в проекте поставщика, из-за которых могут появиться новые уязвимости, реализуемые через запасные части или обновления, которые необходимо принимать во внимание и/или проверять таким же способом, что и оригинальные компоненты системы.

Оценка должна быть направлена на системы, сопряженные с IACS, и должна гарантировать, что они не будут подвергать риску безопасность IACS и наоборот. В качестве примера можно привести системы, которые обеспечивают возможности онлайн-разработки, и системы регулирования среды и силовые системы, из-за которых могут появиться недопустимые риски.

В некоторых случаях ответственность за появление уязвимости лежит на поставщике. Для гарантии качества от поставщика и контроля на этапе проектирования может потребоваться проведение оценки уязвимости. Это особенно важно при заказе запасных частей или обновлений.

На этом этапе процесса оценки необходимо провести детальную проверку сети с физической и эксплуатационной точки зрения, чтобы можно было обнаружить соединения, не показанные на первоначальных простых сетевых схемах. После проведения нескольких оценок такие соединения будут обнаружены.

Приведенные ниже потенциальные источники уязвимостей, связанных с возможностями сетевого соединения, ранее были определены как слабые места в определенных системах и должны быть идентифицированы и проверены:

- точки беспроводного доступа, особенно в случае применения плохо защищенных технологий, например, ранние версии IEEE 802.11;
- модемные соединения, особенно без посылки обратного вызова и не предусматривающие шифрование;
- ПО для дистанционного доступа (например, pcAnywhere®[1)] и Timbuktu®), обычно применяющиеся для доступа специалистов внутри организации или за ее пределами для поддержки систем или операций. Такие приложения обеспечивают достаточный контроль и доступ к конфигурированию для неавторизованного лица;
- технологии дистанционной работы с окнами, например X Windows®;
- внутренние сетевые соединения;
- соединения Интернет;
- телеметрические сети;
- любые сетевые подключения к системе, не являющиеся непосредственным компонентом IACS;
- любые сетевые соединения, используемые для сопряжения компонентов SCADA или системы управления, которые не являются частью специальной физически защищенной сети IACS. Другими словами, любая сеть, выходящая за рамки одной зоны безопасности или проходящая через незащищенные зоны или используемая и для IACS, и других функций одновременно. В состав оборудования, включенного в сетевые соединения, входит радиотелеметрия и внешние сервисы, например, ретрансляция кадров, применяемая для связи между географически разделенными участками.

Большое число промышленных источников обеспечивают безопасность системы управления и содержат списки стандартных уязвимостей, которые можно обнаружить в ходе детальной оценки уязвимости (см. [27] и [29]).

Конечным результатом работы группы является список уязвимостей, расставленных в порядке приоритета с учетом их влияния на риск. После идентификации уязвимостей группа связывает их с угрозами, последствиями и прочими вероятными результатами реализации угрозы и уязвимости. В таком анализе учитывается потенциальное снижение риска после принятия мер физической безопасности. Уязвимости, которые приводят к наибольшим рискам, обычно не представляют сложности. Чтобы завершить процесс оценки уязвимости, методика группы должна включать в себя согласованный метод определения приоритетов уязвимостей, связанных с рисками среднего и низкого уровня.

Результаты детальной оценки рисков оформляются документально, после чего должны быть приняты меры на основе соответствующих рекомендаций (см. А.3.4.2).

Документы с детальным описанием уязвимостей, обнаруженных в ходе детального анализа риска, как правило, включают в себя (в отношении каждой обнаруженной уязвимости) дату анализа, идентификацию включенных объектов, описание уязвимости, фамилию лица, которое вело наблюдения, средства или методы, использованные в процессе. Кроме обнаруженных уязвимостей в такой документации должны быть указаны уязвимости проверенные, но не найденные, а также способ проверки для каждого объекта анализа. Это допускается оформить в виде простого контрольного листа. Документы с описанием уязвимостей являются полезным средством, когда вносятся изменения в оценку риска и возникают определенные вопросы в отношении объектов. Предыдущие контрольные списки и результаты формируют основу для усовершенствования процедур оценки уязвимости в будущем и обеспечения соответствия внутри организации. Организация должна принимать их именно в таком значении, а не рассматривать в качестве статичного определения компонентов такой оценки.

Задачи и документы, связанные с процедурами укрупненного и детального анализа, описанными в настоящем подпункте, и процессом управления рисками в соответствии с А.3.4.2, могут быть объединены в целях эффективности, что позволит выполнить требования определенной организации.

Результаты детальной оценки риска должны периодически обновляться и подвергаться повторной проверке. Кроме того, поскольку детальная оценка риска может устаревать из-за изменений в среде системы управления, в управление программой изменений должны встраиваться триггеры для обновления процедуры оценки риска. Это

[1)] pcAnywhere®, Timbuktu® и X Windows® — это примеры подходящих продуктов, имеющихся на рынке. Данная информация приводится для удобства пользователей настоящего стандарта и не является одобрением таких продуктов со стороны ISA.

очень важный момент, т. к. для большинства организаций легче установить основу для обеспечения информационной безопасности, чем поддерживать ее в надлежащем состоянии на протяжении времени (см. А.4.3).

А.2.3.3.8.8 Типичные ошибки, которые необходимо исключать

В ходе оценки необходимо исключать типичные ошибки, из-за которых процесс оценки может пойти неправильно, предпринимая следующие действия:

a) Разработка решения в ходе оценки

Оценку проводят с целью определения имеющихся рисков, а не для разработки решения, когда группа действует в качестве команды. На решение проблемы и обсуждение преимуществ одного подхода перед другим при оценке одного конкретного объекта может быть потрачено много времени. Усилия необходимо сконцентрировать на понимании рисков и последствий, существующих в данный момент времени или которые могут наступить в обозримом будущем, например, в проекте, находящемся на стадии реализации, в который требуется добавить новое устройство с сетевым интерфейсом;

b) Преуменьшение или преувеличение размера последствия

Необходимо обеспечить качественный подход к оценке последствий инцидента, влияющего на конкретное оборудование, программы или информационный объект. Нельзя допускать преуменьшения размера последствия, из-за чего могут не быть приняты надлежащие меры по снижению рисков. То, что может иметь большое значение для одного конкретного лица, поскольку это напрямую влияет на выполняемую им работу, может совершенно иначе отразиться для организации в целом;

c) Неспособность достичь согласия в отношении результатов оценки риска

Достижение согласия по вопросам риска и последствий имеет крайне важное значение. Если группа не имеет единого понимания риска и важности, достичь согласия о контрмерах будет намного сложнее;

d) Оценка системы без учета результатов оценки других аналогичных систем

Важно оценить, насколько последовательными являются результаты и как они согласуются с результатами, полученными в ходе аналогичных оценок процессов на других площадках. Выводы, сделанные на основе предыдущих аналогичных оценок, и обнаруженные уязвимости могут пригодиться в ходе анализа рассматриваемой системы.

А.2.3.3.8.9 Взаимосвязь с мерами обеспечения физической безопасности

Информационная и физическая безопасность могут быть тесно связаны. В некоторых ситуациях они могут функционировать в качестве независимых уровней защиты, в других ситуациях сильно зависеть друг от друга. Утрата одной из систем может означать потерю обоих уровней защиты. В ходе детальной оценки рисков для системы необходимо учитывать их потенциальное взаимодействие и то, к каким последствиям это может привести.

В некоторых отраслях обычной практикой является использование SIS помимо IACS. Если SIS работает на основе реле, вероятность ее поражения в результате кибератаки, влияющей на IACS, невелика. Можно рассчитывать, что SIS выполнит свою защитную функцию, а последствия кибератаки можно будет ограничить и смягчить. Однако, если работа SIS основана на электронике и привязана к той же сети, что и IACS (некоторые отрасли не рекомендуют применять такую практику), вероятность того, что в результате киберинцидента пострадают обе системы, возрастает и последствия могут быть намного серьезнее.

Другим примером является система доступа к закрытому компьютерному залу по идентификационному жетону. При нормальных обстоятельствах система контроля доступа обеспечивает дополнительную защиту для систем управления.

Однако если сеть будете переполнена атаками типа «отказ от обслуживания», система контроля доступа к двери может не сработать, и у оператора не будет возможности пройти к пульту управления в компьютерном зале. Аналогичным образом на работу пульта управления повлияет перегрузка сети атаками DoS. В таком случае один киберинцидент будет служить двойным препятствием для реагирования на действия устройства управления и может привести к тому, что последствия станут еще серьезнее.

В итоге, методики оценки риска для информационной безопасности необходимо включать в состав методик оценки физических рисков и рисков на площадке.

А.2.3.3.8.10 Оценка риска и жизненный цикл IACS

В А.2.3.3.7 описано, каким образом можно проводить оценку риска в отношении действующих IACS, когда сначала создается и затем периодически применяется CSMS. Оценка риска является наиболее эффективной и менее разрушительной, когда она проводится аналогичным образом на различных этапах жизненного цикла IACS до того, как система запускается в режиме производства:

a) Во время разработки новой или обновленной IACS

Кибер-риск необходимо учитывать заранее, до того как будет внедряться новая или модифицированная IACS, т. к. опыт указывает на то, что всегда будет легче и менее затратно учитывать функцию безопасности на этапе проектирования, чем добавлять ее впоследствии. Процесс укрупненного анализа риска для будущей системы проходит таким же образом, что и для существующей системы. Наилучшие результаты достигаются, когда оценка проводится одновременно с высокоуровневым проектированием, после чего они изучаются в комплексе. Детальную оценку риска также можно выполнять параллельно с детальным проектированием, хотя идентифицированные уязвимости являются гипотетическими и не во всех случаях будут такими специфическими, как для уже внедренной системы. В таком случае оценка риска на этапе разработки позволит определить, какие контрмеры должны

применяться наряду с требуемыми изменениями IACS, чтобы после внедрения можно было избежать большого числа непредвиденных моментов;

b) Во время внедрения новой или обновленной IACS

Даже если на этапе разработки вопросам риска уделяется должное внимание, во время внедрения могут появиться непредвиденные уязвимости. В лучшем случае часть процесса акцептации новой или обновленной IACS включает в себя не только тестирование, но и детальный анализ уязвимостей, как говорилось выше. Поэтому может потребоваться, чтобы организация приняла решение о включении новой или обновленной системы до внесения исправления для недавно обнаруженной уязвимости;

c) Во время выведения IACS из работы

Решение о выведении из работы или сохранении IACS или компонентов IACS зависит от многих факторов, включая затраты, потребность в новой функциональности или возможности, постоянной надежности и доступности технической поддержки поставщика. Влияние на информационную безопасность также является фактором, который необходимо принимать во внимание. Новые компоненты и архитектуры могут улучшить функциональность и/или привести к появлению новых уязвимостей, проблему которых необходимо будет устранять. Поэтому в ходе оценки кибер-риска, при которой проводится анализ необходимости выведения из работы, также рассматривается сценарий, при котором проводится замена старой системы и сценарий, при котором старая система сохраняется на определенный период времени.

Изменения в укрупненный и детальный анализ рисков после вывода IACS из работы вносятся по двум причинам:

1) удаление IACS может повлиять на уязвимость части IACS, оставшейся в работе;

2) если IACS заменена на новую систему, могут появиться новые уязвимости, о чем говорилось ранее.

В качестве примера можно привести возможность сетевого подключения к IACS, оставшейся в работе. Всегда сохраняется возможность такого сетевого подключения через удаляемую IACS. Это означает, что новое решение сетевого подключения вводится для оставшейся IACS и такую конфигурацию необходимо проанализировать на предмет наличия уязвимостей и связанных рисков.

A.2.3.4 Вспомогательные практические методы

A.2.3.4.1 Основные практические методы

К основным практическим методам относятся следующие действия:

a) определение критерия для идентификации устройств, составляющих IACS;

b) определение устройств, поддерживающих важнейшие бизнес-процессы и операции IACS, включая системы IT, поддерживающие такие бизнес-процессы и операции IACS;

c) классификация логических объектов и компонентов с учетом доступности, целостности и конфиденциальности, а также влияния на сферу HSE;

d) определение приоритетов действий по оценке рисков с учетом последствий (например, промышленным операциям, для которых характерны большие риски, присваивается высокий приоритет);

e) определение границ системы для последующего анализа, идентификация всех объектов и важнейших компонентов;

f) разработка сетевой схемы IACS (см. A.2.3.3.8.4);

g) понимание того, риски, допустимость рисков и приемлемость контрмер могут отличаться в зависимости от географического региона или особенности подразделения;

h) ведение актуальных записей всех устройств, составляющих IACS, для последующих оценок;

i) проведение оценки риска на всех этапах жизненного цикла технологии (разработка, внедрение, обновление и вывод из работы);

j) определение частоты проведения повторной оценки или критериев для ее проведения в зависимости от технологии, организации или изменений в промышленной операции.

A.2.3.4.2 Дополнительные практические методы

К дополнительным практическим методам относятся следующие действия:

a) определение и классификация объектов, которые помогают идентифицировать риски для компании. Важное значение имеют люди, принимающие участие в процессе, и используемые технологии. Создание контрольного списка поможет группировать объекты по категориям (см. A.2.3.3.8.3);

b) классифицирование отдельных объектов с учетом сложностей, связанных с доступностью, целостностью и конфиденциальностью. Для каждой категории объекта предусмотрены различные уровни классификации:

Пример — Классификация для конкретного типа данных:

- доступность: низкая — для системы не требуется постоянная работа. Система не является частью опасной операции. Отставание на один или два дня допускается;

- целостность: средняя — проверка данных осуществляется на различных этапах, изменения будут обнаружены;

- конфиденциальность: очень высокая — поддерживается высочайший уровень конфиденциальности данных, имеющих важнейшее значение для бизнеса;

c) определение вероятности (т. е. возможности или примерной частотности) того, что конкретная угроза реализуется успешно с учетом действующего уровня контроля. Важно принимать во внимание и другие стандартные

средства контроля, используемые в производстве/операционной деятельности, которые могут дополнять средства контроля информационной безопасности и снижать вероятность последствия. К ним относятся независимые SIS и прочие технологии PSM, например, пассивные, вспомогательные, независимые резервные устройства. Примерная частотность напрямую связана с общей уязвимостью и угрозами и может быть выражена в количественном виде (в процентах) или более субъективным образом: по уровням — высокий, средний или низкий;

d) определение последствий или влияния успешно реализованной угрозы с учетом бизнеса или оценки риска для IACS.

A.2.3.5 Использованные ресурсы

Данный элемент частично основан на материалах [24], [26], [27], [28], [29], [30], [33], [42].

A.3 Категория «Устранение риска при помощи системы управления кибербезопасностью»

A.3.1 Описание категории

Вторая главная категория CSMS называется «Устранение риска при помощи CSMS». В этой категории раскрывается большое количество требований и информации, содержащейся в CSMS. Категория делится на следующие группы элементов:

- политика безопасности, организация и осознание необходимости;
- избранные контрмеры обеспечения безопасности;
- внедрение.

A.3.2 Группа элементов «Политика безопасности, организация и информированность»

A.3.2.1 Описание группы элементов

В первой группе элементов этой категории описывается разработка базовых политик информационной безопасности, организации, ответственные за обеспечение информационной безопасности и информированность о решении этих вопросов внутри организации. На рисунке A.6 графически представлены элементы, формирующие группу элементов:

- сфера применения CSMS;
- организация безопасности;
- обучение персонала и информированность;
- план бизнес-непрерывности;
- политики и процедуры безопасности.

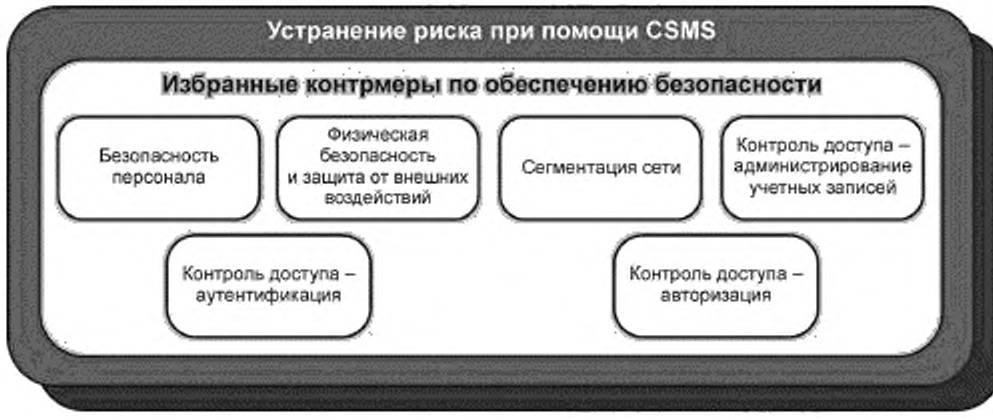


Рисунок A.6 — Графическое представление группы элементов «Политика безопасности, организация и осознание необходимости»

A.3.2.2 Элемент «Сфера применения CSMS»

A.3.2.2.1 Описание элемента

Когда имеется готовое экономическое обоснование и поддержка руководства, следующим шагом будет разработка формальной сферы применения или концепции. Сфера применения должна устанавливать задачи, которые должны быть выполнены (на экономическом уровне), и сроки их выполнения. Она определяет конкретную область, на которую необходимо направлять усилия.

Заявление о сфере применения должно исходить от ответственного исполнителя из состава высшего руководства или управленческой группы, которая будет отвечать за руководство группой на протяжении разработки программы. В конечном итоге, ответственный исполнитель должен будет обеспечивать выполнение программы, включая обмен информацией, финансирование, обеспечение выполнения задач и аудит.

CSMS должна охватывать все деловые подразделения и все географические регионы, в которых присутствует организация. Если для данной работы изначально невозможно заручиться поддержкой руководства, необходимо определить меньший объем работ и использовать это в качестве возможности для построения надежности и демонстрации ценности CSMS.

A.3.2.2.2 Разработка сферы применения CSMS

Руководство должно определить границы, в пределах которых CSMS применяется к организации, а также установить направленность и сферу применения CSMS. Разработка четко определенной области действия позволит руководству достичь своих целей в области CSMS.

Сфера действия должна включать в себя все аспекты IACS, точки интеграции с бизнес-партнерами, заказчиками и поставщиками. Для того, чтобы запустить и контролировать процесс внедрения и продолжающиеся операции в области информационной безопасности внутри компании, необходимо определить основу управления (например, организация).

Значение организации, отвечающей за определение и информирование о корпоративных политиках, связанных с информационной безопасностью, заключается в защите корпоративных объектов с точки зрения кибербезопасности. Компании должны понимать, что в современном деловом мире, использующем Интернет, возможность электронного информационного сообщения является неотъемлемой частью деловой деятельности, и поэтому информационная безопасность имеет большое значение. Коммерческие операции не только остаются в пределах брандмауэра организации, но при этом доступ получают заказчики, поставщики, сторонние организации и партнеры по аутсорсингу.

Общий объем работ должен быть определен с точки зрения трех различных аспектов: коммерческий, архитектурный и функциональный.

С коммерческой точки зрения сфера применения должна давать представление об ответах на следующие вопросы:

- какие корпорации включаются;
- какие подразделения включаются;
- какие географические регионы включаются;
- какие специфические площадки включаются.

С точки зрения архитектуры сфера применения должна давать представление об ответах на следующие вопросы:

- на какие компьютерные системы и сети будут направлены действия;
- будут ли включены SCADA и системы мониторинга;
- будут ли включены компьютерные системы, не связанные с производством (и с поддержкой IT-организации, и без нее), и в производство;
- будут ли включены системы АСУТП (MES);
- будут ли включены системы управления работой горелок и SIS;
- будут ли включены робототехнические системы;
- будут ли включены соединения с поставщиками или заказчиками.

С функциональной точки зрения сферу применения можно разделить на следующие две категории:

a) Работа по прямому управлению рисками

Такие работы включают в себя оценку, доведение до сведения и определение приоритета риска. К примерам можно отнести определение локальных владельцев системы информационной безопасности, сбор данных и ведение инвентарного списка объектов, разработку и сохранение сетевой архитектуры, проведение внешних и внутренних аудитов и передачу соответствующих результатов внутри подразделения или корпорации;

b) Проекты, связанные с управлением рисками

В основе таких работ лежат действия по снижению рисков, идентифицированных в ходе управления рисками. Такие косвенные решения по управлению рисками могут быть реализованы в форме проектов, ограниченных по времени, а также в форме разработки и внедрения действующих услуг.

При определении функциональной сферы необходимо учитывать следующие вопросы:

- каким образом такая сфера применения связана с существующими системами управления рисками;
- каким образом такая сфера применения связана политиками обеспечения информационной безопасности, уже применяемыми к таким системам и организациям;
- каким образом такая сфера применения связана с техническими стандартами и процедурами, уже применяемыми в отношении специфических архитектурных компонентов (т. е. базовые системы технологического контроля, системы SCADA, SIS, системы управления работой горелок и робототехнические системы);
- каким образом такая сфера применения связана с уже профинансированными проектами;
- каким образом такая сфера применения связана с существующими сервисами.

Поддержка руководства служит толчком для действий со стороны менеджеров, отвечающих за назначение ресурсов для управления и реализации задач по снижению рисков IACS.

Определение сферы применения должно быть выполнено ответственным исполнителем из состава высшего руководства, который будет отвечать за руководство группой на протяжении разработки программы. В конечном итоге ответственный исполнитель должен будет обеспечивать выполнение программы, включая обмен информацией, финансирование, обеспечение выполнение задач и аудит.

При наличии поддержки и участия высшего руководства необходимо идентифицировать заинтересованные лица и выделить им время для улучшения работы системы безопасности. Заинтересованные лица несут ответственность за продвижение и реализацию инициативы в области безопасности. Имея поддержку высшего руководства, заинтересованные лица предпринимают следующие шаги и привлекают свои ресурсы для выполнения задач. Необходимо сформировать интегрированную группу, которая включает в себя традиционные камеральные и экономические вычислительные системы, IACS и системы, взаимодействующие с заказчиками, поставщиками и организациями, обеспечивающими транспортировку. Концепция и сфера применения, о которых говорилось выше, помогают понять, кого нужно привлекать к данному процессу, чтобы достичь цели инициативы.

Высшее руководство может назначить руководителя проекта, чья работа будет заключаться в объединении нужных людей для выполнения задач безопасности. Такой человек должен иметь широкое представление о действующем состоянии процедур информационной безопасности в компании. Допуская, что целью является улучшение политики и процедур кибербезопасности для IACS, руководитель проекта должен определить области, которые могут пострадать в результате инцидентов, связанных с безопасностью IACS, и назначить ключевых специалистов, отвечающих за такие области. Основной задачей должно быть определение специалистов, действующих в нужных ролях, независимо от организации, к которой они относятся.

Особо следует отметить, что при различных организационных структурах такие специалисты могут работать в различных организациях. Необходимо разрабатывать экономичную CSMS, сопоставимую с существующими бизнес-процессами и организациями, а не создавать полностью новую организацию. По возможности должны отбираться люди, уже выполняющие правильные задачи и имеющие надлежащий опыт. Разделение подконтрольных вопросов может стать важным заданием такой группы заинтересованных лиц.

Ключевая группа заинтересованных лиц должна быть многофункциональной по своему характеру и объединять в себе квалификации, которыми один отдельный специалист обычно не обладает. Группа должна включать в себя следующих специалистов:

- лицо(а) IACS, которые могут внедрять и обслуживать устройства IACS;
- операционный персонал, отвечающий за создание продукта и выполнение заказов;
- лицо(а), занимающееся управлением технологической безопасностью, в чьи задачи входит обеспечение отсутствия инцидентов в сфере HSE;
- IT-специалист(ы), который(е) может отвечать за проектирование и эксплуатацию сети, обслуживание пультов управления и серверов и т. п.;
- специалист(ы) по безопасности, связанный с физической и информационной безопасностью на площадке;
- дополнительные кадровые ресурсы, которые могут включать специалистов по правовым, кадровым вопросам и по вопросам поддержки клиентов или выполнения заказов.

С течением времени состав группы заинтересованных лиц может изменяться, или же отдельные лица могут переходить на выполнение функции более высокого уровня на различных этапах или во время выполнения различных действий при разработке CSMS. Не имеет значение, какая организация руководит данной работой, скорее имеет значение то, что руководитель демонстрирует правильные основополагающие принципы, способствующие совместной работе в качестве группы, стремящейся к одной цели. У каждой из исходных компаний, к которым относятся указанные выше специалисты, есть что предложить, и каждая из них играет свою роль при принятии решений и выведении результатов в отношении CSMS.

A.3.2.2.3 Предлагаемые практические методы

A.3.2.2.3.1 Основные практические методы

К основным практическим методам относятся следующих действия:

a) описание организации(й), отвечающей(их) за создание, доведение до сведения и контроль системы информационной безопасности внутри компании;

b) определение области действия CSMS, в том числе:

- информационные системы — включая все операционные системы, базы данных, приложения, совместные предприятия и деятельность сторонних организаций;
- IACS — включая все системы технологического контроля, системы SCADA, PLC, рабочие станции конфигурирования и заводские или лабораторные информационные системы и для данных, поступающих в режиме реального времени, и для исторических данных;
- сети, LANs, WANs — включая аппаратное обеспечение, приложения, файерволлы, системы обнаружения вторжений и т. п.;
- точки интеграции с организациями, предоставляющими техническую поддержку или услуги;
- обязанности пользователя — включая политики, направленные на аутентификацию и возможность проведения аудитов;
- защита информации — включая требования к доступу и подотчетность лиц с правом доступа;
- управление рисками — включая процессы идентификации и снижения рисков и остаточных рисков, связанных с документами;
- восстановление после чрезвычайных происшествий — включая идентификацию важнейшего программного обеспечения/услуг;
- требования к обучению;
- соответствие и аудит;

- идентификация объектов;

c) характеристика организации, отвечающей за CSMS, включая:

- организационную структуру;
- местоположение;
- бюджет;
- роли и обязанности, связанные с процессами CSMS.

А.3.2.2.3.2 Дополнительные практические методы

К дополнительным практическим методам относятся следующие действия:

a) получение от руководства подтверждения сферы применения и задач CSMS;

b) четкое понимание ролей и обязанностей организации(й), ответственных за аспекты CSMS;

c) документальное оформление информации о сфере действия CSMS с отдельными положениями, в которых рассматриваются специфические компоненты;

d) учет коммерческих, правовых (например, секретность данных) и регулятивных требований и обязанностей;

e) идентификация и документальное оформление зависимости безопасности процесса от информационной безопасности, а также практик и процедур обеспечения физической безопасности, включая основу организационного взаимодействия.

А.3.2.2.4 Использованные ресурсы

Данный элемент частично основан на материалах [24], [26].

А.3.2.3 Элемент «Организация безопасности»

А.3.2.3.1 Описание элемента

Компании должны определить организацию, структуру или группу людей, отвечающих за безопасность в целом, принимая во внимание, что необходимо учитывать как физические, так и информационные компоненты.

Важно установить индивидуальную ответственность с тем, чтобы можно было управлять и контролировать работу по обеспечению информационной безопасности организации. Информационная безопасность в самом широком понимании охватывает не только данные, но и системы (аппаратное и ПО) для генерации или хранения такой информации, и включает в себя элементы физической безопасности. IACS, партнеры по стоимостной цепочке, сторонние подрядчики, партнеры по совместному предприятию (СП), партнеры по аутсорсингу и специалисты в области физической безопасности должны рассматриваться организацией как часть общей структуры безопасности и, соответственно, включаться в объем ответственности.

А.3.2.3.2 Построение организационной основы безопасности

Ответственность за реализацию программы безопасности начинается с верхнего уровня организации. Руководство должно продемонстрировать четкую заинтересовать в обеспечении информационной безопасности. Информационная безопасность — это ответственность, которую делят все участники предприятия и особенно руководители, возглавляющие группы по управлению бизнесом, производством IT и рисками. Программы обеспечения информационной безопасности с ощутимой поддержкой высшего руководства и участием руководителей организации с большей долей вероятности будут отвечать заявленным требованиям, функционировать более эффективно и быстрее дадут положительные результаты.

Для начала и контроля внедрения общей системы безопасности необходимо определить основу управления. Сфера применения и задачи информационной безопасности для организаций должны включать в себя физическую безопасность и информационную безопасность для IT-систем, поставщиков IACS, сторонних подрядчиков, партнеров по аутсорсингу и компонентов стоимостной цепочки организации. Общая система безопасности должна быть расширена таким образом, чтобы распространяться также и на деятельность СП.

Организации должны определить основу управления для одобрения политики информационной безопасности, присвоения ролей и координирования работы по внедрению информационной безопасности на всех уровнях организации. При такой структуре может потребоваться необходимость решить несколько интересных организационных задач. Структура многих компаний представляет собой трехмерную матрицу, в которой одно измерение представлено направлением деятельности, второе измерение — функцией или дисциплиной, а третье — географическим регионом. Как правило, отдельные менеджеры обладают кругом обязанностей в отношении части или всей такой структуры. Поскольку система настолько же надежна, как и ее самое слабое звено, в конечном итоге потребуется развивать систему информационной безопасности таким образом, чтобы она охватывала всю географию деятельности организации.

Вопрос информационной безопасности затрагивает большое количество различных рисков, которые в целом можно классифицировать на проблемы, связанные с доступностью, целостностью или конфиденциальностью. Проблемы доступности, как правило, решаются при помощи программы планирования бизнес-непрерывности или программой обеспечения сетевой безопасности. Проблемы целостности в контексте производственного процесса обычно решаются программой обеспечения безопасности технологического процесса или обеспечения качества. Проблемы конфиденциальности обычно решаются с помощью программы информационной безопасности. Поскольку информационная безопасность затрагивает так много различных областей риска, что возможно, что ни один менеджер, действующий индивидуально, не будет иметь необходимый объем ответственности для утверждения программы информационной безопасности для всех IACS. В будущем часто придется собирать и убеждать небольшую группу старших менеджеров, которые, вполне вероятно, до этого никогда настолько плотно друг с другом не работали, когда требовалось принять согласованное решение.

Все предприятие (например, корпорация) или отдельные подорганизации могут работать над достижением целей настоящего стандарта. Если работа ведется всем предприятием, оценка рисков проводится на всех уровнях предприятия. В таком случае, например, отдельные заводы, входящие в состав корпорации, могут проводить оценки рисков, но при этом будут применять общую методику оценки рисков, позволяющую сводить эти оценки воедино на корпоративном уровне. Таким образом, если все предприятие ставит целью достижение соответствия, для этого понадобится задать соответствующие основные направления, даже если отдельные подорганизации, например, заводы, делают большую часть работы.

В других ситуациях само предприятие не стремится выполнять требования стандарта, но требует от своих подорганизаций на определенном уровне в индивидуальном порядке добиться соответствия, или некоторые подорганизации работают над достижением соответствия по собственной инициативе. При любом раскладе предприятию потребуется оказывать содействие своим подорганизациям в процессе выполнения определенных требований стандарта, работа с которыми ведется на уровне предприятия, например, обеспечивать защиту корпоративной архитектуры, отбор сотрудников и формулирование текстов договоров с поставщиками услуг. В соответствии с такими сценариями на отдельной площадке завода может применяться собственная методика оценки рисков, могут определяться собственные приоритеты мер по снижению рисков и может быть поддержка руководства на уровне завода в проведении подобной работы. В этих случаях предприятие не проводит оценку своего общего соответствия требованиям стандарта, хотя потенциально может оценивать степень соответствия у отдельных заводов. Такая стратегия имеет наибольший смысл, когда она реализуется в диверсифицированной корпорации или на ином предприятии с высоким уровнем децентрализации.

A.3.2.3.3 Начало работы и получение поддержки

Чтобы старшие менеджеры могли оказывать эффективную поддержку программы обеспечения информационной безопасности, их необходимо убедить в том, что затраты по программе, которые они будут оплачивать из своих бюджетов, будут меньше последствий угрозы, реализовавшейся в их сферах ответственности. Может потребоваться разработка экономического обоснования для управления кибер-рисками, чтобы убедить руководство в необходимости поддержки программы. Руководителям старшего звена потребуется разъяснить бюджетные обязанности и объем ответственности.

Из-за ограниченности по времени многие старшие менеджеры прибегают к помощи консультантов, помогающих им отделять важные вопросы от вопросов, которыми должны заниматься другие люди. Таких людей называют консультантами безопасности. В крупных организациях часто присутствуют организации управленческого аппарата, которые старшие менеджеры используют для составления рекомендаций для решения технически сложных вопросов. Возможно, работу с такими организациями потребуется вести с самого начала в целях сбора достаточных данных, на основании которых будут разрабатываться бизнес-модели. Такие организации могут дать представление о том, какие старшие менеджеры обычно ведут работу со специфическими рисками.

Вполне вероятно, что высшее руководство может выбрать руководителя проекта, в задачи которого будет входить подбор необходимых специалистов для проведения работы по обеспечению безопасности. Такой человек должен иметь широкое представление о действующем состоянии процедур информационной безопасности в компании. Важно понимать, что по-настоящему интегрированная CSMS включает в себя традиционные камеральные и коммерческие компьютерные системы, IACS и системы создания ценности, которые взаимодействуют с заказчиками, поставщиками и организациями, оказывающими услуги по транспортировке. Концепция и сфера применения, о которых говорилось ранее, позволяют понять, кто должен быть привлечен к работе для достижения целей инициативы.

Руководитель проекта должен определить области, которые могут пострадать в результате инцидентов в отношении информационной безопасности IACS, и ключевых специалистов, которые несут ответственность за такие области. Особое внимание следует уделять распределению ролей между специалистами независимо от организации, в которой они работают.

Важно отметить, что при различных организационных структурах такие специалисты могут работать в различных организациях. Целью является разработка экономичной CSMS, сопоставимой с существующими бизнес-процессами и организациями, а не создание полностью новой организации. По возможности, должны отбираться люди, уже выполняющие нужные задачи и имеющие надлежащий опыт. Разделение подконтрольных вопросов может стать важным заданием для такой группы заинтересованных лиц.

Ключевая группа заинтересованных лиц должна быть многофункциональной по своему характеру и объединять в себе квалификации, которыми один отдельный специалист обычно не обладает. Группа должна включать в себя следующих специалистов:

- лицо(а) IACS, которые могут внедрять и обслуживать устройства IACS;
- операционный персонал, отвечающий за создание продукта и выполнение заказов;
- лицо(а), занимающееся управлением технологической безопасностью, в чьи задачи входит обеспечение отсутствия инцидентов в сфере HSE;
- IT-специалист(ы), который может отвечать за проектирование и эксплуатацию сети, обслуживание пультов управления и серверов и т. п.;
- специалист(ы) по безопасности, связанный(е) с физической и информационной безопасностью на площадке;

- дополнительные кадровые ресурсы, которые могут включать специалистов по правовым, кадровым вопросам и по вопросам поддержки клиентов или выполнения заказов.

С течением времени состав группы заинтересованных лиц может изменяться, или же отдельные лица могут переходить на роли более высокого уровня на различных этапах или во время выполнения различных действий при разработке CSMS. Не имеет значения, какая организация руководит данной работой, скорее имеет значение то, что руководитель демонстрирует правильные основополагающие принципы, способствующие совместной работе в качестве группы, стремящейся к единой цели. У каждой из исходных компаний, к которым относятся указанные выше специалисты, есть что предложить, и каждая из них выполняет свою роль при принятии решений и выведении результатов в отношении CSMS.

Как правило, требуется убедить старшего менеджера провести тестирование новых программ в небольшом географическом регионе или на конкретной площадке, чтобы доказать, что новые процедуры/программы работоспособны, прежде чем потратить на это огромное количество ресурсов. Это может стать еще одним эффективным подходом к тому, чтобы получить возможность общения с руководством высшего звена, или же на деле довести до сведения руководителей информацию о бизнес-модели.

Как только будут выбраны соответствующие старшие менеджеры, важно определить, каким образом делать для них презентацию CSMS: в качестве группы или в индивидуальном порядке. Большей эффективности можно добиться, если убеждать их всех одновременно, но они все могут быть не предрасположены к тому, чтобы одновременно участвовать в обсуждениях. Если необходимо убедить группу руководителей, можно попытаться найти «союзника», чтобы тот изучил презентацию, и изложить свои идеи всей группе до презентации. Принимая во внимание большое количество различных областей, подверженных риску, довольно часто приходится убеждать более одной группы руководителей.

Если затраты по программе обеспечения информационной безопасности нельзя определить изначально из-за отсутствия компьютерной инвентарной ведомости или отсутствия стандартных контрмер, может потребоваться провести повторное представление презентаций, когда такие затраты будут определены точнее. На таком раннем этапе следует уделять внимание введению системы для уравнивания затрат, связанных с контрмерами, и с затратами, относимых на счет рисков. В этот период характерно получение неадекватных данных, на основе которых формируется запрос на определенный бюджет для внедрения контрмер.

A.3.2.3.4 Вспомогательные практические методы

A.3.2.3.4.1 Основные практические методы

К основным практическим методам относятся следующие действия:

a) получение поддержки исполнительных руководителей для определения организационной основы решения вопросов безопасности;

b) определение ответственности за информационную и физическую безопасность для персонала с соответствующим уровнем финансирования для внедрения политик безопасности;

c) создание общекорпоративной группы безопасности (или организации), отвечающей за четкое руководство, определение обязательств и контроль. Такая группа может быть неформальной сетевой, организационной или иерархической структурой, под контроль которой подпадают различные подразделения или организации компании. Эта группа назначает уровни ответственности и подтверждает, что внедрены бизнес-процессы, позволяющие защитить объекты компании и информацию;

d) создание или изменение контрактов, в которых рассматриваются вопросы политик и процедур информационной и физической безопасности бизнес-партнеров, сторонних подрядчиков, партнеров по аутсорсингу и т. п., когда такие политики и процедуры безопасности внешних партнеров влияют на безопасность IACS;

e) координирование или интегрирование организации по физической безопасности, когда между рисками для физической и информационной безопасности возникает наложение друг на друга и/или синергия.

A.3.2.3.4.2 Дополнительные практические методы

К дополнительным практическим методам относятся следующие действия:

a) определение ответственности за информационную безопасность IACS:

- отдельное лицо, выполняющее любую функцию, несет ответственность за информационную безопасность всей организации. Такое лицо возглавляет многофункциональную команду, представляющую различные подразделения и функциональные отделы. Группа демонстрирует свою ответственность за обеспечение информационной безопасности и определяет направления деятельности для организации. Это включает в себя участие в объектах и промышленных операциях, а также выделение соответствующих ресурсов для решения вопросов безопасности;

- отдельная группа отвечает за безопасность IACS либо в производственной организации, либо в проектной организации. Несмотря на то, что такой подход имеет свои преимущества благодаря тому, что руководство владеет информацией о рисках, связанных с IACS, они могут быть утрачены, если эта группа не взаимодействует вплотную с людьми, отвечающими за традиционные IT-объекты и физическую безопасность;

- вся группа безопасности отвечает за физические и логические объекты. В данной иерархической структуре безопасностью занимается отдельная организация с отдельными группами, отвечающими за системы физической и информационной безопасности. Такой подход может пригодиться в небольших организациях с ограниченными ресурсами;

b) координирование работы с правоохранительными органами, регулятивными органами и поставщиками интернет-услуг вместе с другими соответствующими организациями, поскольку это связано с угрозами террористи-

ческих атак или иными внешними угрозами. Организации, которые установили отношения с локальными аварийно-спасательными службами, расширяют такие связи с тем, чтобы обеспечивать обмен информацией и реагировать на инциденты, связанные с системой информационной безопасности;

c) обеспечение того, что внешние поставщики, оказывающие влияние на безопасность организации, придерживаются тех же политик и процедур безопасности, за счет чего поддерживается единый уровень безопасности IACS. Политики и процедуры безопасности поставщиков второго и третьего уровня также должны выполнять требования корпоративных политик и процедур безопасности, если они влияют на безопасность IACS:

- компании должны принимать во внимание повышенный риск безопасности, связанный с аутсорсингом, в рамках процедуры принятия решения о том, какие ресурсы следует привлекать по схеме аутсорсинга, и процедуры выбора партнера по аутсорсингу;
- контракты с внешними поставщиками, регулирующие как физический, так и логический доступ;
- ожидания в отношении конфиденциальности информации и права на интеллектуальную собственность должны быть четко определены;
- процедуры управления изменения должны быть четко определены;

d) удаление права доступа внешнего поставщика на этапе заключения/расторжения контракта. Своевременность таких действий имеет крайне важное значение и четко прописывается в контакте.

A.3.2.3.5 Использованные ресурсы

Данный элемент частично основан на материалах [23], [26], [30], [43].

A.3.2.4 Элемент «Обучение персонала и информированность»

A.3.2.4.1 Описание элемента

Информированность о безопасности всеми членами персонала является важным инструментом для снижения рисков информационной безопасности. Информированные и бдительные сотрудники являются одной из наиболее важных линий защиты в обеспечении безопасности системы. При работе с IACS вопросу кибербезопасности необходимо уделять такое же внимание, как и безопасности и эксплуатационной целостности, поскольку последствия могут быть настолько же тяжелыми. Поэтому весь персонал (сотрудники, подрядчики или сторонние организации) должен осознавать важность обеспечения надежной работы системы. Программа обучения персонала и осознания важности обеспечения безопасности позволяет всем сотрудникам (работникам, подрядчикам и т. п.) получать информацию, необходимую для идентификации, изучения, рассмотрения и, по мере необходимости, устранения уязвимостей и угроз для IACS, и гарантировать, что их собственные рабочие практики предусматривают эффективные контрмеры. Весь персонал должен пройти надлежащее техническое обучение, связанное с известными угрозами и уязвимостями аппаратного обеспечения, ПО и объектами социального инжиниринга. Программы обучения персонала и осознания важности обеспечения безопасности наиболее эффективны, если они разработаны с учетом особенностей слушателей, соответствуют требованиям политики компании и на регулярной основе доводятся до сведения персонала. Через программу обучения персонал своевременно получает важную информацию. Эффективная программа позволяет сотрудникам понимать, для чего требуются новые или обновленные средства контроля безопасности, и разрабатывать идеи, которые они смогут использовать для снижения уровней риска и влияния на организацию, если методы контроля не встроены в систему.

A.3.2.4.2 Разработка программы обучения персонала и обеспечение понимания важности

Обучение продолжается практически весь период времени, пока идет разработка и внедрение CSMS. Оно начинается после того, как определен фронт работ и идентифицирована группа заинтересованных лиц. Целью программы обучения является обеспечение всего персонала необходимой информацией, чтобы сотрудники знали о возможных угрозах для системы и их обязанностях по обеспечению надежной работы производственных объектов.

Организация должна разработать программу обучения вопросам информационной безопасности в соответствии с общей программой обучения организации. Обучение должно проводиться в два этапа:

1) общее обучение для всего персонала;

2) обучение с учетом роли специалиста в проекте с упором на определенные обязанности и виды ответственности. Прежде чем приступить к разработке программы обучения, важно определить объем, сроки обучения и роли специалистов внутри организации.

Общая программа обучения должна разрабатываться для всего персонала. Пользователи пройдут обучение правильным процедурам обеспечения безопасности, правильному применению информации для снижения рисков. В программу также необходимо включать такие компоненты, как юридическая ответственность, меры контроля и индивидуальные обязанности по обеспечению безопасности.

В процессе обучения должны рассматривать риски и обязанности, связанные с ролью сотрудника в организации. Для таких сотрудников потребуется более специализированное и интенсивное обучение. Для проведения обучения необходимо привлекать профильных специалистов. Обучение можно проводить в аудитории, в сети Интернет или в форме практического обучения. В рамках такого обучения можно предусматривать обучение, предоставляемое поставщиками, для детального обсуждения инструментария и связанных рисков.

Программа должна включать в себя инструмент для изучения и изменения программы, когда возникает такая необходимость, и инструмент оценки эффективности программы. Также, необходимо установить сроки для проведения периодического повторного обучения.

Обязательство руководства в отношении проведения обучения и обеспечении понимания важности обеспечения безопасности имеет крайне важное значение в создании стабильной и надежной вычислительной среды и

для IT, и для IACS. В частности, что касается среды IACS, надежная и стабильная среда обеспечивает надежную эксплуатацию оборудования и снижение вероятностей инцидентов для сферы HSE. Это достигается за счет ресурсов для разработки и организации обучения, а также предоставления персонала, у которого есть возможность пройти обучение.

После разработки программы обучения по вопросам информационной безопасности организация должна провести соответствующее обучение для всего персонала. Место и время проведения обучения должны выбираться таким образом, чтобы это не сказывалось отрицательным образом на прочих обязанностях обучаемого персонала.

Общее обучение проводится в рамках инструктажа нового сотрудника и в рамках инструктажа по контракту для временного или стороннего персонала. Требуемое обучение должно соответствовать уровню контракта, который будет заключаться с организацией. Может предоставляться специализированное обучение:

a) Обучение заинтересованных лиц

Обучение проводится для группы заинтересованных лиц, а также группы лиц, работающих в среде IACS, которые могут пострадать в конечном итоге. Для группы заинтересованных лиц потребуется специализированное обучение по типам рассматриваемых рисков, сфере применения и концепции, одобренным руководством, любой вспомогательной информации об инцидентах, наступивших в таких системах либо внутри организации, либо в пределах отрасли в целом, а также по типам архитектур и систем, используемым внутри организации. Для обмена такой информацией не обязательно проводить очное обучение. Для этого можно использовать презентации, подготовленные для деловых встреч, собрания по обмену информацией, объявления по электронной почте;

b) Обучение сотрудников в процессе подготовки к новым функциям

Обучение сотрудников будет требоваться по мере того, как они готовятся приступить к исполнению новых функций, либо в рамках системы прямого управления рисками, либо в рамках системы управления рисками, связанными с проектами. На этом этапе практически все участники среды IACS должны изучить определенный объем программы обучения. Некоторые функции, связанные с прямым управлением рисками, будут включать в себя обязанности в случае проведения самооценки или внутренних аудитов;

c) Обучение аудиторов

Потребуется провести обучение для аудиторов, которое позволит им понять особенности систем и сетей, являющихся предметом их аудитов, а также созданные специфические политики;

d) Продолжающееся обучение

Поскольку будут появляться новые сотрудники и посторонний персонал, потребуется регулярно проводить обучение на всех уровнях, вносить изменения, т. к. политики и услуги меняются с течением времени, и нужно будет обеспечивать повышение квалификации, чтобы сотрудники сохраняли свои компетенции в рамках занимаемой роли и выполняемых обязанностей.

Важно подтверждать, что в ходе обучения сотрудники получают представление о своей роли и обязанностях. Аттестация знаний имеет две функции:

1) она помогает понять, насколько хорошо персонал знает программу обеспечения безопасности организации,

2) помогает оценить эффективность программы обучения.

Аттестация проводится различными способами, включая письменное тестирование по вопросам программы обучения, оценку знаний по завершении курса, проверку результатов выполненной работы или документально оформленных изменений в работе по обеспечению безопасности. Способ аттестации должен быть согласован заранее на этапе разработки программы обучения и доведен до сведения персонала.

Ведение и контроль журналов обучения сотрудников и графиков актуализации программы обучения должны осуществляться на постоянной основе. Документирование результатов обучения позволит организации гарантировать, что весь персонал прошел требуемое обучение должностным функциям и обязанностям. Аналогичным образом это поможет определить потребность в дополнительном обучении и выявит необходимость проведения повторного периодического обучения.

С течением времени уязвимости, угрозы и связанные контрмеры изменяются. В результате потребуется вносить изменения в программу обучения. Необходимо периодически (например, ежегодно) проводить анализ программы обучения на предмет ее эффективности, приемлемости, содержания и соответствия используемым в настоящее время инструментам, корпоративным практикам и нормативным актам и по мере необходимости вносить соответствующие изменения. Подписка на услуги оповещения о нарушениях безопасности позволит гарантировать наличие актуальных данных о недавно обнаруженных уязвимостях и угрозах.

A.3.2.4.3 Вспомогательные практические методы

A.3.2.4.3.1 Основные практические методы

К основным практическим методам относятся следующие действия:

a) изучение ролей, связанных с сохранением защищенной системной среды, в рамках учебных курсов по вопросам обеспечения безопасности;

b) проведение очных курсов или обучение без отрыва от производства по вопросам требований к каждой выполняемой роли;

c) подтверждение знаний через аттестацию и/или экзамены;

d) привлечение профильных специалистов для каждого учебного курса, для ознакомления с дополнительными материалами и консультациями;

e) периодическое изучение и утверждение программы обучения и оценка ее эффективности;

f) своевременное доведение важной информации до сведения всего персонала через реализацию программы информирования и формирования осведомленности;

g) первоначальное обучение всего персонала и периодическое последующее обучение (например, на ежегодной основе).

Несмотря на то, что ни один из этих основных практических методов не характерен для обучения по вопросам безопасности IACS, задачи и содержание программы обучения должны отражать взаимосвязь между безопасностью IACS и последствиями для сферы HSE.

A.3.2.4.3.2 Дополнительные практические методы

К дополнительным практическим методам относятся следующие действия:

a) определение обучения по вопросам информационной безопасности в качестве составляющей общей работы компании в области обучения для всего персонала;

b) индивидуальное составление учебного курса по вопросам информационной безопасности с последовательным изложением материалов для конкретной роли в организации;

c) регулярное ведение и изучение журналов с результатами обучения персонала и графиков актуализации, в зависимости от должностей/ролей сотрудников;

d) организация обучения информационной безопасности, предоставляемого поставщиками;

e) определение сроков, периодичности и содержания программы информирования и формирования осведомленности и документальное оформление программы в целях повышения осведомленности организаций в области средств контроля информационной безопасности;

f) включение компонента обзора основных положений программы информирования и формирования осведомленности для всего персонала в целях обеспечения их осведомленности о практиках безопасности в их первый день работы;

g) ежегодное изучение программы обучения и программы информирования и формирования осведомленности на предмет их эффективности, приемлемости, содержания и соответствия используемым инструментам и корпоративным практикам.

A.3.2.4.4 Использованные ресурсы

Данный элемент частично основан на материалах [2], [23], [24], [26].

A.3.2.5 Элемент «План непрерывности бизнеса»

A.3.2.5.1 Описание элемента

План непрерывности бизнеса определяет процедуры поддержания на устойчивом уровне или возобновления важных бизнес-операций в процессе восстановления после существенного сбоя. План непрерывности бизнеса разрабатывается для целей принятия мер реагирования на последствия после чрезвычайных происшествий, нарушений безопасности и не предоставление обслуживания. Разработка детального плана позволит гарантировать возможность восстановления и использования важнейших систем IACS в максимально возможные короткие сроки после наступления существенного сбоя.

A.3.2.5.2 Область применения плана непрерывности бизнеса

Прежде чем приступить к разработке плана бизнес-непрерывности, важно понять, когда и в каких ситуациях такой план должен применяться. Незапланированное вмешательство может быть в виде стихийного бедствия (т. е. торнадо, ураган, землетрясение или наводнение), непреднамеренного происшествия, вызванного воздействием человека (например, случайное повреждение оборудования, пожар, взрыв или ошибка оператора), преднамеренного происшествия, вызванного воздействием человека (например, бомбовая атака, применение огнестрельного оружия, вандализм, хакерские или вирусные атаки) или отказа оборудования. Если рассматривать потенциальные отказы оборудования, на восстановление после отключения механического оборудования может уйти стандартное время в размере нескольких минут или часов и несколько дней, недель или месяцев после стихийного бедствия. Поскольку зачастую управление надежностью и обслуживанием электрического/механического оборудования регулируется отдельной дисциплиной, некоторые организации предпочитают определять бизнес-непрерывность таким образом, который бы исключал подобные источники отказов. В связи с тем, что бизнес-непрерывность в основном связана с продолжительными последствиями технологических отказов, часть организаций также определяют минимальный предел прерывания в отношении рассматриваемых рисков. Для целей информационной безопасности IACS не рекомендуется применять любые такие ограничения. Необходимо принимать во внимание как продолжительные перерывы (восстановление после стихийного бедствия), так и короткие перерывы (восстановление работы). План также включает в себя и другие аспекты восстановления после чрезвычайных происшествий, например, управление в чрезвычайных обстоятельствах, человеческие ресурсы и взаимодействие со СМИ или прессой.

Поскольку некоторые такие потенциальные нарушения включают в себя происшествия, вызванные воздействием человека, важно организовывать работу с учетом физической безопасности, что позволить понять риски, связанные с такими происшествиями, и контрмеры по обеспечению физической безопасности для их предупреждения. Для организации физической безопасности также важно понимать, на каких участках производственной площадки установлены IACS, которые могут привести к рискам более высокого уровня.

A.3.2.5.3 Процесс планирования непрерывности бизнеса

Прежде чем приступить к разработке плана действий при наступлении потенциальных перебоев, важно определить специфические цели для различных систем и подсистем, участвующих в процессе, с учетом стандарт-

ных потребностей компании. Восстановление системы подразумевает восстановление всех линий связи и возможностей IACS и обычно выражается через целевое время восстановления и время на восстановление таких линий связи и возможностей. Восстановление данных подразумевает восстановление данных, описывающих состояние производства или продукта в прошлом, и обычно выражается через целевую точку восстановления или наибольший период времени, в течение которого допускается отсутствие данных.

После того, как будут определены цели восстановления, необходимо сформировать перечень потенциальных нарушений и разработать и документально оформить процедуру восстановления. Для большей части незначительных нарушений работа по ремонту и замене оборудования на основании инвентарного запаса важнейших запасных частей может оказаться действенной для достижения целей восстановления. В других случаях требуется разработка чрезвычайных план. Принимая во внимание потенциальную стоимость таких планов, работу по их изучению следует вести вместе с менеджерами, отвечающими за планирование бизнес-непрерывности, что позволить определить, насколько они оправданны.

Необходимо определить требования для группы по работе с бизнес-непрерывностью и сформировать такую группу. Группа должна включать в себя владельцев IACS и прочих потенциальных владельцев объектов промышленной эксплуатации. В случае существенного нарушения такая группа должна определить приоритет важнейших систем компании и систем IACS, что позволит возобновить операции.

Необходимо разработать график тестирования всех или части восстановительных процедур. Как правило, тестирование процедур для конкретной подсистемы проводится ежегодно и в результате ротации конкретных подсистем оказывается, что за 5—10 лет все системные процедуры в конечном итоге проходят тестирование. Такая периодичность приводится в качестве примера и определяется организацией в рамках процесса планирования.

Особое внимание следует уделять проверке резервных копий для данных по конфигурации системы и данных о производстве или продукте. Тестированию должны быть подвергнуты не только эти данные при создании резервных копий, но и процедуры, выполняемые для их хранения, которые должны проверяться с определенной периодичностью в целях подтверждения того, что резервные копии и соответствующие данные пригодны для использования и являются точными. Резервные копии должны храниться при таких условиях среды, которые не повлияют на их пригодность, и в надежном месте, легко доступном в случае необходимости для авторизованного персонала.

При наступлении инцидента от организации может потребоваться предоставить следователям (сторонним или внутренним) судебные данные об инциденте.

По прошествии времени потребуется пересмотреть и внести изменения в план бизнес-непрерывности, что позволит показать изменения в структуре управления, организации, бизнес-модели, отраслевые изменения и т. п.

A.3.2.5.4 Вспомогательные практические методы

A.3.2.5.4.1 Основные практические методы

К основным практическим методам относятся следующие действия:

a) формирование группы по работе с бизнес-непрерывностью, с привлечением заинтересованных лиц организации (т. е. владельцев компании, IT-персонал и персонал IACS) для разработки плана;

b) определение приоритета важнейших бизнес-систем и систем IACS с учетом особенностей системы и времени, требуемого на восстановление. Это определяется границами допустимости риска и целями восстановительных процедур;

c) определение времени/ресурсов, требуемых для восстановления системы, расположения резервных файлов, аппаратного обеспечения, периодичности резервирования, потребности в запасных частях и т. п., чтобы гарантировать возможность восстановления важнейших систем при наступлении чрезвычайного происшествия;

d) обеспечение доступности записей, связанных с управлением документацией и процедурами резервирования/восстановления, различными способами из различных мест (например, электронные копии, которые хранятся в хранилище, и бумажные копии, хранящиеся на площадке и в защищенном объекте), чтобы исключить все до единой критические точки;

e) изучение возможного влияния на третьи лица, например, совместные предприятия и цепочки поставок;

f) определение потребности в дополнительном страховании деятельности;

g) определение специфических ролей и обязанностей для каждой части плана. Некоторые организации подразделяют группу на подгруппы, подотчетные координационному комитету. Примеры таких подгрупп: оценка ущерба, возобновление и восстановление, линии связи (внешние и внутренние), реагирование в чрезвычайных ситуациях;

h) назначение ответственности за осуществление плана бизнес-непрерывности и четкое определение обстоятельств, при которых начинается осуществление плана;

i) детальное определение обстоятельств, при которых принимаются специфические чрезвычайные меры. Выбор мер определяется конкретным сценарием. Требуется рассмотреть последствия чрезвычайного происшествия для IT или IACS, оказывающих физическое воздействие на производственные объекты;

j) определение типа, количества и особенностей требуемых ресурсов и их назначения;

k) детальное описание способов коммуникации для членов группы, а также непредвиденных обстоятельств, при которых теряется электронная почта, происходит сбой телефонной связи и т. п. в случае существенного чрезвычайного происшествия;

l) определение частоты и способа проведения тестирования, аттестации и оценки плана бизнес-непрерывности и использование этих результатов для усовершенствования и актуализации плана в целях повышения его эффективности;

m) детальное описание рисков, связанных с работой по плану бизнес-непрерывности, также способы их устранения и/или смягчения;

n) определение данных, для которых требуется особый подход к обработке и защите, а также информации, имеющей крайне важное значение для обеспечения непрерывной деятельности;

o) установление промежуточных процедур для обеспечения возможности осуществления минимального набора операций. На данном промежуточном этапе будет уместным сокращение ассортимента продукции;

p) определение и хранение резервных систем (аппаратное/программное обеспечение, документация) в безопасном месте;

q) тестирование резервных систем в соответствии с заранее определенным графиком на предмет надлежащей работы систем и правильного восстановления данных;

r) идентификация и/или хранение запасов для использования группой реагирования в чрезвычайных ситуациях и помощи при проведении восстановительных работ (например, вода в бутылках, детоксикационные души, аварийный запас сжатого воздуха или респираторы);

s) определение процесса возобновления нормальной деятельности.

A.3.2.5.4.2 Дополнительные практические методы

К дополнительным практическим методам относятся следующие действия:

a) определение приоритетов IT-систем и систем IACS по типу их воздействия на бизнес или операционную деятельность с учетом границ допустимости риска в организации. IACS могут влиять на IT-системы, которые выпали из поля зрения, поскольку не проводились совместная проверка и определение приоритетов систем в качестве единого целого. Планирование действий на случай чрезвычайных происшествий и планов восстановления должно предусматривать взаимосвязь этих систем;

b) распределение важнейших резервированных систем в различных географических регионах. Если это неосуществимо, резервные данные и оборудование должны храниться в месте, не подверженном риску наступления аналогичного происшествия, который характерен для главной системы (т. е. возвышение на случай наводнения или бетонный бункер на случай торнадо);

c) тестирование и актуализация планов бизнес-непрерывности на периодической основе или по мере необходимости;

d) привязка планов бизнес-непрерывности к системе управления изменениями, за счет чего обеспечивается актуальное состояние плана бизнес-непрерывности в случае существенных изменений;

e) тестирование планов информирования на периодической основе или по мере необходимости и назначение ответственных лиц за ведение актуального списка телефонов сотрудников;

f) предоставление важной контактной информации ключевой группе (карта, имеющаяся у каждого члена группы);

g) хранение письменных копий плана каждым членом группы на дому;

h) введение процедур/или контрактов для приобретения дополнительного аппаратного обеспечения, ПО и запасов, если в них существует необходимость. Следует иметь в виду, чтобы в плане бизнес-непрерывности время на замену оборудования/программ для IACS было сопоставимо со временем замены оборудования, находящегося под контролем. В некоторых случаях на ремонт/замену такого оборудования уходит большое количество времени, существенно превышающее время замены систем управления;

i) заключение предварительных соглашений о гарантированном уровне обслуживания с поставщиками услуг по восстановлению после чрезвычайных происшествий.

A.3.2.5.5 Использованные ресурсы

Данный элемент частично основан на материалах [23], [37], [48], [51].

A.3.2.6 Элемент «Политика и процедуры безопасности»

A.3.2.6.1 Описание элемента

В каждой системе управления существуют наборы общих требований, которые должны выполняться системой, и перечни организаций, которые подпадают под эти требования. В настоящем стандарте эти требования именуются политиками. Также существуют описания того, как физические лица и организации выполняют требования в системе управления. В настоящем стандарте эти описания именуются процедурами.

Для CSMS политика является общим руководством по требованиям к кибербезопасности в организации. Она содержит инструкции в отношении того, что организация должна понимать под кибербезопасностью, как она должна выполнять программу кибербезопасности и определять границы допустимости рисков. Политика для CSMS создается на основе корпоративной политики более высокого уровня, которая разрешает ее составление. Политика содержит негативные последствия невыполнения, включающие возможный разрыв трудового договора или даже уголовное преследование.

В процедурах подробно описано, каким образом политики для CSMS реализуются в организации. Они могут быть менее строгими по сравнению с политиками и могут включать положения, оговаривающие исключения, поскольку очень сложно создать процедуры для каждой возможной ситуации или события.

Политики для CSMS и процедуры, разработанные организацией, должны давать персоналу четкое представление о его роли и обязанностях по сохранению имущественных объектов организации.

А.3.2.6.2 Разработка политики безопасности

Разработка политики безопасности для организации не должна рассматриваться как линейная задача. После завершения первоначальной стадии разработки политики организации необходимо изучить и проанализировать эффективность этой политики и внести в нее необходимые изменения. Политика не должна разрабатываться отдельно от других систем управления рисками в организации.

Разработка и реализация политики безопасности подразумевает участие высшего руководства, задействованного во всех сферах деятельности организации и несущего ответственность за такие типы систем. Выработав и утвердив политику безопасности, высшее руководство может продемонстрировать стремление к непрерывному совершенствованию. Обязательство руководства, относящееся к политике безопасности, подразумевает признание руководством политики безопасности ответственностью бизнеса, которая разделяется между всеми участниками команды руководителей, а также признание ее политикой, имеющей физические и киберкомпоненты. Процедуры безопасности должны быть интегрированы в общие бизнес-стратегии и пользоваться поддержкой руководства.

Многие организации с IACS внедряют политики для таких систем, как техника безопасности, физическая безопасность IT, а также для поведения работников. В начале процесса разработки CSMS необходимо попытаться внедрить политики кибербезопасности в систему с существующими политиками и процедурами. Это зачастую требует изменения политики в различных системах управления рисками. Например, в существующих системах управления рисками риски уже могут быть охарактеризованы и могут быть установлены границы допустимости рисков, которые должны учитываться при разработке новой CSMS. Пояснения по объединению политик и систем управления рисками приведены в IEC/TS 62443-1-1 (подпункт 5.6). Политики безопасности, относящиеся к рискам IACS, также рассматривают широкий диапазон вопросов от организационных требований к руководству до технически детальных требований к конфигурации системы. Рекомендуется, чтобы эти политики были выделены в отдельные подгруппы, чтобы пользователи, интересующиеся конкретными темами, могли легко их найти.

Во многих обстоятельствах политики и процедуры безопасности могут считаться контрмерами, снижающими риск. Они могут принимать несколько форм от административных процедур до автоматизированных средств безопасности. Необходимо стремиться к тому, чтобы общая стоимость реализации контрмер была меньше совокупного влияния риска. Уменьшение стоимости реализации контрмер при сохранении уровня снижения риска является более ценным для организации. В случаях, когда существует эффект масштаба, управление технологиями будет осуществлять IT-дисциплина в случаях, когда масштаб может быть выгодно использован. Таким образом, подробные политики безопасности IT-дисциплины должны быть проверены на предмет возможного использования для IACS.

При разработке политик кибербезопасности важно учитывать требования по соответствию стандарту, а также процесс аудита. Поскольку IACS необходимо оценить на соответствие политике безопасности, необходимо убедиться, что выработанные политики не противоречат друг другу, и что более важно — политикам управления рисками. Например, политика безопасности на конкретном атомном предприятии требует, чтобы все стационарные компьютеры были защищены паролем. Эта политика также требует, чтобы все операторские станции были защищены паролем, но они должны быть открыты в соответствии с нормами техники безопасности. Соблюдение политики защиты паролем стационарных компьютеров приведет к несоблюдению политик по охране труда, технике безопасности и охране окружающей среды. Политика кибербезопасности должна была быть изначально создана с учетом влияния, которое она окажет на все системы предприятия. Более удачным подходом будет создание политики, которая предписывает защищать стационарные компьютеры от несанкционированного использования, а затем составить процедуры, которые могут потребовать защиты паролем в некоторых случаях, а в других ситуациях необходимо просто обеспечивать физическую изоляцию.

А.3.2.6.3 Определение границ допустимости рисков для организации

Организация должна выработать политику определения границ допустимости рисков, относящуюся к уровням риска, соответствующим определенным комбинациям вероятности и последствий. Эта политика может быть основана на качественной оценке рисков, включающей перечень имущественных объектов или сценариев с ранжированием общей вероятности и последствий, которые были определены и присвоены в рамках процесса оценки рисков организации (см. А.2.3).

На типичной шкале уровней риска, приведенной в таблице А.3, вероятность и последствия разбиты на три уровня. Уровень риска также разбит на три уровня. Уровни риска в каждом блоке (высокий, средний и низкий) соответствуют конкретной комбинации вероятности и последствий. Организация вырабатывает политику определения границ допустимости рисков, относящуюся к определенному уровню корпоративной реакции на риск. Например, риски в категории «Высокий» могут являться допустимыми в течение 6 месяцев; риски из категории «Низкий» не стоят усилий, затраченных на них; средний уровень риска заслуживает средних усилий. Другими словами организация установила, что она может допускать высокий уровень риска не более 6 мес.

А.3.2.6.4 Анализ и пересмотр политики кибербезопасности

Политики кибербезопасности должны регулярно анализироваться, утверждаться для подтверждения их актуальности и выполнения и пересматриваться, что требуется для того, чтобы они оставались актуальными. Когда политика кибербезопасности имеет более высокий уровень, она не должна актуализироваться так часто, поскольку она описывает «что», а не «как». Процедуры, описывающие способы действия, могут изменяться при появлении новых угроз или технологий, но обоснование защиты системы останется неизменным.

А.3.2.6.5 Применение политик кибербезопасности

При создании политики кибербезопасности необходимо определить метод их применения. Например, политики безопасности могут быть выложены в корпоративный Интернет, и пользователи могут пройти обучение и узнать, каким образом политика скажется на них. Политики являются основой CSMS, поэтому метод их применения должен соответствовать применению системы управления.

А.3.2.6.6 Вспомогательные методы

А.3.2.6.6.1 Основные методы

К основным методам относятся следующие действия:

a) определение обязательств, участия и поддержки руководства при создании и реализации политик кибербезопасности;

b) анализ и утверждение всеми подразделениями и отделами, к которым относится политика, включая управление деятельностью;

c) опубликование письменных документов, описывающих политики безопасности;

d) регулярный анализ, подтверждение и пересмотр политик для подтверждения их актуальности и выполнения;

e) донесение и распространение политик кибербезопасности среди персонала.

А.3.2.6.6.2 Дополнительные методы

К дополнительным методам относятся следующие действия:

a) создание политик, соответствующих определенному жизненному циклу организации. Политики не подлежат постоянным изменениям или изменениям в связи с актуальными вопросами;

b) создание вспомогательных политик, которые определяют, каким образом политика более высокого уровня выполняется для этих групп. Например, ограничения по защите паролем и контроль физического доступа могут быть неуместными в некоторых ситуациях, связанных с производственным управлением. На этот случай должны быть предусмотрены процедурные гарантии с исключениями;

c) создание политик безопасности для разрешения ряда проблем с безопасностью, включая снижение рисков и изменение отношения персонала к кибербезопасности;

d) приведение политик безопасности в соответствие с общими политиками и стратегиями организации;

e) интеграция политик кибербезопасности в общую политику безопасности, которая также рассматривает физические элементы;

f) определение лиц и способа выполнения политики;

g) определение того, каким образом пользователи должны выполнять положения политик;

h) обеспечение среды последовательного управления политикой;

i) определение того, какие политики применяются к конкретным пользователям и группам пользователей;

j) определение системы измерения степени соответствия политикам.

А.3.2.6.7 Использованные ресурсы

Этот элемент был частично основан на материалах [23], [26], [30], [43].

А.3.3 Группа элементов «Избранные контрмеры по безопасности»

А.3.3.1 Описание группы элементов

Второй группой элементов в данной категории являются «Избранные контрмеры по безопасности». Элементы в этой группе описывают основные типы средств управления безопасностью, которые являются частью хорошо спроектированной CSMS. В настоящем стандарте не предпринимается попытка описать полную реализацию любой из избранных контрмер по безопасности. В нем рассматриваются аспекты политики, процедур и практических методов, относящихся к этим конкретным контрмерам по безопасности. На рисунке А.7 графически показаны шесть элементов группы:

- безопасность персонала;
- физическая безопасность и безопасность среды;
- сегментация сети;
- контроль доступа — администрирование учетных записей;
- контроль доступа — аутентификация;
- контроль доступа — авторизация.



Рисунок А.7 — Графическое представление группы элементов «Избранные контрмеры по обеспечению безопасности»

CSMS — это система, посредством которой отбираются и выполняются избранные контрмеры по безопасности организации. Таким образом, конкретные контрмеры считаются скорее результатом этой системы, чем частью самой системы. Однако, контрмеры, рассматриваемые в настоящем подпункте, были включены в настоящий стандарт, поскольку их применение является основополагающим для разработки политики и архитектуры безопасности. По этой причине они должны быть рассмотрены до создания CSMS.

А.3.3.2 Элемент«Безопасность персонала»

А.3.3.2.1 Описание элемента

Безопасность персонала подразумевает анализ существующего и будущего персонала для определения того, будет ли он выполнять свои обязанности по безопасности IACS, а также для определения и обучения таким обязанностям. Работники, подрядчики и временный персонал, которые имеют доступ к секретной информации о производственной деятельности или сетям IACS, аппаратному и ПО создают потенциальный риск при обнаружении или изменении секретной информации или предоставлении несанкционированного доступа к IT-системам.

А.3.3.2.2 Требования к безопасности персонала

Во многих организациях требования к безопасности персонала основаны на обеспокоенности по поводу инсайдерских угроз и возможности аварий, вызванных невнимательным отношением к деталям или несоответствием персонала занимаемой должности из-за отсутствия должной подготовки или применения веществ, затуманивающих сознание. Реализация политики по безопасности персонала позволяет уменьшить число таких проблем.

При разработке программы по безопасности персонала в нее необходимо включить весь персонал, имеющий доступ к рассматриваемым системам, не ограничиваясь исключительно персоналом, пользующимся оборудованием традиционного компьютерного зала.

Компьютеры в работе IACS являются инструментами, используемыми для продуктивной и безопасной работы оборудования. Персонал управляет ключевыми для деятельности системами, поэтому необходимо предпринять все возможные меры для того, чтобы он был квалифицированным и соответствовал занимаемой должности. Этот процесс начинается при найме и продолжается до расторжения трудового договора. Для того, чтобы система работала в безопасном режиме, требуется постоянное внимание со стороны руководства и сотрудников.

В политике по безопасности персонала должно быть четко указано обязательство организации и обязанности персонала по безопасности. В ней должны быть рассмотрены обязанности по безопасности всего персонала (отдельных работников и организации в целом) от найма до окончания работы, особенно для должностей, связанных с секретностью (включающих работников, перспективных и контрактных работников, сторонних подрядчиков и подразделения компании, например, по связям с общественностью).

Весь персонал, включая вновь нанятых работников или работников, переведенных с других должностей на должности, связанные с секретностью (например, требующие привилегированного доступа), должен тщательно отбираться на стадии подачи заявления на трудоустройство. Отбор должен включать установление личности, личных и трудовых референций и уровня образования и подготовки. Проверка биографии также может включать кредитную историю, участия в криминальной деятельности и связи с наркотиками, поскольку эта информация может быть полезной при определении пригодности кандидата (с учетом выполнения местных законов о защите частной жизни). Третьи стороны, подрядчики и аналогичные лица должны проходить не менее жесткую проверку, чем работники на сравнимых должностях. Работники и подрядчики также могут проходить непрерывную проверку,

например, в отношении финансовой, криминальной деятельности или деятельности, связанной с наркотиками. Из-за большого количества секретной информации о производственной деятельности и возможных рисков, связанных с охраной труда, техникой безопасности и охраной окружающей среды, в некоторых IACS может возникнуть необходимость в проверке широкой группы работников, которые имеют доступ к IACS. Производственные работники могут проходить проверку биографии на том же уровне, что и обычные администраторы IT-системы. Термины «отбор» и «проверка биографии» намеренно оставлены без пояснений, чтобы организация могла определить уровень проверки персонала. Термин «должности, связанные с секретностью» также должен быть определен организацией, поскольку подразумевается, что некоторые должности могут оказывать незначительное или нулевое воздействие на безопасность системы.

Во время найма в условиях трудоустройства должны быть четко указаны обязанности работника в отношении кибербезопасности. Эти обязанности должны действовать в течение разумного периода времени после прекращения трудоустройства. При найме подрядчиков или работе со сторонним персоналом их обязанности по безопасности должны быть документированы и включены во все соглашения. По возможности обязанности должны быть четко установленными.

Персонал должен быть осведомлен об ожиданиях организации в отношении безопасности и своих обязанностей посредством четко документированных положений, передаваемых организацией. Персоналу необходимо принять на себя взаимную ответственность для обеспечения безопасной и надежной работы организации. Организации могут рассмотреть возможность подписания соглашения о конфиденциальности или неразглашении всем персоналом объектов по обработке информации. Любые соглашения о конфиденциальности должны быть рассмотрены и подписаны работниками при найме. Сторонние подрядчики и временный персонал, не включенные в официальное соглашение о неразглашении, также должны подписать соглашение о конфиденциальности перед началом работы.

Организации должны создавать должностные инструкции на основе разделения обязанностей для обеспечения того, чтобы доступ к информации осуществлялся исключительно для выполнения должностных обязанностей, а для выполнения высокорискованных операций требовалось больше одного человека. Эти обязанности должны быть разделены между персоналом для проведения соответствующих проверок и соблюдения баланса, чтобы ни у одного лица не было полного контроля над действиями, которые меняют работу IACS. Роли и обязанности по безопасности для конкретной должности должны периодически анализироваться и пересматриваться для соответствия меняющимся потребностям компании.

Весь персонал должен следить за ситуациями, которые могут привести к инцидентам с безопасностью. Компаниям необходимо обучить руководство, чтобы оно контролировало поведение персонала, которое может привести к кражам, мошенничеству, ошибкам или сложностям с безопасностью. Необходимо установить дисциплинарную процедуру за нарушение кибербезопасности довести ее до сведения персоналу. Она должна быть привязана к законным или карательным мерам против таких преступлений в стране.

A.3.3.2.3 Вспомогательные методы

A.3.3.2.3.1 Основные методы

К основным методам относятся следующие действия:

a) проверка персонала при найме, например, проверка биографии перед наймом или переводом на работу, связанную с секретностью, особенно, для должностей, связанных с секретностью;

b) проверка персонала, в первую очередь занимающего должности, связанные с секретностью, на регулярной основе для выявления финансовых проблем, криминальной деятельности или проблем с наркотиками;

c) предоставление информации об условиях найма или контракта всему персоналу с указанием личной ответственности за кибербезопасность;

d) документирование и предоставление информации об ожиданиях организации по безопасности и обязанностях персонала на регулярной основе;

e) принятие персоналом взаимной ответственности за обеспечение безопасной и надежной работы организации;

f) разделение обязанностей среди персонала для выполнения соответствующих проверок и поддержания баланса;

g) подписание всем персоналом соглашения о конфиденциальности или неразглашении;

h) установление процедуры дисциплинарного воздействия для персонала, нарушившего политику организации по безопасности.

A.3.3.2.3.2 Дополнительные методы

К дополнительным методам относятся следующие действия:

a) распределение должностных функций на основе разделения обязанностей для обеспечения доступа к информации только для выполнения должностных обязанностей и необходимости в участии нескольких лиц для завершения высокорискованных операций;

b) документирование обязанностей по безопасности и включение их в должностные инструкции, контракты и другие соглашения с третьими сторонами.

A.3.3.2.4 Использованные ресурсы

Данный элемент основан на материалах [2], [23], [26], [30], [43].

А.3.3.3 Элемент «Физическая безопасность и защита от внешних воздействий»

А.3.3.3.1 Описание элемента

Физическая безопасность и защита от внешних воздействий относятся к созданию безопасной среды для защиты материальных или физических имущественных объектов (т. е. компьютеров, сетей, информационного или производственного оборудования) от повреждения, утраты, несанкционированного доступа или ненадлежащего использования. Физическая безопасность и защита от внешних воздействий информационной системы является общей дисциплиной, заимствующей знания и опыт из других областей физической безопасности или безопасности оборудования. Меры обеспечения физической безопасности и защиты от внешних воздействий должны быть разработаны для дополнения мер по кибербезопасности, предпринятых для защиты этих имущественных объектов.

Меры по обеспечению физической безопасности и защиты от внешних воздействий отличаются друг от друга, но они взаимоувязаны, поскольку созданы для защиты имущественных объектов организации от угроз. Меры по обеспечению физической безопасности предпринимаются для физической защиты имущественных активов организации от несанкционированного доступа, утери, повреждения, ненадлежащего использования и т. д. Меры по обеспечению защиты от внешних воздействий предпринимаются для защиты имущественных объектов организации от условий среды, которые могут сделать их непригодными для использования или повредить информацию, которую они содержат.

Несмотря на то, что политики и процедуры по кибербезопасности имеют большое значение для надлежащей защиты информации и систем управления, для действительно эффективной защиты они должны дополняться соответствующим уровнем физической безопасности. Например, даже использование такого жесткого контроля, как аутентификация и контроль доступа, не достаточно хорошо защищает систему, если существует возможность войти в объект и физически удалить или повредить электронные носители данных.

А.3.3.3.2 Основания для физической безопасности и защиты от внешних воздействий

А.3.3.3.2.1 Общие положения

Во многих организациях требования безопасности среды и защиты от внешних воздействий по периметру относятся только к физическим имущественным объектам организации и могут не соответствовать требованиям по кибербезопасности. Из-за объединения нескольких организаций на площадке (т. е. бизнес-партнеров, подрядчиков и третьих сторон) может потребоваться дополнительная физическая защита имущественных объектов IACS. На объектах IACS физическая безопасность ориентирована больше на защиту имущественных объектов системы, чем на саму производственную информацию. Проблема заключается не столько в фактической краже или повреждении вычислительных и управляющих устройств, сколько в воздействии, которое они могут оказать на поддержание безопасности производства.

При разработке программы физической безопасности имущественных объектов важно включить в нее все системы, а не ограничиваться традиционным оборудованием компьютерного зала. В IEC/TS 62443-1-1 рассматриваются критерии, которые могут использоваться для определения имущественных объектов, которые должны учитываться в составе CSMS.

Компьютеры, входящие в IACS, являются инструментами продуктивного и безопасного управления объектом. Они являются средством, как и защищаемый имущественный объект. В некоторых случаях установка оборудования в закрытом помещении угрожает безопасности и/или производительности, поскольку время реагирования при получении доступа к оборудованию может увеличиться.

При определении процедур физической безопасности для защищаемого имущественного объекта необходимо исходить из практических инженерных соображений, уравнивающих все риски. Несмотря на то, что обычной практикой является расположение маршрутизаторов и другого сетевого оборудования в закрытой среде, применение этой практики для другого оборудования может быть нецелесообразным. Полевые устройства (т. е. исполнительные механизмы клапанов, пускатели двигателей и реле) обычно приводятся в действие напрямую на месте установки без передачи сигналов управления через сеть IACS. Защита всех полевых устройств по отдельности может быть очень дорогостоящей, поэтому процедуры контроля доступа при физическом ограждении периметра обычно требуются на объектах, связанных с высоким риском.

В А.3.3.3.2.2—А.3.3.3.2.14 описаны процедуры, которые необходимо учитывать при создании безопасной среды для защиты материальных имущественных объектов от физического повреждения из-за физического проникновения или условий среды.

А.3.3.3.2.2 Политика безопасности

Письменная политика безопасности содержит инструкции в отношении того, что организация должна понимать под безопасностью, как она должна реализовывать и анализировать программу безопасности для дальнейшего совершенствования. Эти письменные политики позволяют персоналу четко понимать свою роль и обязанности в сохранении имущественных объектов организации. Организации необходимо установить политику физической безопасности и защиты от внешних воздействий, которая будет дополнять политику кибербезопасности и политику физической безопасности. Основной целью является ликвидация любых разрывов, которые могут существовать между этими двумя политиками. Политика физической безопасности и защиты от внешних воздействий должна соответствовать и выполнять политики, указанные выше, а также другие политики безопасности, относящиеся к безопасности системы управления. Для определения необходимых процедур физической безопасности используется детальная оценка рисков физической безопасности.

А.3.3.3.2.3 Периметр безопасности

Информация или имущественные объекты, имеющие критическое значение, должны быть расположены в безопасной зоне, защищенной периметром безопасности или средствами управления доступом. Такие средства управления физической безопасностью применяются совместно с мерами по кибербезопасности для защиты информации. Для создания барьеров от несанкционированного доступа к оборудованию необходимо создать один или несколько периметров безопасности. Несколько периметров могут находиться в состоянии «один внутри другого» для обеспечения более жесткого контроля. Например, внутри пульта управления может находиться закрытый шкаф с доступом с помощью ключ-карты на территории объекта с охраняемым ограждением по периметру.

А.3.3.3.2.4 Управление доступом

На каждом барьере или границе необходимо предусмотреть соответствующие средства управления доступом. К таким средствам относятся закрываемые ворота, калитки с соответствующими замками или защитным устройством. Средства управления доступом должны соответствовать уровню безопасности, требуемому в зоне, защищаемой такими устройствами, и необходимости в быстром доступе.

А.3.3.3.2.5 Защита от внешних воздействий

Имущественные объекты необходимо защищать от повреждений, вызываемых угрозами среды, например, пожаром, водой, дымом, пылью, излучением и ударами. Особое внимание необходимо уделить системам противопожарной защиты, применяемым в зонах, влияющих на IACS, для того, чтобы системы, ответственные за защиту объекта, обеспечивали защиту устройств IACS, не вызывая дополнительных рисков для производственной деятельности.

А.3.3.3.2.6 Процедуры безопасности

Персоналу необходимо выполнять и обеспечивать исполнение процедур физической безопасности, которые были созданы для усиления средств управления доступом и других средств физического контроля. Персонал не должен обходить какие-либо средства автоматизированного управления доступом или иные автоматизированные средства физического контроля. Примером работника, обходящего средство физического контроля, является работник, предотвращающий закрытие входной двери пульта управления с помощью стула.

А.3.3.3.2.7 Отдельные точки отказа

Отдельных точек отказа необходимо по возможности избегать. Наличие резервных систем обеспечивает увеличение надежности системы, которая способна справляться с незначительными инцидентами, не влияя на предприятие или организацию, например, использование резервной системы электроснабжения в критически важной системе обеспечивает функционирование такой системы при повреждении одного источника питания.

А.3.3.3.2.8 Соединения

Все соединения (т. е. электроснабжение и связь, включая проводку для полевых входов-выходов, шинопроводы входов-выходов, сетевые кабели, кабели соединения контроллеров, модемов и т. д.), контролируемые организацией, должны быть надлежащим образом защищены от небрежного отношения или повреждения. Эти меры включают размещение соединений в закрытых шкафах или в огороженных зонах. Уровень физической безопасности для соединений должен быть соизмеримым с уровнем безопасности систем, к которым они подключаются. При рассмотрении физической безопасности необходимо учитывать последствия повреждений, вызываемых средой. Эти соединения должны быть также защищены от естественных факторов, например, нагрева, пожара, пыли и т. д., которые могут привести к неисправности.

А.3.3.3.2.9 Техническое обслуживание оборудования

Все оборудование, включая вспомогательное оборудование регулирования условий окружающей среды, должно проходить надлежащее техническое обслуживание для обеспечения правильной эксплуатации. Необходимо составлять графики технического обслуживания и проводить профилактическое техническое обслуживание. Записи о техническом обслуживании оборудования необходимо сохранять для определения тенденций при необходимости внесения корректировок в графики технического обслуживания.

А.3.3.3.2.10 Аварийная сигнализация

Необходимо создать надлежащие процедуры для контроля и передачи аварийных сигналов при обнаружении угрозы для физической безопасности или защиты от внешних воздействий. Персонал должен реагировать на все аварийные сигналы соответствующими мерами. Все оборудование, с учетом его уровня безопасности, должно иметь средства сигнализации на случай физического проникновения или угроз среды. Они могут включать датчики движения, камеры или дверную сигнализацию на случай физического проникновения и пожарную сигнализацию, датчики воды или температурные датчики на случай возникновения угрозы со стороны среды.

А.3.3.3.2.11 Жизненный цикл оборудования

Необходимо создавать надлежащие процедуры в отношении добавления, вывода из эксплуатации и списания всего оборудования и проводить аудит таких процедур. Рекомендуемой практикой является отслеживание имущественных объектов. Эти процедуры включают списание и форматирование рабочих станций, очищение накопителя и т. д. Закупка аппаратного обеспечения также должна учитывать способ отслеживания оборудования, а также его очищения и утилизации, когда в нем больше нет необходимости.

А.3.3.3.2.12 Информация в физической форме

Вся информация, имеющая физическую форму (т. е. письменные и напечатанные документы, магнитные носители данных и компакт-диски), должна быть надлежащим образом защищена от физических угроз. Такая за-

щита может включать размещение информации в закрываемых помещениях или шкафах для предотвращения несанкционированного доступа. Также необходимо уделить внимание защите информации от угроз среды, например, магнитных полей, высокой влажности, нагрева или прямых солнечных лучей и других угроз, которые могут повредить информацию. Аналогично процедурам для оборудования, должны существовать процедуры для безопасной утилизации физических носителей данных, ставших ненужными.

A.3.3.3.2.13 Использование имущественных объектов за пределами контролируемой среды

Особое внимание необходимо уделить использованию имущественных объектов, которые влияют на IACS за пределами сети системы. Необходимые меры должны включать размещение имущественных объектов на интегрирующем устройстве системы до монтажа. Кроме того, такие объекты, как ноутбуки с доступом к сети IACS, используемые за пределами площадки, должны рассматриваться как продолжение сети системы с выполнением всех соответствующих процедур физической безопасности и защиты от внешних воздействий. Необходимо уделять внимание установлению единого уровня безопасности для имущественных объектов, которые временно находятся за пределами нормальных границ безопасности. Это может потребовать специального планирования или использования оборудования для защиты таких объектов от несанкционированного доступа или использования или от повреждений, вызванных средой.

A.3.3.3.2.14 Промежуточная защита имущественных объектов

Во время и после любого события, связанного с физической безопасностью или защитой от внешних воздействий в критически важных системах может быть нарушено электроснабжение или другое обслуживание. Необходимо предпринять меры для защиты таких критически важных систем. Они могут включать снабжение резервным электропитанием, сооружение навеса или перегородок для предотвращения повреждений водой и т. д.

A.3.3.3.3 Вспомогательные практические методы

A.3.3.3.3.1 Основные практические методы

К основным практическим методам относятся следующие действия:

a) создание физических периметров безопасности для установления барьеров от несанкционированного доступа к оборудованию. На каждом барьере или границе необходимо предусмотреть необходимые средства управления доступом;

b) защита имущественных объектов от повреждений, вызванных угрозами среды, например, пожаром, водой, дымом, пылью, излучением и ударами;

c) выполнение и обеспечение исполнения персоналом процедур физической безопасности, которые были созданы для усиления средств физического контроля и контроля доступа;

d) установка резервных источников электроснабжения для устранения отдельных точек отказа;

e) защита всех внешних соединений от небрежного отношения или повреждений;

f) техническое обслуживание всего оборудования, включая оборудование регулирования условий окружающей среды, для обеспечения надлежащей эксплуатации;

g) создание процедур для контроля и подачи аварийного сигнала при возникновении угрозы физической безопасности или безопасности среды;

h) создание и проведение аудита процедур в отношении добавления, вывода из эксплуатации и списания всех имущественных объектов;

i) использование специальных процедур для защиты имущественных объектов, которые оказывают влияние на систему промышленной автоматики за пределами сети системы.

A.3.3.3.3.2 Дополнительные практические методы

К дополнительным практическими методами относятся следующие действия:

a) использование пристяжных тросов безопасности, закрываемых шкафов, защищенных входов в домашний офис, скрытие оборудования и снабжение имущественных объектов ярлыками и бирками;

b) использование настроек пароля для команд самозагрузки и входа в систему на компьютерах, расположенных за пределами пульта управления, зашифрованных файловых систем, ноутбуков, использующих тонкие клиенты и т. д.;

c) защита компьютерного оборудования, расположенного за пределами пульта управления, например, маршрутизаторов или брандмауэров, путем размещения его в закрытой среде;

d) укомплектование персоналом пультов управления. Эта мера часто является первоочередной мерой физической защиты. Следует использовать пульты управления для размещения информационных и технологических имущественных объектов;

e) возврат персоналом, увольняющимся из организации, оборудования в исправном рабочем состоянии;

f) использование системы слежения за оборудованием для определения его местоположения и лиц, ответственных за него;

g) защита от воздействия среды имущественных объектов, включая использование надлежащих корпусов для оборудования в местах, где оно может подвергаться воздействию пыли, высоких или низких температур, влажности и т. д.

A.3.3.3.4 Использованные ресурсы

Этот элемент частично основан на материалах [2], [23], [27], [31].

А.3.3.4 Элемент «Сегментация сети»

А.3.3.4.1 Описание элемента

Сегментация сети предполагает разделение ключевых имущественных объектов IACS на зоны с общими уровнями безопасности в целях управления рисками безопасности для достижения необходимого уровня безопасности зоны. Сегментация сети является важной контрмерой безопасности, применяемой совместно с другими уровнями защиты для снижения риска, связанного с IACS.

Современные IACS объединяются с бизнес-системами в пределах партнерских компаний и между ними. Несмотря на необходимость в возможности подключения и плотной компоновке, IACS не нуждаются в подавляющем большинстве данных, проходящих через корпоративные сети. Участие устройств IACS в передаче всего этого трафика увеличивает вероятность возникновения инцидента безопасности в системе. В соответствии с принципом наименьшего приоритета и использования информации только в служебных целях архитектура IACS должна быть спроектирована таким образом, чтобы ненужные пакеты связи отфильтровывались/удалялись и не попадали в устройства системы. Сегментация сети предназначена для разделения устройств на зоны общей безопасности, где применяются установленные методы обеспечения безопасности для достижения необходимого уровня безопасности. Целью является минимизация вероятности инцидента безопасности, угрожающего функционированию IACS. Разделение устройств на зоны не всегда означает их изоляцию друг от друга. Зоны безопасности соединяются кабелями, которые облегчают осуществление связи между сегментированными зонами безопасности.

Основным принципом безопасности является использование контрмер безопасности, соответствующих уровню риска. Сегментация сети IACS может не потребоваться, если уровень рисков безопасности является низким. Элемент управления рисками и реализации предоставляет дополнительную информацию в отношении управления рисками. Он должен быть рассмотрен до реализации контрмер по сегментации сети, рассмотренных в настоящем элементе CSMS.

А.3.3.4.2 Сегменты и зоны сети

В IEC/TS 62443-1-1 (раздел 6) приведены базовые модели и возможность обеспечения контекста для рассмотрения данной контрмеры. Сети сегментируются посредством использования определенного типа барьерного устройства, которое способно контролировать трафик через него. В сетях Интернет, использующих протокол TCP/IP, наиболее распространенными барьерными устройствами являются брандмауэры, маршрутизаторы и трехуровневые коммутаторы. Зачастую IACS состоят из нескольких сетей, использующих различные физические технологии и приложения. Такие сети, не основанные на протоколе TCP/IP, также используют барьерные устройства для разделения и сегментации передачи данных. К барьерным устройствам могут относиться автономные шлюзовые устройства или модули устройств IACS, интегрированные в сетевой интерфейс.

В то время, как размещение барьерного устройства в сети может создать новый сетевой сегмент и зону безопасности, зона безопасности может объединять множество сетевых сегментов. На рисунке 8 ниже показана возможная сегментированная архитектура для обычной IACS. На этом рисунке предпринята попытка показать, каким образом уровни функционального оборудования могут преобразовываться в физическое оборудование реальной IACS и логическую схему зоны. (Рисунок является довольно обобщенным и включает не все сетевые устройства, необходимые для реальной установки).

Важно не путать функциональные уровни базовой модели с уровнями безопасности зон безопасности. Несмотря на то, что обычно оборудование более низкого уровня играет большую роль в безопасности автоматизированного производства, использование стратегии сегментации, полностью соответствующей уровням оборудования, может быть нецелесообразным или невозможным.

На этом рисунке зона управления включает в себя оборудование с общим целевым уровнем безопасности. На рисунке показан сегмент сети управления технологическим процессом на основе протокола TCP/IP (PCN), сегмент фирменной сети автоматического регулирования (RCN) и сегмент фирменной сети полевых устройств (FDN). Эти сети соединены с оборудованием уровня 0, 1, 2 и 3, описанном в базовых моделях в IEC/TS 62443-1-1 (подпункт 5.2). Барьерные устройства каждого из этих сетевых сегментов регулируют вход и выход из соответствующих сегментов.



Рисунок А.8 — Соответствие между базовой архитектурой и примером сегментированной архитектуры

А.3.3.4.2.2 Зона управления

Для систем промышленной автоматики и контроля с низким уровнем риска может быть необходимым применение сегментации сети в качестве контрмеры, что потребует создания отдельной зоны управления. Однако для систем со средним или высоким уровнем риска сегментация сети является контрмерой, обеспечивающей очень значительное снижение риска.

Общепринятой передовой практикой является использование барьерного устройства, например, брандмауэра, для управления передачей данных по кабелю, соединяющему зону управления с бизнес-зоной, как показано на рисунке А.8.

Общепринятые стратегии фильтрования с помощью барьерных устройств:

a) базовая конфигурация барьерного устройства должна отклонять любую передачу данных по умолчанию и разрешать передачу данных в качестве исключения только для выполнения критических потребностей бизнеса. Это применяется как к периодической интерактивной связи пользователя по кабелю, так и к непрерывной межзадачной связи между устройствами в этих двух зонах. По возможности передача данных должна фильтроваться портами и сервисами между согласованными парами IP для устройств, передающих данные по кабелям;

b) порты и сервисы, часто используемые в качестве векторов атаки, не должны открываться через барьерное устройство. Если сервис необходим в соответствии с экономическим обоснованием, необходимо использовать дополнительные контрмеры для компенсации риска. Например, входной http, который является обычным вектором атаки, может быть необходим для выполнения важной функции бизнеса. Дополнительные компенсирующие контрмеры, например, блокирование входных скриптов и использование прокси-сервера http, помогут уменьшить риск при открытии этого порта и сервиса с высоким уровнем риска;

c) чем меньше количество портов и сервисов, открываемых через барьерное устройство, тем лучше. Технологий передачи данных, которые требуют большого количества открываемых портов, необходимо избегать.

Барьерное устройство может служить хорошим автоматизированным инструментом выполнения практических методов обеспечения безопасности в зоне управления, например, задерживания входящих электронных сообщений и передачи данных в/из Интернета.

A.3.3.4.2.3 Демилитаризованная зона (DMZ)

В системах промышленной автоматики и контроля с высоким уровнем риска использование DMZ совместно с зоной управления обеспечивает дополнительную возможность снижения риска между бизнес-зоной с низким уровнем безопасности и зоной управления с высоким уровнем риска. Уровень безопасности для DMZ выше, чем у бизнес-зоны, но ниже, чем у зоны управления. Функцией этой зоны является ликвидация или значительное снижение прямой передачи данных между зоной управления и бизнес-зоной.

В DMZ должны быть расположены устройства, которые функционируют как устройства связи или буферы между устройствами бизнес-зоны и зоны управления. Передача данных настраивается между устройством в бизнес-зоне и DMZ. Затем устройство в DMZ передает информацию получающему устройству в зоне управления. В идеальном случае порты и сервисы, используемые между устройством в бизнес-зоне и DMZ, отличаются от портов и сервисов, используемых между устройством DMZ и конечным устройством зоны управления. Это снижает вероятность прохождения вредоносного кода или злоумышленника по комбинированному кабелю, соединяющему бизнес-зону с зоной управления.

Стратегии фильтрования, перечисленные выше для зоны управления, применимы также и для DMZ. Однако некоторые более рискованные протоколы, например, telnet, могут допускаться для облегчения управления устройствами в DMZ и зонах управления.

Есть несколько случаев, в которых использование DMZ может иметь преимущества. Они включены в настоящий стандарт для иллюстрирования концепций безопасности. Приведенный перечень не является исчерпывающим или подробным перечнем способов применения DMZ:

a) минимизация количества лиц, имеющих прямой доступ к устройствам зоны управления

К серверам с архивными данными часто имеют доступ лица, находящиеся в местной сети LAN в бизнес-зоне. Вместо того, чтобы размещать сервер с архивными данными в зоне управления и разрешать прямой доступ к этому устройству из бизнес-зоны большому числу пользователей, уровень безопасности зоны управления можно поддерживать на высоком уровне, разместив сервер в зоне DMZ;

b) обеспечение более высокого уровня безопасности для важных устройств IACS

В случае сервера с архивными данными, указанном выше, одним из вариантом может быть размещение сервера в местной сети LAN, где расположено большинство пользователей. Это снизит число людей, которым требуется доступ к сети PCN. Однако, поскольку бизнес-зона является зоной с низким уровнем риска, сервер с архивными данными будет находиться в менее надежной среде. Потенциальная угроза для сервера будет выше;

c) компенсация задержек коммутации

Зона DMZ обеспечивает дополнительную защиту для важных устройств IACS, коммутация которых проводится с задержкой в ожидании результатов тестов коммутационной совместимости от поставщика приложения;

d) обеспечение повышения безопасности для зоны управления путем перемещения устройств управления на более высокий уровень безопасности

DMZ хорошо подходит для размещения таких устройств, как антивирусные серверы и серверы управления патчами. Эти устройства могут использоваться для управления применением модулей безопасности к зоне управления и устройствам DMZ с более высоким уровнем контроля, что позволяет избежать прямого соединения зоны управления с высоким уровнем безопасности с серверами, которые могут взаимодействовать с сотнями устройств.

A.3.3.4.2.4 Зона системы безопасности

Некоторые IACS могут использовать набор блокировок безопасности, основанных на применении реле или микропроцессоров. Для микропроцессорного логического устройства SIS могут потребоваться другие методы обеспечения безопасности по сравнению с теми, что применяются в зоне управления. Для этой зоны необходимо определить целевой уровень безопасности, для достижения которого реализуются соответствующие контрмеры.

A.3.3.4.2.5 Изолированная система промышленной автоматики и контроля

Риск, связанный с системой промышленной автоматики и контроля, может быть слишком велик, чтобы допускать какую-либо возможность угрозы со стороны внешнего агента. Объект может принять решение об отсоединении всех кабелей между зоной управления и другими зонами. Необходимо серьезно рассмотреть возможность применения этой стратегии сетевой сегментации.

Предприятия, решающие применить подход в отношении изоляции, не избавляются автоматически от всех рисков. Даже в этом случае может существовать большая уязвимость, которая может быть использована локально. Для снижения рисков, оставшихся после изоляции IACS от бизнес-зоны, должны применяться соответствующие уровни кибер- и физической защиты.

A.3.3.4.3 Архитектура сегментации SCADA

Выше была рассмотрена сегментированная архитектура для IACS, обычно применяемой на одном работающем объекте. Сегментация в равной степени может применяться и для систем типа SCADA. На рисунке A.9 показан возможный подход к сегментации для этого типа архитектуры. Несмотря на то, что зона DMZ и зона системы безопасности, рассмотренные для IACS одного работающего объекта, не показаны из-за недостатка места, они также могут применяться в архитектуре SCADA.

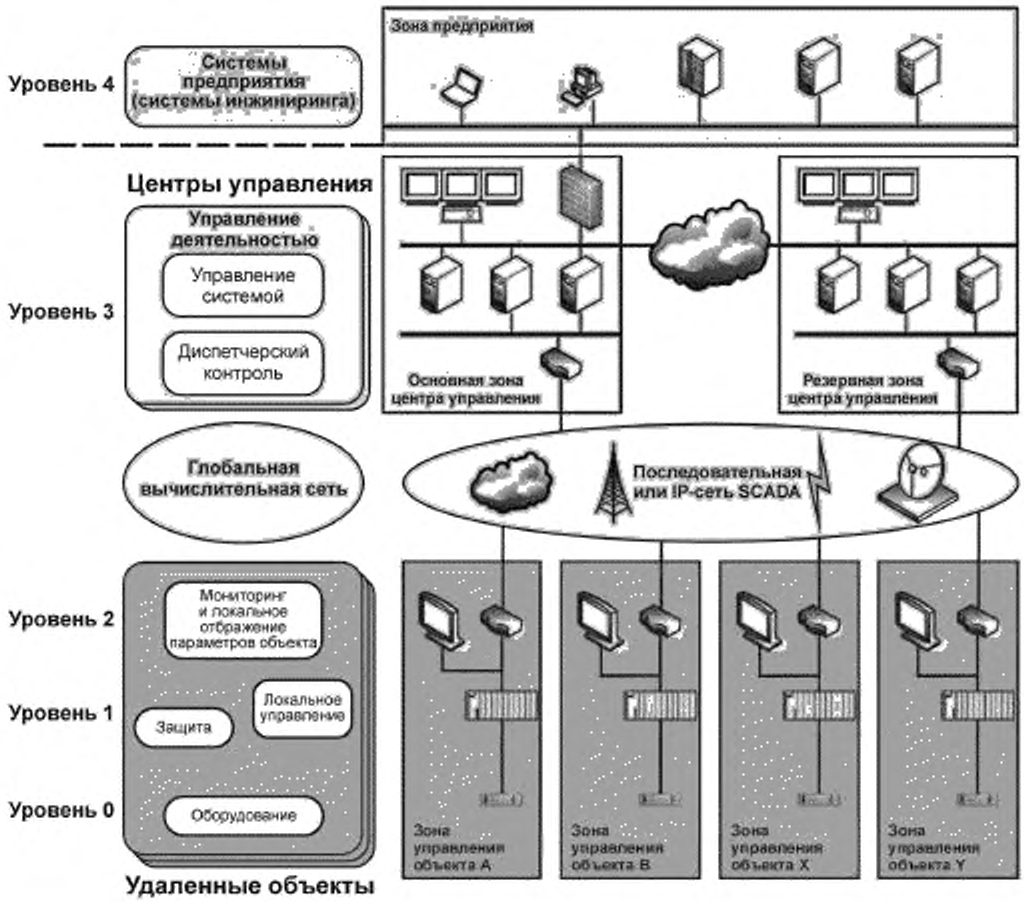


Рисунок А.9 — Соответствие между базовой архитектурой SCADA и примером сегментированной архитектуры

А.3.3.4.4 Предлагаемые практические методы

А.3.3.4.4.1 Основные практические методы

К основным практическим методам относятся следующие действия:

a) использование барьерных устройств, например, брандмауэров, для сегментации устройств IACS с высоким уровнем риска на зоны управления;

b) использование шлюзовых устройств или внутренних барьерных устройств в устройствах IACS для отделения сетей автоматического регулирования от PCN;

c) использование разумных методов управления изменениями в конфигурации барьерных устройств;

d) отсоединение IACS с высоким уровнем риска от бизнес-зоны.

А.3.3.4.4.2 Дополнительные практические методы

К дополнительным практическим методам относятся следующие действия:

a) применение дополнительных барьерных устройств в зоне управления для дополнительной сегментации сети;

b) применение общего профиля безопасности с центральным управлением на всех барьерных устройствах зоны управления;

c) использование архитектуры сегментации с помощью зоны DMZ;

d) проведение автоматизированной проверки верного кофигурирования барьерных устройств в соответствии с проектным заданием.

А.3.3.4.5 Использованные ресурсы

Данный элемент был частично основан на материалах [1].

А.3.3.5 Элемент «Контроль доступа: администрирование учетных записей»

А.3.3.5.1 Общее описание контроля доступа

Контроль доступа предназначен для определения того, кто и какие ресурсы могут получить доступ в помещение или системы, а также какой тип доступа предоставляется. Ненадлежащее использование данных и систем может иметь серьезные последствия, включая нанесение вреда человеческой жизни, экологический ущерб, финансовые убытки и ущерб для корпоративной репутации. Эти риски возрастают, когда персонал имеет излишне обширный доступ к данным и системам. Очень важно, чтобы политика безопасности, содержащая правила и процедуры контроля доступа, была четко сформулирована и доведена до всего персонала (т. е. работников, совместных предприятий, сторонних подрядчиков и временных работников).

Одним из наиболее важных элементов безопасности для любой компьютерной системы является создание разумного и уместного набора процедур контроля доступа. Существует три ключевых аспекта, связанных с контролем доступа: администрирование учетных записей, аутентификация и авторизация.

Каждый из них описан отдельно в соответствующем подпункте настоящего стандарта. Однако все три аспекта должны разрабатываться совместно для создания разумной и надежной стратегии контроля доступа.

В каждом из трех аспектов контроля доступа необходимо установить правила для подтверждения контроля доступа пользователя к системам и данным. Такие правила обычно применяются к группам пользователей. Они должны иметь доступ к системам и данным, которые должны соответствовать определенным бизнес-требованиям, однако доступ не должен предоставляться, если отсутствует определенная бизнес-цель.

Существуют правила, которые выполняются административными способами, и правила, которые выполняются автоматически путем использования технологий. Оба вида правил должны быть включены в общую стратегию контроля доступа. Примером административного правила является удаление учетной записи работника или подрядчика после их ухода из организации. Примером правила, выполняемого путем применения технологии, является подключение удаленных пользователей к корпоративной сети для использования VPN.

Помимо правил, существуют также процедуры физической и кибербезопасности, которые применяются совместно для создания общей инфраструктуры безопасности системы. Процедуры физической безопасности включают такие меры, как закрываемые помещения, где располагается оборудование пользовательского интерфейса. В А.3.3.3 настоящего стандарта приведено базовое описание элементов физической безопасности, которые относятся к кибербезопасности.

Существует два аспекта контроля доступа: в реальном времени и в автономном режиме. Зачастую автономному контролю доступа к IACS уделяется недостаточно внимания. Автономный контроль, описанный в настоящем стандарте как администрирование учетных записей, является первой стадией процесса и включает определение привилегий пользователей и необходимых им ресурсов. Они основаны на роли пользователя и выполняемой работе. Автономный контроль также включает стадию одобрения ответственной стороной до того, как производится конфигурация учетной записи для предоставления доступа.

А.3.3.5.2 Описание элемента



Рисунок А.10 — Контроль доступа: администрирование учетных записей

Администрирование учетных записей, одна из трех составляющих контроля доступа, приведенных на рисунке А.10, является методом, связанным с начальной настройкой допуска и привилегий доступа к конкретным ресурсам в сети или системе и периодического просмотра этих допусков и привилегий. Оно может быть связано с физическим доступом к ресурсам. Администрирование учетных записей в среде IACS выходит за пределы традиционного определения доступа к учетной записи конкретного пользователя в операционной системе. В среде IACS учетные записи в большей степени относятся к ролям по выполнению функций на конкретной машине, а не к данным, к которым они имеют доступ. Роль пользователя в организации может измениться с течением времени, поэтому процесс администрирования может более часто использоваться для учетных записей системы. Привилегии зачастую включают доступ к файловым директориям, количество часов доступа и количество выделенного места для хранения. Роль, присваиваемая на уровне приложения для учетной записи, определяется и осознается

на стадии администрирования. Это происходит в несколько шагов: выявление ресурсов, необходимых для выполнения служебных функций работника, независимое утверждение доверенным лицом и настройка/конфигурация компьютерной учетной записи, которая автоматически предоставляет ресурсы при необходимости.

Помимо задачи создания учетных записей и присваивания ролей пользователям на уровне операционной системы, многие производственные приложения требуют присвоения дополнительных ролей. Системные администраторы в системе промышленной автоматики и контроля должны иметь достаточную степень квалификации и надежности для выполнения функций по администрированию учетных записей в работающих приложениях по управлению оборудованием. Процесс управления изменениями для внесения изменений в учетные записи должен четко определять временные ограничения, которые должны выполняться в связи с рисками безопасности во время определенных последовательностей операций управления.

А.3.3.5.3 Аспекты администрирования учетных записей

А.3.3.5.3.1 Общие положения

При разработке программы администрирования учетных записей необходимо включить в нее все рассматриваемые системы, не ограничиваясь исключительно традиционным оборудованием компьютерного зала.

А.3.3.5.3.2 Правила управления доступом пользователя к системам, данным и конкретным функциям

Каждая организация должна установить правила управления доступом пользователя к системам, данным и функциям. Эти правила должны быть основаны на риске для системы и ценности информации. Правила должны быть распространены среди персонала.

А.3.3.5.3.3 Стандартный процесс администрирования

Для создания учетных записей необходимо следовать стандартному административному процессу. Несмотря на то, что для одной организации может быть более экономически целесообразно предусмотреть функцию администрирования учетных записей для всех компьютерных систем в компании, в IACS и IT-системах за административный контроль создания учетных записей и процесса их ведения может отвечать другой персонал. Это зачастую связано с различным набором рисков, связанных с этими системами. Утверждение учетных записей также может потребовать утверждения контролером, ознакомленным с задачами и работой IACS.

А.3.3.5.3.4 Ролевые учетные записи

Для создания таких учетных записей необходимо следовать стандартному административному процессу. Учетные записи являются ролевыми и предоставляют пользователю привилегии и доступ к ресурсам, которые необходимы для выполнения конкретной служебной функции.

А.3.3.5.3.5 Минимальные привилегии

Пользователям должны быть предоставлены минимальные привилегии и разрешения, необходимые для выполнения их задач. Доступ должен предоставляться, исходя из необходимости выполнения конкретной служебной функции. Ролевые привилегии должны учитывать особые требования к установке ПО, конфигурирующим сервисам, потребности в обмене файлами и необходимость в удаленном доступе.

А.3.3.5.3.6 Разделение обязанностей

Процесс администрирования учетных записей включает принципы разделения обязанностей, при этом утверждение и осуществление конфигурирования учетной записи проводится разными лицами. Этот принцип обеспечивает дополнительный уровень защиты, чтобы один работник не мог создать угрозу для системы.

А.3.3.5.3.7 Определение отдельных пользователей

Должна существовать возможность идентификации каждого пользователя по отдельным учетным записям, если только такие учетные записи не связаны с рисками по охране труда, технике безопасности и охране окружающей среды. В таких случаях необходимо применять другие средства контроля физической безопасности для ограничения доступа. Доступ необходимо контролировать с помощью аутентификации (т. е. ID пользователя и пароля, личных идентификационных номеров (PIN) или символов). Такие персональные данные не должны предоставляться кому-либо, за исключением определенных особых ситуаций. Исключением является пульт управления, на котором операторы функционируют в качестве единой рабочей команды. В этой ситуации каждый в команде может использовать одни и те же регистрационные данные. (Дополнительно эта тема рассматривается в А.3.3.6.). На случай, если работник забыл пароль, должна существовать альтернативная процедура идентификации.

А.3.3.5.3.8 Авторизация

Доступ должен предоставляться с разрешения соответствующего менеджера (из ответственной компании или партнерской организации). Одобрение проводится контролерами, ознакомленными с производственными/эксплуатационными задачами, и обучением, которое работник прошел для выполнения этой роли.

А.3.3.5.3.9 Ненужные учетные записи

Учетные записи являются средством контроля доступа к системе, поэтому необходимо осуществлять деактивацию, приостановление или удаление учетных записей и аннулирование разрешений на доступ, когда необходимость в таких записях отпадает (например, при смене должности, увольнении и т. д.). Эти действия должны предприниматься соответствующим менеджером после того, как пропадает необходимость в учетной записи.

А.3.3.5.3.10 Разрешение на просмотр учетных записей

Необходимость доступа к критически важным системам должна напрямую подтверждаться на регулярной основе. Созданные учетные записи должны периодически просматриваться, чтобы удостовериться, что они все еще используются, роль и требования к доступу являются верными, а пользователь авторизован и имеет минимальные требуемые разрешения. Неактивные или ненужные учетные записи должны удаляться. Если учетная

запись не используется в течение продолжительного времени, необходимость в ней должна непосредственно подтверждаться владельцем или заказчиком записи.

А.3.3.5.3.11 Учет записей

Одной из основных функций администрирования учетных записей является учет всех отдельных учетных записей. Учет ведется для всех учетных записей, включая информацию о работнике, предоставленных разрешениях и ответственном менеджере.

А.3.3.5.3.12 Управление изменениями

Процесс управления изменениями для администрирования учетных записей должен четко определять любые временные ограничения, которым необходимо следовать из-за рисков безопасности при внесении изменений во время определенных производственных последовательностей. Эти изменения имеют такое же значение, как и изменения в технологическом процессе, ПО и оборудовании. Процесс администрирования учетных записей должен быть объединен со стандартными процедурами управления безопасностью технологического процесса и включать в себя действия по утверждению и документированию. Лица, утверждающие учетные записи для выполнения производственных/эксплуатационных функций, могут отличаться от лиц, утверждающих пользователей IT-систем. Утверждение проводится контролерами, ознакомленными с задачами производства/эксплуатации и конкретным обучением, которое работник прошел для выполнения конкретной функции.

А.3.3.5.3.13 Пароли по умолчанию

Многие системы управления имеют пароли по умолчанию, которые используются при настройке и подготовке системы к использованию. Эти пароли учетных записей часто широко известны или могут быть легко определены из опубликованной литературы или других источников. Пароли по умолчанию необходимо заменить сразу после настройки и до подключения к системе.

А.3.3.5.3.14 Аудит администрирования доступа

Необходимо проводить периодическую проверку соответствия информации об администрировании учетных записей. Это обеспечивает выполнение владельцами документов или информации соответствующих политик, стандартов или других требований, установленных организацией.

А.3.3.5.4 Вспомогательные практические методы

А.3.3.5.4.1 Основные практические методы

К основным практическим методам относятся следующие действия:

a) предоставление минимальных привилегий и разрешений пользователям, необходимых для выполнения их задач. Доступ должен предоставляться, исходя из необходимости выполнения конкретной служебной функции;

b) контроль идентификации и доступа для каждого пользователя с помощью подходящего способа аутентификации (например, ID пользователя и пароля). Такие регистрационные данные (т. е. пароли, PIN и/или символы) не сообщаются никому, за исключением конкретных особых ситуаций;

c) создание альтернативного процесса идентификации в случае, если работник потерял регистрационные данные или забыл пароль;

d) предоставление, изменение или прекращение доступа с разрешения соответствующего менеджера (из организации, организации-подрядчика или из сторонней организации). Должен вестись учет всех записей, включая информацию о работнике, разрешениях и ответственном менеджере;

e) приостановление или удаление всех учетных записей и отмена разрешений, как только учетные записи становятся ненужными (например, при смене должности);

f) регулярный просмотр всех созданных учетных записей, чтобы удостовериться, что они все еще используются и требуют доступа к критически важным системам;

g) подтверждение необходимости в учетных записях соответствующим менеджером, если учетные записи не используются в течение продолжительного времени;

h) незамедлительная смена паролей по умолчанию;

i) письменное согласие всего персонала (т. е. работников, совместных предприятий, сторонних подрядчиков и временных работников) на выполнение политики безопасности, включая политики контроля доступа.

А.3.3.5.4.2 Дополнительные практические методы

К дополнительным практически методам относятся следующие действия:

a) использование инструментов (т. е. инициализации и управления персональными данными) управления процессом создания, приостановления и удаления учетных записей. Система инициализации также управляет документооборотом при одобрении, с помощью которого владелец бизнеса одобряет доступ, включая регистрацию. Это также позволяет автоматизировать процесс создания/приостановления учетных записей в целевых системах;

b) увязка процесса администрирования учетных записей с кадровым процессом таким образом, чтобы работник мог изменить триггерные просмотры и обновление учетных записей;

c) определение и документирование ролей в приложениях/привилегий пользователей (т. е. служебных функций, увязанных с ролями к приложениям и разрешениями на доступ для каждой роли) владельцем информации о приложении или заместителем;

d) уделение особого внимания пользователям с привилегированным доступом (т. е. более частые просмотры и проверка биографии);

e) предоставление пользователям разрешения на несколько учетных записей, исходя из их конкретной служебной роли на конкретный момент времени. Работник будет использовать учетную запись системного админи-

стратора для обновления приложения на конкретном оборудовании, но ему также понадобится учетная запись оператора для использования и проверки приложения.

А.3.3.5.5 Использованные ресурсы

Этот элемент основан частично на материалах [6].

А.3.3.6 Элемент «Контроль доступа: аутентификация»

А.3.3.6.1 Описание элемента

Примечание — Для получения дополнительной информации по элементу «Контроль доступа» см. А.3.3.5.1.

Аутентификация, вторая из трех составляющих контроля доступа, приведенных на рисунке А.11, является методом определения сетевых пользователей, хостов, приложений, сервисов и ресурсов для компьютеризированной операции для предоставления им необходимых разрешенных прав и обязанностей. Метод использует комбинацию факторов идентификации или регистрационных данных. Аутентификация является необходимым условием предоставления доступа к ресурсам системы.



Рисунок А.11 — Контроль доступа: аутентификация

С аутентификацией в среде IACS связано несколько сложностей, не характерных для обычных ситуаций в IT. Существующие технологии IT аутентификации имеют несколько ограничений, которые недостаточно подходят для среды промышленной автоматики и контроля и могут в действительности привести к повышению рисков, связанных с охраной труда, техникой безопасности и охраной окружающей среды, за счет повышения рисков кибербезопасности.

В среде IACS важно удостовериться, что нужные люди имеют доступ к необходимой информации и системам, и аутентификация не мешает им выполнять свою работу. Неспособность аутентифицировать действительно существующего пользователя может иметь последствия с точки зрения охраны труда, техники безопасности и охраны окружающей среды, если пользователь не сможет выполнять свою работу в критической ситуации. В среде IACS огромное внимание уделяется совмещению мер физической аутентификации с методами электронной аутентификации.

Физическое местоположение пользователя может оказывать существенное влияние на уровень риска доступа. Например, пользователь, подключающийся к системе из здания, в котором существуют службы охраны и система считывания пропусков на входе, связан с более низким уровнем риска, чем пользователь, подключающийся к системе из другого региона мира. Стратегия аутентификации включает совместное использование средств контроля физической и кибербезопасности для контроля общего риска. Стратегия четко определяет требования к аутентификации для особых ситуаций.

Существует несколько типов стратегий аутентификации с различной степенью строгости. Строгие методы аутентификации включают методы точного определения пользователей. Простые методы аутентификации включают методы, которые можно легко обойти для получения нежелательного доступа к информации.

Физическое местоположение пользователя может оказывать существенное влияние на риск доступа к IACS. Аутентификация для этих случаев рассмотрена в А.3.3.6.2—А.3.3.6.4.

А.3.3.6.2 Аутентификация для локальных пользователей

Очень важно, чтобы только обученные и уполномоченные работники могли выполнять действия на станциях HMI системы промышленного контроля, например, операторских станциях управления. Во многих отраслях управление оборудование осуществляется с пультов управления, укомплектованных несколькими операторами. Эти операторы часто работают как команда и выполняют действия на нескольких станциях HMI в рамках обычных служебных функций. Часто применяются общие учетные записи для команды операторов. Если на станциях HMI не предусмотрены экономически целесообразные, надежные и строгие схемы аутентификации, рекомендуется использовать средства физического контроля для обеспечения того, что только уполномоченные лица выполняли действия на станциях HMI пульта управления. Управление доступом к пультам управления должно осуществляться путем применения технологий контроля доступа в сочетании с административными процедурами. Следует учиты-

вать последствия с точки зрения охраны труда, техники безопасности и охраны окружающей среды при разработке процедур контроля доступа.

А.3.3.6.3 Аутентификация для удаленных пользователей

Удаленным пользователем является пользователь, находящийся за пределами периметра рассматриваемой зоны безопасности.

Пример — Удаленным пользователем может быть лицо, находящееся в офисе в том же здании, лицо, подключающееся по WAN, или лицо, подключающееся по сети общественной инфраструктуры.

Методы физического или административного контроля, на основе визуальной аутентификации, не подходят для удаленных интерактивных пользователей. Однако, существует множество технологических схем аутентификации, которые могут использоваться. Важно использовать схему аутентификации с уместным уровнем строгости для верного определения удаленного интерактивного пользователя. Производственная деятельность с низким потенциалом возникновения инцидентов в сфере охраны труда, техники безопасности и охраны окружающей среды, имеющая незначительные финансовые последствия, может быть защищена с использованием нестрогих методов аутентификации, например, с помощью простого ID пользователя и пароля. Однако производственная деятельность, имеющая серьезные финансовые последствия или последствия с точки зрения охраны труда, техники безопасности и охраны окружающей среды, должна быть защищена путем использования технологий строгой аутентификации. Для этих типов деятельности рекомендуется, чтобы система была спроектирована таким образом, чтобы удаленным пользователям не разрешалось осуществлять функции управления, а разрешался бы только мониторинг.

А.3.3.6.4 Аутентификация для межзадачной связи

Предыдущие пункты были посвящены интерактивным пользователям. Не менее важным является применение подходящей схемы аутентификации для межзадачной связи между серверами приложений или между серверами и управляемыми устройствами. Интерфейс связи должен использовать методы проверки того, что устройство, посылающее запрос, действительно является устройством, выполняющим соответствующую задачу. К способам, с помощью которых критически важные интерфейсы могут выполнить аутентификацию межзадачного взаимодействия между устройствами, относятся проверка адреса IP, проверка MAC, использование секретного кода или зашифрованного ключа для проверки того, что запрос поступает от нужного устройства. Интерфейсы с низким уровнем риска могут использовать менее надежные способы аутентификации. Примером ненадежного взаимодействия является анонимный FTP для загрузки/выгрузки/сравнения программ между HMI системы управления и архивом данных.

А.3.3.6.5 Основания для аутентификации

А.3.3.6.5.1 Общие положения

При разработке программы контроля доступа необходимо включить в нее все рассматриваемые системы, не ограничиваясь только традиционным оборудованием компьютерного зала.

a) Определение стратегии аутентификации

Компании должны выработать стратегию или подход к аутентификации, определяющий используемый способ аутентификации;

b) Аутентификация всех пользователей перед использованием системы

Все пользователи должны пройти аутентификацию перед использованием запрашиваемого приложения. Аутентификация может включать методы физической аутентификации и кибераутентификации;

c) Создание надежных учетных записей для системного администрирования и/или конфигурирования приложений

Для всех учетных записей системного администрирования и конфигурирования приложений должны использоваться надежные ID пользователей и пароли. Системному администратору обычно не требуется быстрый доступ для выполнения системных задач на компьютерах. Более важным по сравнению с быстрым доступом является предотвращение выполнения системных задач необученным персоналом;

d) Локальное администрирование

В критически важных системах рекомендуется выполнять функции системного администрирования или конфигурирования приложений на локальном устройстве для уменьшения риска нарушения работы сети, что может привести к проблемам с управлением оборудованием. Системный администратор или менеджер приложений должен координировать все изменения с оператором конкретной зоны, чтобы не оказывать воздействия на производство во время конфигурирования.

А.3.3.6.5.2 Аутентификация для локальных пользователей

Если применяемая практика связана с риском задержки способности оператора по осуществлению быстрых корректирующих действий в производственной деятельности со станции управления HMI, обычные методы IT-аутентификации могут быть неприменимы. Для достижения надежной работы системы управления и быстрого реагирования необходимо комбинированное применение методов физического контроля и киберконтроля для получения наилучших результатов. Такие методы включают без ограничения:

- открываемые вручную замки (например, ключом или комбинацией) на дверях в помещения или шкафы, содержащие компоненты системы управления;
- автоматические замки (например, считыватели пропусков или карт);

- постоянное присутствие персонала на пульте управления;

- индивидуальная ответственность персонала пульта управления за предоставление доступа только уполномоченному персоналу и выполнение действий на операторских станциях управления только обученным персоналом.

Примеры распространенных IT методов, которые могут быть неприменимы в среде промышленной автоматики и контроля:

a) Отдельные ID пользователей и пароли для каждого оператора в команде

Во многих отраслях управление деятельностью осуществляется с пультов управления, на которых работает несколько операторов. Такие операторы зачастую работают как команда, и выполняют действия на нескольких станциях HMI в рамках выполнения обычных служебных функций. Требования регистрации, аутентификации и авторизации операторов при каждом использовании нового HMI увеличивает время реагирования на события;

b) Доступ к контроллерам и активным серверам директорий неместного домена для аутентификации учетной записи

Сетевые проблемы могут помешать своевременному входу при такой архитектуре;

c) Автоматическая блокировка доступа к учетной записи после определенного числа неудачных попыток входа

При определенных условиях, которые требуют быстрой реакции оператора, оператор может переволноваться и ввести неверный пароль. Если в этом случае пароль будет заблокирован, это может поставить под угрозу способность оператора разрешить ситуацию;

d) Надежные длинные пароли, состоящие из сочетания буквенных, числовых и специальных символов

Несмотря на то, что надежные пароли являются дополнительной мерой безопасности, на пультах управления требование ввода такого пароля может увеличить время реагирования со стороны оператора. Аналогичный уровень безопасности может быть достигнут физическими средствами, например, закрытой дверью или постоянным присутствием на пульте управления персонала, знающего уполномоченных операторов;

e) Изменение пароля после определенного количества дней

Последствия смены пароля схожи с последствиями применения надежных паролей — она может увеличить время реагирования на ситуацию, требующую быстрой реакции. Пароли необходимо менять при смене персонала, однако смена паролей после истечения определенного периода времени может быть неэффективной;

f) Использование режимов сохранения экрана с защитой паролем

Многие станции HMI предназначены для сообщения только об исключительных ситуациях. Оператор может не предпринимать никаких действий на операторской станции до появления предупредительного сигнала. Режимы сохранения экрана могут помешать оператору, заблокировав изображение управляемого объекта и увеличивая время реагирования на аварийную ситуацию.

A.3.3.6.5.3 Аутентификация удаленных пользователей

Как правило, удаленным пользователям нет необходимости быстро реагировать на ситуации, привычные для операторов. Кроме того, для удаленных пользователей вопрос контролируемости имеет большее значение, чем доступность. Поэтому часть практик, стандартных для IT-безопасности, также пригодится и для удаленных пользователей. К таким практикам относятся следующие:

a) Аутентификация всех удаленных пользователей на соответствующем уровне

Организация должна внедрить схему аутентификации с соответствующим уровнем строгости для положительной аутентификации удаленного интерактивного пользователя;

b) Регистрация и контроль всех попыток доступа к важнейшим системам

Система должна регистрировать все попытки доступа к важнейшим системам. Организация должна изучать такие попытки независимо от того, удались они или нет;

c) Деактивация учетной записи доступа после неудачных попыток удаленного входа в систему

После определенного количества неудачных попыток входа в систему дистанционным пользователем система должна деактивировать учетную запись пользователя на определенный период времени. Это позволяет обнаруживать агрессивные перехваты пароля в системе. Несмотря на то, что удаленным пользователям обычно не требуется быстро реагировать на рабочие ситуации, могут сложиться такие обстоятельства, например, в компьютерных залах или дистанционных объектах без присутствия персонала (например, системы SCADA, контролирующие электрическую систему распределения), в которых требуется быстрый доступ из удаленного объекта. В таких случаях деактивация учетной записи не может быть адекватной мерой. Каждая организация должна организовать аутентификацию дистанционных пользователей таким образом, который подходит под ее обстоятельства и уровень допустимости риска;

d) Требование повторной аутентификации после неактивности дистанционной системы

После определенного периода неактивности дистанционный пользователь должен пройти повторную аутентификацию, чтобы снова зайти в систему. Таким образом можно гарантировать, что учетная запись не остается открытой для доступа с дистанционного устройства. Несмотря на то, что дистанционным пользователям обычно не требуется подсоединяться к системе управления на длительный период времени, могут сложиться обстоятельства, например, в компьютерных залах или дистанционных объектах без присутствия персонала (например, системы SCADA, контролирующие электрическую систему распределения), в которых дистанционному оператору может потребоваться контролировать систему на протяжении длительного периода времени. В таких случаях требование

провести повторную аутентификацию не может быть адекватной мерой. Каждая организация должна организовать аутентификацию дистанционных пользователей таким образом, который подходит под ее обстоятельства и уровень допустимости риска.

Для дистанционных пользователей требуемый уровень аутентификации должен быть пропорционален риску, угрожающему системе, в отношении которой осуществляется попытка доступа. Простая аутентификация может применяться, если система не контролирует операции с высоким риском HSE. Для систем, в которых реализуются риски HSE, больше соответствует строгая аутентификация.

Примеры простой аутентификации:

- модемное соединение напрямую с устройствами промышленного контроля или сетями, в которых используются простая аутентификация с помощью идентификаторов пользователей и пароля;
- подсоединение устройств промышленного контроля или сетей через корпоративную сеть LAN или WAN, в которых используются простая аутентификация с помощью идентификаторов пользователей и пароля;
- использование системы аутентификации Microsoft Windows® с помощью идентификаторов пользователей и пароля на уровне приложений в устройствах промышленного контроля.

Примеры строгой аутентификации:

- использование двухфакторной аутентификации с помощью физического токена или смарт-карты, для которой требуется и наличие физического устройства и знание уникальной информации (например, персональный идентификационный номер, PIN-код), которой владеет пользователь;

Примечание — Уровень безопасности повышается благодаря защищенному вводу PIN-кода, например, когда PIN-код вводится с использованием надежного считывателя кодов, препятствующего работе клавиатурного перехватчика;

- аутентификация с использованием смарт-карт или биометрических данных;
- аутентификация пользователей в зависимости от их местоположения;
- модемное соединение с устройствами промышленного контроля или сетями, в которых используется посылка обратного вызова на заранее определенный телефонный номер;
- соединение устройств промышленного контроля или сетей к корпоративной сети LAN или WAN и использование смарт-карт или биометрической аутентификации;
- подключение домашних компьютеров к устройствам промышленного контроля или сетям с использованием VPN-соединения и двухфакторной аутентификации с помощью токена и PIN-кода.

A.3.3.6.5.4 Аутентификация для связи между задачами

Как правило, межзадачные соединения не контролируются напрямую, как например, интерактивные сессии с пользователями. Аутентификация межзадачных соединений в основном будет использоваться во время пуска промышленной операции и затем через регулярные промежутки времени. В системах должно быть реализовано определенное техническое решение для аутентификации каждого устройства или сети.

Примечание — В IEC/TR 62443-3-1 [6] приведено пояснение этих и других технологий. В нем описываются преимущества и недостатки, а также применимость к среде IACS.

A.3.3.6.6 Вспомогательные практические методы

A.3.3.6.6.1 Основные практические методы

К основным практическим методам относятся следующие действия:

a) установление стратегии или подхода, которые определяют метод используемой аутентификации.

Метод может варьироваться в зависимости от рисков, последствий, связанных с бизнес-процессом и чувствительностью данных;

b) освоение различных стратегий для подключения пользователей, находящихся в различных географических местоположениях (включая дистанционные объекты), или для устройств с особыми требованиями безопасности. Для установления общего уровня безопасности пользователя учитываются характеристики физической безопасности, взаимодействующие с характеристиками информационной безопасности;

c) аутентификация всех пользователей до предоставления права пользования определенным приложением. Это требование может быть отменено, если имеются компенсирующие средства физического контроля;

d) требование ручного ввода пользовательского идентификатора и пароля в качестве минимального уровня электронной аутентификации;

e) аутентификация межзадачного соединения через известный MAC и/или IP-адрес, специальный электронный ключ, имя устройства и т. п.

A.3.3.6.6.2 Дополнительные практические методы

Дополнительным практическим методом является авторизация пользователей внутри закрытого объекта, при которой используются защитные блокировки или устройства считывания идентификационных карт, для доступа к системам с более высоким уровнем риска по сравнению с рисками для дистанционного пользователя.

A.3.3.6.7 Использованные ресурсы

Данный элемент частично основан на материалах [6], [23].

A.3.3.7 Элемент «Контроль доступа: авторизация»

Дополнительная информация по элементу «Контроль доступа» приведена в A.3.3.5.1.



Рисунок А.12 — Контроль доступа: авторизация

Авторизация, третья составляющая контроля доступа, приведенная на рисунке А.12, представляет собой автоматизированную процедуру, выполняемую компьютерной системой, для предоставления доступа к ресурсам после успешной аутентификации пользователя и идентификации его связанной учетной записи доступа. Предоставленные права доступа определяются настройкой конфигурации учетной записи доступа на этапе администрирования учетной записи.

Некоторые стандартные процедуры авторизации, использованные в общем рабочем IT-пространстве, могут не подходить или не соответствовать IACS. Например, учетные записи доступа в стандартной IT-системе, в основном организуются на уровне пользователей с ограниченным набором назначенных ролей (т. е. стандартный администратор пользователей или систем). Обычно для каждого пользователя назначается одна роль. Доступ к учетным записям в стандартной системе IACS будет ролевым с большей гранулярностью разрешений (т. е. оператор, инженер, специалист по приложениям, разработчик и системный администратор). Для пользователей могут быть назначены множественные роли в зависимости от определенной должностной функции, которую они должны выполнять в определенное время. Возможно, пользователю потребуется войти в систему для работы с определенным устройством и отдельно для работы с приложением, чтобы авторизоваться и получить право вносить изменения в переменные управления системы промышленного контроля. Или же он должен будет выйти из системы и повторно зайти для выполнения задач системного администрирования на том же устройстве.

В настоящем подпункте приводится анализ средств управления, предназначенных для защиты информации и объектов от намеренного и неумышленного разрушения, изменения или раскрытия. Особое внимание уделяется мерам, позволяющим гарантировать, что аутентифицированные агенты (т. е. персонал, приложения, сервисы и устройства) имеют доступ к требуемым информационным объектам.

Чувствительная к раскрытию информация должна быть защищена способом, позволяющим и сохранить конкурентное преимущество, и защитить конфиденциальную информацию о сотрудниках.

Регламент авторизации, требуемый организацией, будет определять способ назначения ролей для определенных пользователей или групп пользователей и конфигурации привилегий для таких учетных записей доступа. Способность внедрения требуемой политики авторизации зависит от характеристик базовых систем, позволяющих различать функции и данные, требуемые для различных должностных ролей.

Таким образом, определение политики авторизации является интерактивной процедурой, в ходе которой организация определяет совершенную политику и затем принимает решение, насколько точно можно достигнуть цели, используя возможности ее систем и сети. При создании новой системы поддержка требуемой политики авторизации может быть элементом закупочной спецификации. При проектировании конфигурации новой сети можно добавлять такие технологии, как брандмауэры для дистанционных пользователей, чтобы создавать дополнительный уровень авторизации для важнейших устройств, описанный в А.3.3.7.1.

А.3.3.7.1 Аспекты авторизации

А.3.3.7.1.1 Общие положения

При разработке программы контроля доступа важно включать в сферу применения все системы, а не ограничиваться традиционными объектами компьютерного зала:

a) Политика авторизации

В политике авторизации необходимо установить правила, определяющие привилегии, разрешенные для учетных записей сотрудников, выполняющих различные роли. Такая политика должна быть оформлена документально и должна применяться в отношении всего персонала после аутентификации;

b) Методы логического и физического разрешения доступа к устройствам IACS

Разрешение на доступ к устройствам IACS должно быть логическим (правила, которые предоставляют и/или ограничивают доступ для известных пользователей в зависимости от их ролей), физическим (замки, камеры и прочие средства контроля, ограничивающие доступ к активной панели управления);

c) Доступ к информации или системам через учетные записи на базе ролей

Учетные записи должны быть с ролевым доступом для управления доступом к соответствующей информации или системам для роли такого пользователя. Последствия для системы безопасности являются важнейшим компонентом определения ролей.

A.3.3.7.1.2 Авторизация локальных пользователей

Во многих технологических процессах контроль операций осуществляется из компьютерных залов, в которых работает несколько операторов. Такие операторы выступают в качестве группы и выполняют операции на многочисленных HMI-станциях в рамках своих обычных должностных функций. Авторизация для выполнения определенных должностных функций обеспечивается приложением. Локальный пользователь получает доступ к определенным устройствам или операционным панелям в зависимости от учетной записи с ролевым доступом. Как правило, для каждого лица используются единый идентификатор пользователя и пароль. Такой командный подход к управлению компьютерным залом может конфликтовать со стандартной политикой и практикой IT-авторизации.

При разработке стратегии авторизации необходимо учитывать последствия, связанные с безопасностью. Для промышленных операций, характеризующихся высоким уровнем уязвимости, привилегии авторизации должны быть заданы на уровне устройства локального технологического управления. Для назначения привилегий не должен требоваться доступ к устройствам на уровне LAN или WAN. Таким образом соблюдается базовый принцип управления, позволяющий минимизировать потенциальные критические точки.

Конфигурация учетных записей доступа должна предусматривать предоставление минимальных привилегий, требуемых для роли. Должно быть организовано обучение для определения общих уровней квалификации в отношении каждой должностной роли. Необходимо избегать индивидуализации отдельных учетных записей в соответствии с уровнями квалификации сотрудников. Все пользователи, выполняющие одинаковую должностную функцию, должны пользоваться учетными записями, сконфигурированными для одной роли.

A.3.3.7.1.3 Авторизация дистанционных пользователей

Процесс авторизации дистанционных пользователей предусматривает функцию авторизации на устройстве конечного узла на уровне приложения. В критических средах управления на барьерном устройстве (файерволл или маршрутизатор) должна быть реализована стратегия дополнительной авторизации адреса для сети IACS. Когда пользователь авторизуется на барьерном устройстве, для него должны быть назначены права доступа на базе ролей, чтобы пользователь мог лишь попытаться осуществить соединение с заранее назначенными устройствами в сети IACS. Вход в систему на конечном узле должен обеспечивать привилегии пользователя для выполнения функций на устройстве. Такой дополнительный уровень авторизации адреса должен предусматриваться для объектов с высоким уровнем уязвимости.

Учетные записи на основе ролей должны учитывать географическое местоположение учетной записи. Лицо может использовать одну учетную запись при работе на площадке и другую при подключении из дома, когда локальному персоналу требуется его помощь. Такая практика должна быть четко определена в административных процедурах. Соответствие административным процедурам должно быть основано на контроле действий отдельных пользователей.

A.3.3.7.2 Вспомогательные практические методы

A.3.3.7.2.1 Основные практические методы

К основным практическим методам относятся следующие действия:

a) разрешение доступа к устройствам IACS с логическими средствами контроля (правила, которые предоставляют или ограничивают доступ для известных пользователей в зависимости от их ролей) и/или физическими средствами контроля (замки, камеры и прочие средства контроля, ограничивающие доступ к активной панели управления);

b) регистрация и контроль всех попыток доступа к важнейшим компьютерным системам, в том числе успешные и неудачные.

A.3.3.7.2.2 Дополнительные практические методы

К дополнительным практическим методам относятся следующие действия:

a) защита сетевых соединений между организацией и другими организациями через управляемый файервол;

b) использование прокси-сервера аутентификации для всего исходящего доступа к сети Интернет;

c) предоставление доступа для дистанционного пользователя через подключение модема на устройстве промышленного контроля только в случае необходимости;

d) использование скрытого доступа при выполнении задач с высоким уровнем риска (например, промышленные операции с последствиями для сферы HSE или несущие в себе критические бизнес-риски);

e) отделение данных с высоким уровнем чувствительности и/или бизнес-последствиями от прочей внутренней информации таким образом, чтобы действующие средства контроля авторизации могли ограничивать доступ к такой информации;

f) отделение бизнес-сети от сети IACS с устройством контроля доступа и ограничение пользовательского доступа к важнейшим объектам по обе стороны.

A.3.3.7.3 Использованные ресурсы

Данный элемент частично основан на материалах [6], [23], [27], [30], [43].

А.3.4 Группа элементов «Внедрение»

А.3.4.1 Описание группы элементов

Третья группа элементов в этой категории называется «Внедрение». Этот элемент внутри группы затрагивает вопросы, связанные с внедрением CSMS. На рисунке А.13 представлено четыре элемента группы:

- управление рисками и принятие мер;
- разработка и обслуживание системы;
- управление документацией и информацией;
- планирование действий и реагирование при происшествиях.



Рисунок А.13 — Графическое представление группы элементов: Внедрение

А.3.4.2 Элемент «Управление рисками и принятие мер»

А.3.4.2.1 Описание элемента

Основой любой системы CSMS или программы безопасности является поддержание риска на допустимом уровне. Управление риском и принятие мер затрагивает такие вопросы, как отбор, разработка и принятие мер безопасности, соизмеримых с уровнем риска. При этом в них может учитываться свойственная им более надежная концепция промышленной безопасности, использование продуктов с внутренне присущими возможностями надежной защиты, контрмеры ручного и процедурного обеспечения безопасности, а также основанные на технологии контрмеры для предотвращения или снижения риска инцидентов, связанных с безопасностью.

Несмотря на то, что риск невозможно устранить навсегда, им можно управлять. В этом подпункте описывается метод измерения риска и управления риском через внедрение разнообразных контрмер по обеспечению безопасности, позволяющих снизить вероятность возникновения инцидента или масштаба последствия такого инцидента.

В большинстве случаев для измерения риска используются такие понятия как размер ущерба и/или общественное сознание. Несмотря на то, что оценка производственных потерь в результате инцидента, связанного с информационной безопасностью, не составит труда, невозможно установить точную стоимость происшествия, приведшего к телесному повреждению или смерти человека. Компании должны определить свои границы допустимости риска на случай определенных происшествий и использовать данную стратегию для управления риском.

А.3.4.2.2 Построение системы управления риском и принятия мер

Поскольку устранение всех рисков обычно является непрактичным или невозможным, организации должны обращать особое внимание на наиболее важные приложения и инфраструктуры, чтобы смягчить риск до приемлемого уровня. Когда принимается решение о необходимых контрмерах, решается задача уравновешивания риска и ущерба. Решения должны приниматься на основе оценки рисков и оформляться документально, чтобы служить основой для будущего планирования и реагирования.

Организации должны проводить анализ результатов оценки рисков, устанавливать стоимость мероприятий по снижению каждого риска, сравнивать стоимость с риском наступления происшествия и выбирать такие контрмеры, стоимость которых меньше потенциального риска. Учитывая, что устранение всех рисков может оказаться непрактичным или невозможным, необходимо сначала сосредоточить усилия на наиболее важных приложениях и инфраструктурах. Часто одни и те же риски наступают в более, чем одном месте. Имеет смысл подобрать стандартный набор контрмер, которые могут использоваться в более, чем одной ситуации, и затем определить, когда следует их применять. Такой подход позволит организации использовать общие решения и снижать расходы на разработку и внедрение мер, таким образом повышая уровень защищенности организации. Один из способов подразумевает разработку общей системы внедрения мер, которая включает в себя оценку рисков, определение уровня допустимости риска, оценку и выбор контрмер и стратегии действий по снижению рисков.

Исходя из предположения, что в каждой организации будет отличный уровень допустимости риска, определяемый нормативами, бизнес-двигателями и ключевыми значениями, можно заключить, что уровень допустимости риска организации в отношении инцидентов с IACS определяет объем работ, которые организация готова провести для снижения уровня риска до приемлемого уровня. Если организация имеет низкий уровень риска, она может быть готова затратить большее количество финансовых и/или человеческих ресурсов в целях повышения уровня обеспечения защиты IACS.

В таблице А.2 показана чувствительность организации к различным типам рисков, а различные последствия разделены на категории высокого, среднего и низкого уровня. Когда такие категории последствий рассматриваются в совокупности с вероятностью возникновения инцидента, как показано в таблице А.1, формируется матрица категорий последствий и вероятностей инцидента. При отсутствии аналитического способа количественной оценки вероятности и последствия может быть целесообразным просто устанавливать количественные уровни риска в точках пересечения в матрице: низкий, средний и высокий. Такие уровни риска отражают чувствительность организации к рискам, как показано в таблице А.3. Под такими уровнями подразумеваются пороги допустимости риска, на которых строится стратегия принятия мер по снижению рисков. Это простой способ выражения отношения организации к риску.

Стратегия снижения уровня риска может включать в себя различные контрмеры, архитектурные практики, выбор устройств IACS и решения, когда и где следует их применять в зависимости от уровня риска, показанного в таблице А.3. В системах с высоким уровнем риска должны применяться более комплексные контрмеры для обеспечения высокого уровня защиты.

Один из способов, позволяющих зафиксировать решения организации в отношении принимаемых контрмер, подразумевает разработку таблицы, в которой указываются специфические контрмеры, используемые для устройств IACS, в зависимости от уровня риска IACS. Пример потенциальной контрмеры показан в таблице А.4.

В таблице определен набор стандартных решений для достижения требуемого уровня обеспечения безопасности. Применение таких контрмер обязательно кроме случаев, когда есть уникальное ограничительное условие, из-за чего использование такого решения для определенной системы IACS становится нежелательным. Стратегия организации по снижению риска также может включать в себя рейтинги уровней риска, необходимые для определения приоритетов и сроков принятия установленных контрмер, приведенных в таблице А.4. Возможно, системы IACS с высокими рейтингами рисками требуют более срочных мер, чем IACS с низким уровнем риска.

Контрмеры по устранению определенного риска могут отличаться для различных типов систем. Например, средства контроля аутентификации пользователей для сервера управления с расширенной сферой приложения, связанного с DCS, могут отличаться от средств контроля аутентификации для HMI на линии упаковки. Рекомендуется документальное оформление и доведение до сведения информации о выбранных контрмерах, вместе с инструкциями по применению контрмер.

Таблица А.4 — Пример контрмер и практик на основе уровней риска IACS

Контрмеры и архитектурные практики	IACS с высоким уровнем риска	IACS со средним уровнем риска	IACS с низким уровнем риска
Двухфакторная аутентификация для контроля доступа к устройству	Требуется	Требуется	По выбору
Усовершенствование операционной системы	Требуется	Рекомендуется	По выбору
Использование сегментации сети	Требуется	Требуется	По выбору
Использование антивирусного приложения	Требуется	Требуется	Требуется
Использование WLAN	Не разрешается	Может быть разрешено	Разрешается
Строгая аутентификация по паролю на уровне приложения	Требуется	Рекомендуется	Рекомендуется
Прочие контрмеры	—	—	—

Для защиты устройств IACS могут и должны применяться различные контрмеры, способствующие снижению IT-рисков. Указания по специфическим контрмерам рассматриваются в других частях стандарта серии МЭК 62443, которые находятся на этапе разработки, например МЭК 62443-3-2 [7] и МЭК 62443-3-3 [8], и посвящены более глубокому изучению доступных контрмер и их применению в среде IACS.

Во многих организациях для работ в отношении CSMS используется ограниченный комплекс финансовых и человеческих ресурсов. Важно применять эти ресурсы с максимальной выгодой. Управление риском начинается с понимания уязвимостей, существующих внутри IACS, и потенциальных последствий, которые могут наступить после реализации уязвимости. После изучения рисков компании необходимо разработать систему управления для

снижения рисков или поддержания их на допустимом уровне. Часть моделей безопасности, рассмотренных в IEC/TS 62443-1-1, будет применяться при создании системы принятия мер. Модели включают в себя модель уровня защиты совместно с зональной и трактовой моделью.

Примечание — В настоящем подпункте описывается один из возможных способов решения задачи этого ключевого элемента CSMS с использованием моделей безопасности по IEC/TS 62443-1-1. Не имеется единого правильного подхода к работе с этим элементом. При использовании альтернативных подходов можно разработать очень функциональную схему управления риском.

Подробное описание и пример по управлению риском и принятия мер дают представление о структуре процесса, применяемого для снижения рисков информационной безопасности для существующей системы в едином промышленном рабочем пространстве. Такая схема в равной степени применяется и к новым IACS, расположенным в различных местах на земле.

Независимо от того, какой детальный подход используется для управления рисками и принятия мер, в хорошей системе качества на протяжении жизненного цикла IACS учитываются следующие основные наборы задач:

- решение проблемы риска для IACS;
- принятие контрмер;
- документальное оформление информации по контрмерам и остаточным рискам;
- управление остаточным риском на протяжении жизненного цикла IACS.

Эти задачи подробно рассмотрены в А.3.4.2.3—А.3.4.2.5 и графически представлены в моделях жизненного цикла, описанных в IEC/TS 62443-1-1, 5.11.

А.3.4.2.3 Оценка риска для IACS для определения уровня риска безопасности IACS

А.3.4.2.3.1 Общие положения

Зональная и трактовая модель, модель жизненного цикла обеспечения безопасности и референтная модель подробно описаны в стандарте IEC/TS 62443-1-1. В настоящем подпункте рассмотрены вопросы использования и интеграции указанных моделей.

В А.2.3 представлены указания по выполнению процедуры, необходимой для анализа риска IACS. Это одна из самых первых задач на этапе оценки модели жизненного цикла обеспечения безопасности. Организация должна разработать и документально оформить процесс оценки риска с тем, чтобы его можно было применять к различным IACS с различным местоположением в организации и получать воспроизводимые результаты.

В настоящем подпункте объясняется, каким образом этап оценки встраивается в общую стратегию управления рисками. Это демонстрируется через сценарии проверки существующей IACS и улучшение состояния информационной безопасности этой системы для снижения риска. На рисунке А.14 показан этап оценки для модели жизненного цикла обеспечения безопасности.

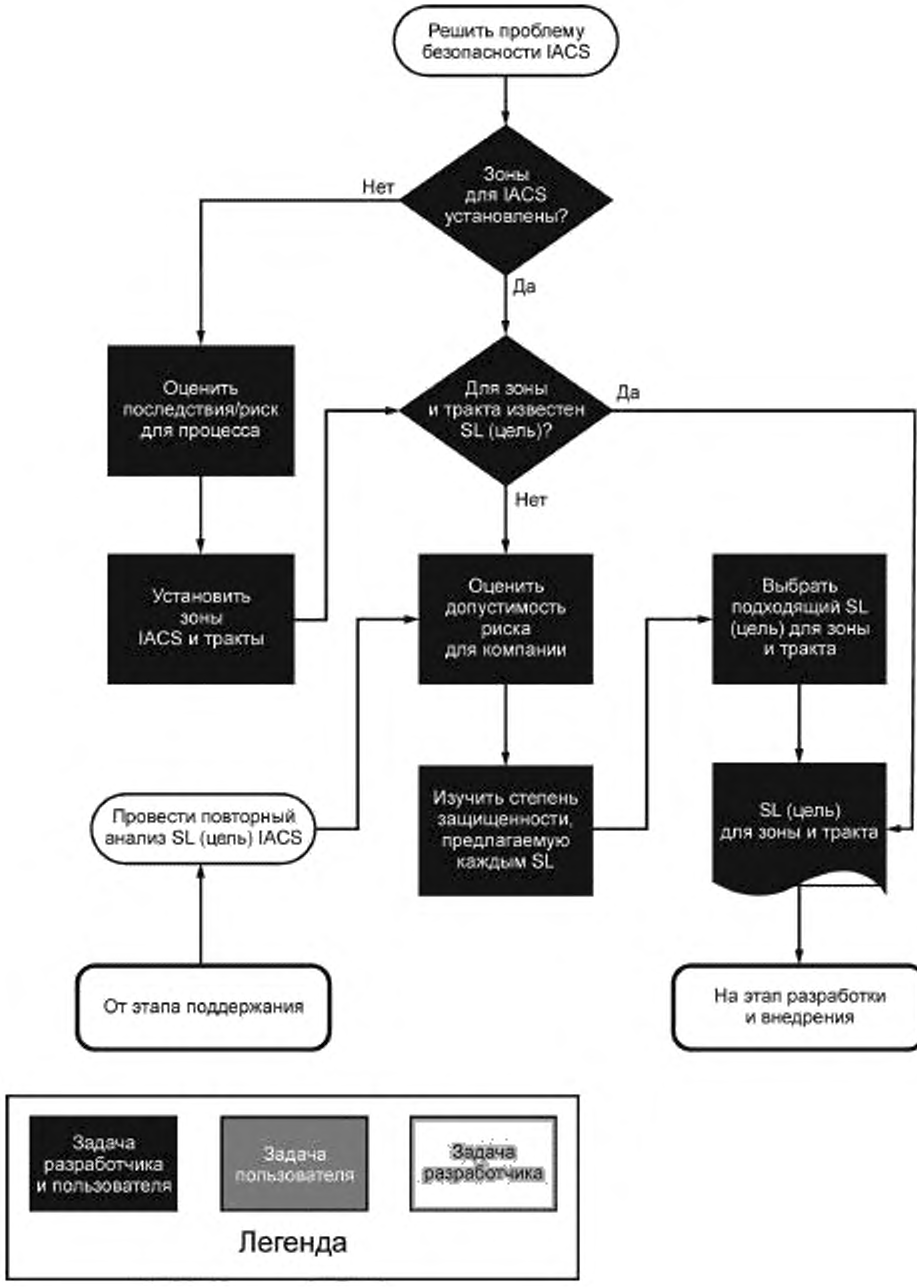


Рисунок А.14 — Модели жизненного цикла обеспечения безопасности: Этап оценки

Для действующей IACS, по которой никогда не проводилась процедура оценки риска и в которой еще не была принята зональная модель, работа начинается с компонента под названием «Оценить последствие/риск для процесса».

Целью оценки является понимание влияния риска на бизнес в случае появления угрозы для IACS в форме кибер-инцидента, в результате чего она будет неспособна выполнять назначенные функции управления или непредусмотренные функции. После того, как будет оформлена документация по риску, связанному с IACS, необходимо выполнить работы по управлению и смягчению риска.

По результатам анализа риска составляется таблица, в которой указывается рейтинг последствия и рейтинг вероятности для каждого объекта IACS или определенного комплекса объектов. В таблице А.5 приводится пример результатов, полученных в ходе детальной оценки риска, и результатов, полученных путем объединения данных из таблиц А.1, А.2 и А.3. Рейтинг вероятности назначается с учетом оценки уязвимости каждого указанного объекта, а также вероятности реализуемых связанных угроз.

Таблица А.5 — Пример таблицы для объекта IACS с результатами оценки

Объект IACS	Рейтинг последствия	Рейтинг вероятности
Панель управления в операторской	A	Средний
Дистанционная панель управления	C	Высокий
Инженерная станция конфигурации	A	Высокий
Сервер архивных данных	B	Средний
Контроллер	A	Средний
Шлюз	B	Средний
Прочие устройства	C	Низкий

А.3.4.2.3.2 Определение уровня риска IACS

В таблице А.3 показана упрощенная примерная модель для перевода чувствительности организации к риску в качественные уровни риска IACS. Модель должна подготавливаться ответственными руководителями организации предварительно, до проведения анализа риска.

Точки пересечения рейтингов «Последствия» и «Вероятность» представляют собой уровни риска.

Пример — Устройство IACS с последующим рейтингом B и вероятностью «Высокая» представляет собой устройство высокого риска.

Концепции определения риска, приведенные в таблице А.3, могут применяться к объектам IACS, приведенным в таблице А.5, в которой сводятся общие рейтинги для IACS, как показано в таблице А.6. В этой таблице определенные уязвимости упорядочены по приоритетам.

У каждого устройства имеется уровень риска информационной безопасности, связанный с ним. В хорошо интегрированной IACS функции контроля, предусмотренные для каждого устройства, в значительной степени зависят от целостности прочих устройств в IACS. На функциональную целостность системы контроля будет влиять целостность самого слабого устройства.

Упрощающее допущение заключается в том, что устройство с наиболее высоким уровнем риска определяет внутренне присущий уровень риска для всей IACS. На примере, приведенном в таблице А.6, видно, что внутренне присущий уровень риска для IACS является высоким риском, поскольку несколько устройств IACS имеют уровень риска, идентифицированный как высокий риск.

Таблица А.6 — Пример объектной таблицы IACS с результатами оценки и уровнями риска

Объект IACS	Рейтинг последствия	Рейтинг вероятности	Уровень риска для устройства IACS
Панель управления в операторской	A	Средний	Высокий риск
Дистанционная панель управления	C	Высокий	Средний риск
Инженерная станция конфигурации	A	Высокий	Высокий риск
Сервер архивных данных	B	Средний	Средний риск
Контроллер	A	Средний	Высокий риск

Окончание таблицы А.6

Объект IACS	Рейтинг последствия	Рейтинг вероятности	Уровень риска для устройства IACS
Шлюз	B	Средний	Средний риск
Прочие устройства	C	Низкий	Низкий риск

Понимание этого базового уровня внутренне присущего риска является ключом к реализации плана по управлению рисками. Он устанавливает целевой уровень защиты, требуемый для снижения риска. Таким образом определяется обоснованность реализации плана по снижению риска и управления риском, если IACS еще не работает на целевом уровне. Для снижения риска IACS до приемлемого уровня могут быть использованы различные контрмеры безопасности. Однако в случае неудачного применения контрмер может возникнуть инцидент, последствия которого будут иметь масштаб, установленный в ходе выполнения задачи анализа риска.

А.3.4.2.3.3 Определение безопасных зон и связь устройств IACS с зонами

Референтная модель, описанная в IEC/TS 62443-1-1, определяет различные операционные уровни или уровни оборудования IACS. Несмотря на то, что в пределах IACS могут быть различные операционные уровни, требования к информационной безопасности могут быть аналогичны для некоторых таких операционных уровней или уровней оборудования. Есть возможность включить несколько операционных уровней/уровней оборудования в единую логическую безопасную зону.

Модель уровня безопасности вводит концепцию использования зон, назначенных для одного из трех или более уровней безопасности. Чтобы представить, как это работает, можно предположить, что имеется три уровня безопасности, в качественном выражении описанные как «Низкий», «Средний» и «Высокий». Задача заключается в том, чтобы проверить потребности в защите различных объектов IACS и отнести их к этим различным зонам.

В таблице А.6 показан уровень информационной безопасности IACS для каждого из объектов. Для объектов с высоким уровнем риска требуется высокий уровень информационной защиты для снижения риска. Такие объекты должны быть отнесены к общей зоне безопасности. Объекты с более низкими уровнями риска должны быть отнесены к зоне с меньшей потребностью в защите. На данном этапе управления рисками целесообразно привязывать установленные зоны безопасности к физической сетевой схеме, подготовленной для анализа риска.

С учетом современных технологий принятия контрмер зоны безопасности, как правило, будут совпадать с сегментами физической сети. В зависимости от результатов анализа риска отдельное устройство IACS в данный момент может быть не установлено в соответствующем сегменте сети. В таком случае возможно потребуется перенести устройство в другой сегмент сети. Объект с низким уровнем риска может быть отнесен к зоне безопасности с более высоким уровнем риска, но объекты с высоким уровнем риска не должны располагаться в зоне безопасности с низким уровнем риска. Если это произойдет, возрастет риск недопустимого последствия в случае инцидента, связанного с информационной безопасностью.

На этапе внедрения модели жизненного цикла обеспечения безопасности устройства с потребностями в защите, не соответствующими зоне, в которой физически расположены такие устройства, должны быть перенесены в соответствующие сетевые сегменты, что позволит выполнить требования безопасности.

Организация может принять решение об установлении общего подхода к зонам безопасности в попытке улучшить эффективность управления рисками. Один из способов заключается в принятии шаблонной корпоративной архитектуры, включающей в себя стратегии сегментации сетей и зоны безопасности для различных типов устройств и систем, используемых на предприятии. На рисунке А.15 приведен пример шаблонной архитектуры зоны безопасности для организации. На рисунке А.16 представлено, каким образом объекты IACS привязываются к зонам в шаблонной архитектуре, построенной по принципу трехзвенной архитектуры.

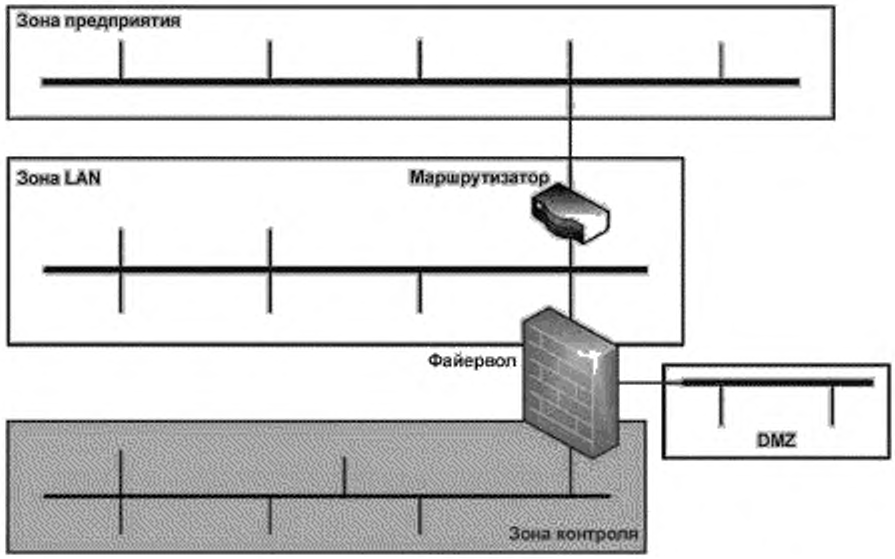


Рисунок А.15 — Шаблон архитектуры корпоративной зоны безопасности

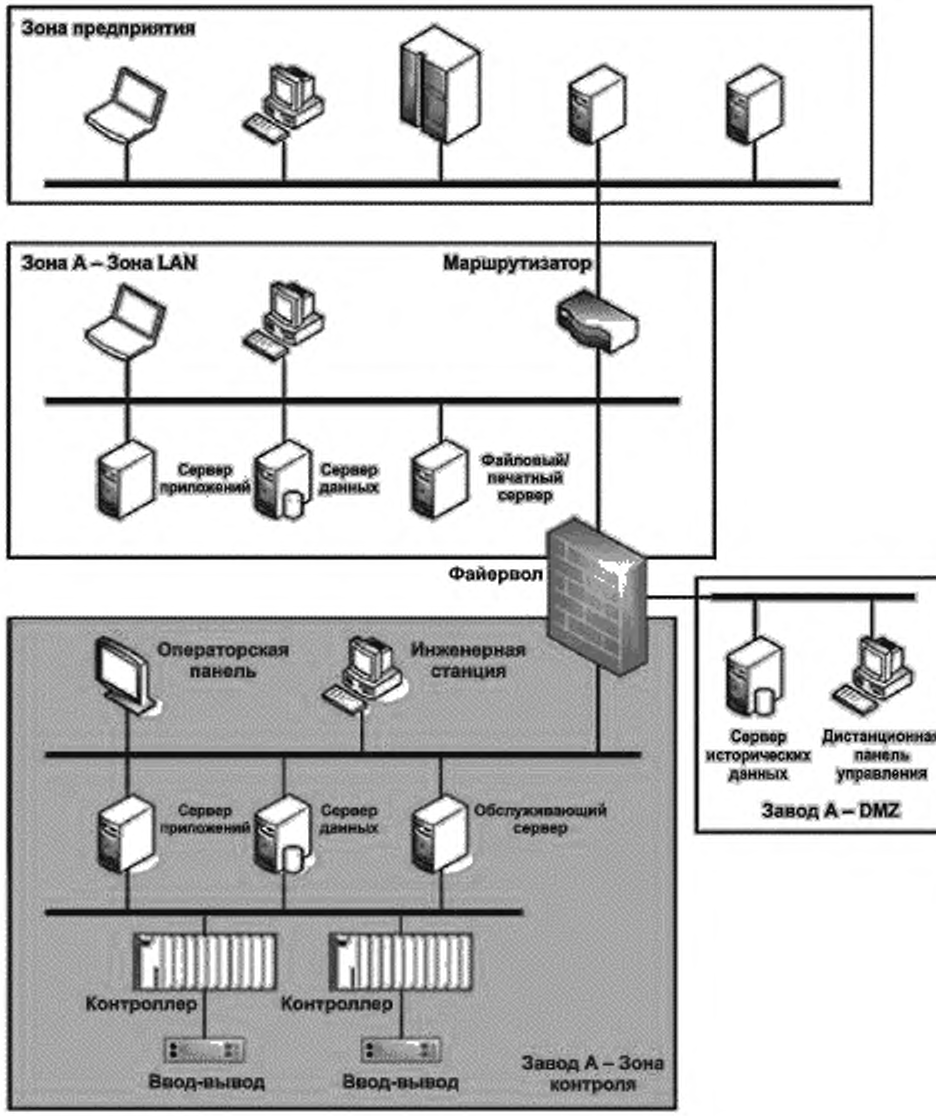


Рисунок А.16 — Зоны безопасности для примерной IACS

А.3.4.2.3.4 Определение целевого уровня безопасности (SL)

Модель уровня безопасности вводит концепцию назначения уровня безопасности для зоны. Из примера, приведенного на рисунке А.16, видно, что внутренне присущий уровень риска IACS был определен как высокий с учетом результатов детальной оценки риска для каждого устройства IACS. Для защиты устройств, входящих в зону контроля завода А, необходимо использовать дополнительные контрмеры безопасности. При использовании уровней безопасности, перечисленных в IEC/TS 62443-1-1 (таблица 8), целесообразно назначать для каждой из зон целевой уровень безопасности в соответствии с таблицей А.7.

Таблица А.7 — Целевые уровни безопасности для IACS, взятой для примера

Зона	Целевые уровни безопасности = SL (цель)
Зона контроля завода А	Высокий
Демилитаризованная зона завода А	Средний
Зона LAN завода А	Низкий
Зона предприятия	Низкий

А.3.4.2.3.5 Выбор устройств и структура системы с учетом SL (потенциал)

Необходимо изучить возможности каждого устройства по обеспечению требуемого уровня безопасности, чтобы понять преимущества и уязвимости, создаваемые им для зоны. Несмотря на то, что на данном этапе времени не представляется возможным выполнить количественную оценку SL (потенциал), имеются другие методы количественной оценки соответствующего SL (потенциал) устройств, составляющих IACS. Такие компоненты оценки обычно входят в состав детальной оценки уязвимости. Например:

- если устройство является веб-сервером, на котором работает инструмент оценки для определения уязвимых мест приложений веб-сервера и возможности их устранения;
- запуск инструмента оценки для определения количества сервисом и портов, требуемых для функционирования приложения в устройстве;
- требуемых портов и сервисов, позволяющая установить, использовались ли взломщиками такие порты ранее для изучения уязвимостей системы;
- проверка операционной системы устройства и определение, поставляются ли до сих пор патчи для устранения ошибок защиты и обновления для используемой версии;
- запуск инструмента оценки для ввода нестандартных исходных параметров, позволяющего определить, продолжит ли приложение функционировать в случае нестандартных потоков данных;
- проверка истории эксплойтов основных технологий, использованных в работе устройства, для установления вероятности будущих эскплойтов.

Организация должна установить определенные технические критерии для устройства, которое будет использоваться в определенном целевом SL, в зависимости от результатов оценки уязвимости. Если SL (потенциал) устройства слишком низкий для того, чтобы обеспечивать SL (цель) для зоны, может потребоваться выбрать альтернативное устройство. Для существующей IACS, состоящей из устройств более старшего поколения, возможно потребуется заменить устройство на более новое с более высоким SL (потенциал). Таким примером может быть компьютеризированная станция управления, работающая на основе операционной системы Microsoft Windows® NT. Результаты детального анализа уязвимостей для данного устройства и приложений указывают на наличие существенных уязвимостей. Характеристик безопасности, встроенных в такую устаревшую операционную систему, намного меньше, чем во многих операционных системах нового поколения. Кроме того, патчи для устранения ошибок защиты для таких уязвимостей больше не поставляются разработчиком. По этой причине SL (потенциал) этого устройства можно описать как относительно слабый.

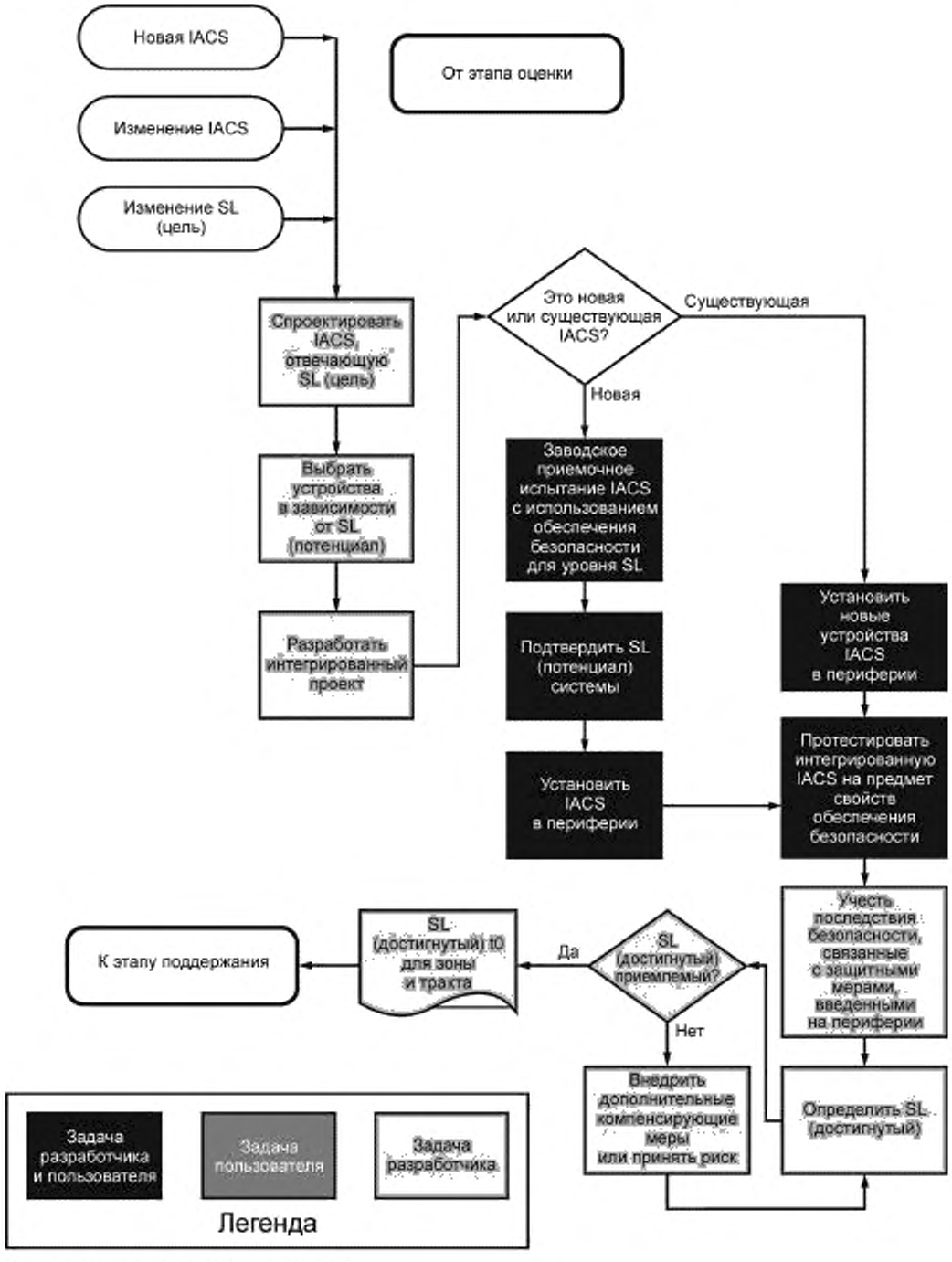
Необходимо проверять SL (потенциал) каждого нового устройства IACS, чтобы гарантировать поддержку целевого SL (цель) для зоны. Несмотря на то, что количественные измерения SL (потенциал) могут быть недоступны и/или могут не публиковаться, разработчики могут предоставить часть количественных измерений, полученных на основе оценок, проведенных ими или третьими лицами с использованием стандартных инструментов безопасности и полевой эксплуатации. Такие результаты детальной оценки уязвимости должны учитываться и использоваться в процессе принятия решения относительно выбора новых устройств IACS.

Предварительное проектирование, определяющее устройства IACS и назначения по зонам, должно переходить в детальное проектирование с определением всего оборудования и сетевых сегментов, которые будут использоваться в IACS. Именно на этом этапе необходимо менять местоположение устройств, потребность которых в защите от риска не соответствует SL (цель) для зоны. В результате этой работы будет сформирована детальная сетевая схема с указанием местоположения всех IACS и сетевых устройств, входящих в состав общей системы IACS.

А.3.4.2.4 Разработка и внедрение избранных контрмер для каждой зоны

А.3.4.2.4.1 Общие положения

На этапе разработки и внедрения модели жизненного цикла уровня безопасности ведется работа над мерами и задачами снижения риска. Общая концепция данного этапа заключается в использовании контрмер в отношении IACS, позволяющих достичь целевого SL для зоны, установленного на этапе оценки. На рисунке А.17 показаны несколько различных стартовых точек. Такой подход применяется к введению новой IACS, изменению существующих IACS в форме нового оборудования, и повышению уровня безопасности существующих IACS. Рисунок А.17 представлен скорее всего в качестве системы критериев, определяющих вектор мышления в ходе работы, чем детальной структурной схемы или контрольного списка действий, обязательных к исполнению.



Примечание – t0 = в момент времени 0.

Рисунок А.17 — Модель жизненного цикла уровня безопасности «Этап разработки и внедрения»

Начальной точкой данного этапа является цель безопасности, которую необходимо достичь. Она понимается как целевой уровень безопасности для каждой зоны IACS. На этапе оценки были установлены такие цели и назначены зоны для каждого устройства IACS. Задача заключается в использовании этого предварительного похода и подготовки детального проектирования для дальнейшей реализации.

А.3.4.2.4.2 Офлайновое тестирование защищенности

Насколько функциональное тестирование IACS важно для введения IACS, чтобы было обеспечено выполнение требований операционного объекта, настолько важно проводить тестирование защищенности устройств, гарантирующее, что будут достигнуты требуемые уровни операционной целостности и надежности. На рисунке А.3.4.3 более подробно рассказывается о тестировании защищенности.

Если IACS является новой системой, тестирование защищенности должно проводиться, пока система находится в офлайновой среде. Это могут быть заводские приемочные испытания на заводе разработчика или этап подготовки к производству на конечной полевой площадке. Местоположение не настолько важно, как гарантия того, что принимаются меры по тестированию защищенности. Несмотря на то, что может быть очень полезно провести тестирование защищенности всех устройств и контрмер, использованных на конечном этапе их установки, с точки зрения осуществимости и целесообразности это может не иметь смысла. Поэтому концепция тестирования должна основываться больше на SL (потенциал) устройств IACS и контрмерах, которые не являются специфическими для места установки в периферии.

В А.3.4.2.3.5 говорилось о нескольких инструментах, которые необходимо учитывать при тестировании SL (потенциал). Такие моменты обычно включаются в детальную оценку уязвимости. Тестирование защищенности должно включать в себя не только тестирование с целью анализа способности противостоять стандартным угрозам, появляющимся во время работы, но также должно включать меры, которые будут приниматься в рамках текущей поддержки системной безопасности. К ним относятся (но не ограничиваются этим):

- тестирование процесса инсталляции патч-файлов и обновлений;
- тестирование процесса инсталляции патч-файлов и обновлений для обновлений IACS разработчика;
- тестирование офлайновой среды разработки системы;
- тестирование внедрения антивирусного ПО и обновлений сигнатур вредоносного ПО.

Работа в рамках тестирования защищенности, показанного в центре рисунка А.17, проводится с целью подтверждения, что SL (потенциал) устройств соответствует основе проектирования.

А.3.4.2.4.3 Полевое тестирование защищенности

Компоненты, показанные справа на рисунке А.17, определяют действия в рамках тестирования, связанные средой конечного адресата. С этой точки начинается тестирование и/или проверка всех использованных контрмер, если достигнутый уровень защищенности равен или превосходит целевой уровень защищенности, заложенный для зоны при проектировании.

Если выполняется установка новой IACS, может быть, следует провести такое тестирование до вывода IACS в онлайновый режим. Если необходимо модифицировать и заменить существующее устройство IACS или внедрить несколько новых контрмер для обеспечения безопасности IACS, то офлайновое полевое тестирование будет невозможным. Наоборот, частой проблемой является внедрение нового устройства или контрмеры и полевое тестирование на предмет того, что меры безопасности не оказали недопустимого воздействия на базовую рабочую функцию IACS.

Следует принимать во внимание, что тестирование производительности системы должно включать в себя реагирование системы на стандартные и нестандартные происшествия, связанные с промышленными операциями, а также стандартные и нестандартные происшествия, связанные с инцидентами в сфере безопасности. В совокупности они позволяют установить общую степень надежности и целостности системы.

Учитывая, что каждая промышленная операция немного отличается, невозможно определить готовую определяющую процедуру для данного тестирования. Потребуется выполнить большой объем проектировочных работ, чтобы определить наилучший способ проведения тестирования, которое позволило бы гарантировать, что функции безопасности отвечают целям безопасности и делают возможным достижение целевого SL.

А.3.4.2.4.4 Достижение целевого SL

Для достижения целевого SL в поле требуется определенная степень итерирования. Периферия не является совершенным миром. Обычно целесообразно применять стандартный набор контрмер ко всем устройствам в пределах зоны, чтобы достичь желаемого уровня безопасности. Избранная контрмера, установленная для внедрения на всех устройствах, может быть непригодна для использования на конкретном устройстве, т. к. операционное или физическое ограничение изначально не было учтено при проектировании системы безопасности. Поэтому важно понимать, что в реальных ситуациях может потребоваться устранить или добавить контрмеры для отдельных устройств в пределах зоны. Это необходимо для достижения нужного равновесия между преимуществом безопасности и риском, что позволит удовлетворить интересы всех сторон, участвующих в процессе принятия решений.

А.3.4.2.4.5 Демонстрирование процесса проектирования на примере IACS

В А.3.4.2.4.4 описаны принципы внедрения контрмер безопасности, необходимых для достижения SL (цель) для зоны. В настоящем подпункте описан процесс проектирования и применение этих принципов на реальном примере.

В таблице А.6 описывается сервер исторических данных с уровнем риска «Средний». Благодаря использованию корпоративной шаблонной архитектуры безопасности было установлено, что это устройство должно быть расположено в зоне безопасности SL (цель) среднего или более высокого уровня. DMZ завода А была определена

в качестве подходящей зоны для данного устройства, несмотря на то, что в настоящее время устройство расположено в зоне LAN завода А.

При подготовке физического внедрения DMZ завода А выполняется проверка SL (потенциал) сервера архивных данных, которая позволяет определить соответствие SL (цель). Изучение уязвимостей, установленных в результате детальной оценки уязвимости, позволяет выяснить, что:

- операционная система для сервера — Microsoft Windows® NT, для которой обновления безопасности отсутствуют;
- на сервере не работают антивирусные приложения. Разработчик архивного приложения не подтвердил совместимость антивирусных программных продуктов с архивным приложением.
- большинство пользователей архивного приложения расположены в офисных участках с компьютерным соединением с зоной LAN завода А с более низким уровнем защищенности;
- работа по усовершенствованию сервера путем закрытия ненужных задач проведена безуспешно, т. к. разработчик архивного приложения не подтвердил, что приложение будет работать правильно при отключении серверов.

Из этого следует, что внутренне присущий SL (потенциал) сервера архивных данных не соответствует SL (цель) DMZ завода А.

В связи с тем, что внутренне присущий SL (потенциал) слишком низкий, проверяется использование дополнительных контрмер, в результате чего можно определить, насколько успешно они могут помочь снизить риск и достичь SL (цель). Проверяются такие дополнительные контрмеры, как ограничение доступа к сети Интернет, ограничение электронной почты, деактивация медиа-портов на таком сервере, использование строгих паролей. Несмотря на то, что они могут быть полезны для снижения рисков, есть вероятность, что использование таких дополнительных защитных практик не позволит скомпенсировать внутренне присущий низкий SL (потенциал) сервера архивных данных.

В связи с тем, что сервер архивных данных напрямую взаимодействует со шлюзом IACS сети управления, слабые места этого устройства также снижают SL (достигнутый) зоны контроля завода А. Из этого следует вывод, что наилучшим способом решения таких проблем с недопустимым уровнем SL (достигнуто) и DMZ завода А и зоны контроля завода А является замена действующего сервера архивных данных на более новое программное приложение, работающее на основе операционной системы с действующей поддержкой. После проверки SL (потенциал) более нового сервера и архивного приложения, гарантирующей соответствие с SL (цель), выполняется проверка и внедрение сервера и приложения в DMZ завода А во время отключения промышленной операции.

Есть несколько важных моментов, о которых стоит упомянуть в связи с таким примером. SL (достигнуто) зоны зависит от SL (потенциал) устройств в зоне, а также от связи между зонами и в их пределах. При анализе уязвимости устройства учитываются не только внутренне присущие свойства устройства, взятые отдельно, но также возможность взаимодействия этого устройства в сети. Это важно учитывать, т. к. IACS, в которой используются устройства только с высоким SL (потенциал) в отдельности, при рассмотрении в совокупности не обязательно достигают желаемого высокого SL (цель) для зоны. Например, новое устройство IACS, в которое внедряется новая OS, даже если есть все патчи и запущено антивирусное ПО, имеет более низкий SL (достигнуто) при прямом подключении к корпоративной IT-сети. И наоборот, когда одно устройство ограничивает физический доступ и подключаемость к сети, устройства с более низким SL (потенциал) вместе могут достигнуть более высокого SL (достигнуто) для зоны.

Безопасность тракта между зонами также может влиять на SL (достигнуто) зоны. Например, тракт с использованием беспроводной связи, а не физического кабеля, может иметь высокий уровень SL (достигнуто) для тракта и влиять на SL (достигнуто) зон, связанных трактом.

Аналогичным образом, на SL (достигнуто) рассматриваемой зоны может влиять уровень безопасности зоны, связанной с рассматриваемой зоной. В данном примере пользователи архивного приложения находятся в зоне с более низким уровнем безопасности, чем сервер архивных данных. Даже если SL (достигнуто) тракта между такими зонами высокий, более низкий SL (достигнуто) зоны LAN завода А может оказывать потенциально негативное воздействие на SL (достигнуто) DMZ завода А.

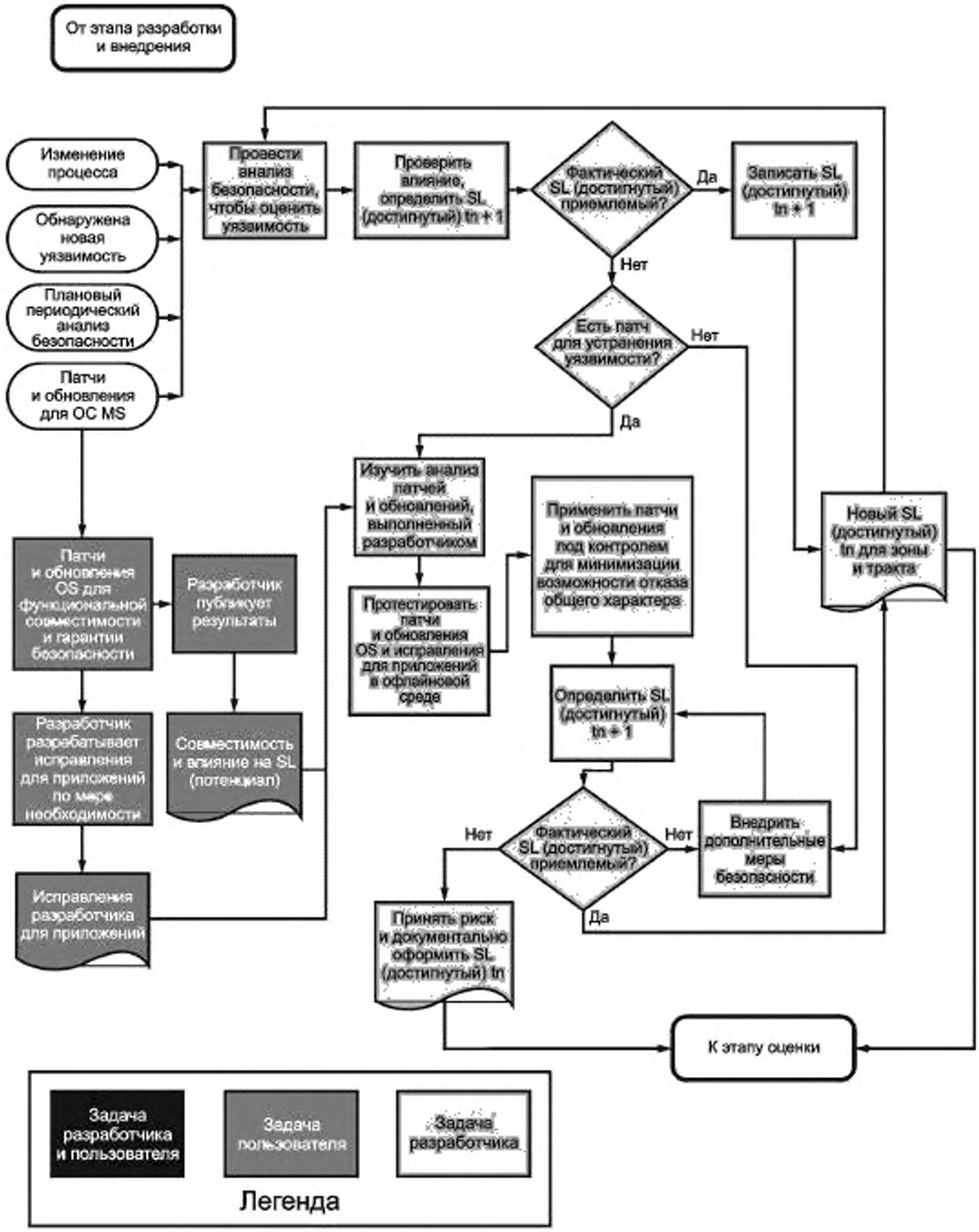
A.3.4.2.5 Поддержание уровней безопасности для каждой зоны

A.3.4.2.5.1 Общие положения

Уровень безопасности устройства постоянно ослабевает. Практически каждую неделю обнаруживаются новые уязвимости в системе безопасности. Пока известны и не устранены эксплойты, использующие уязвимости, IACS могут оставаться в опасности и SL (достигнуто) зоны потенциально будет ниже чем SL (цель). В отношении такой реальной ситуации должен применяться план для поддержания уровня безопасности зоны на приемлемом уровне.

Этап поддержания модели жизненного цикла обеспечения безопасности, приведенный на рисунке А.18, отражает циклический комплекс действий, важных для поддержания безопасности зоны. Инициирующие факторы начала повторной оценки риска включают в себя (но не ограничиваются этим):

- изменение в физической промышленной операции или изменения в IACS, которые могут привести к новым рискам;
- новая уязвимость, обнаруженная в программном модуле, используемом в IACS;
- выпуск новой OS или патча для приложения, которые запускают использование кода эксплойта для подключения к Интернет;
- плановые периодические аудиты и обзоры системы безопасности.



Примечание – tn = в более поздний момент времени по сравнению с 0.

Рисунок А.18 — Модель жизненного цикла уровня безопасности «Этап поддержания»

А.3.4.2.5.2 Исправления в устройствах IACS с помощью патчей

На рисунке А.18 приведен укрупненный анализ того, каким образом корректировка при помощи патчей встраивается в этап поддержания модели жизненного цикла обеспечения безопасности. Положения настоящего подпункта не должны восприниматься как комплексное обсуждение всех аспектов, связанных с патчами. Его целью является иллюстрация итеративного аспекта проверки состояния SL (достигнуто) зоны и необходимости принимать комплексные решения относительно того, какие патчи должны быть использованы и когда их следует применять.

Разработчики устройств и приложений IACS разделяют ответственность с пользователями за решение задач, связанных с устранением рисков безопасности. Пользователям необходимы разработчики, чтобы понимать внутренние механизмы приложений IACS, чтобы определять применимость патча и выполнять сквозное автоматизированное регрессивное тестирование совместимости приложения IACS с патчами операционной системы и основными обновлениями. Поскольку при инсталляции патчей возможно вмешательство в нормальную работу программного приложения IACS, пользователям нужен максимум гарантий того, что инсталляция обновленного ПО не приведет к неисправности устройства управления.

На рисунке А.18 показано, что тестирование совместимости разработчика является первым шагом многоэтапного плана тестирования до проведения масштабной инсталляции патчей в работающей IACS. Необходимо проводить дополнительное тестирование с целевой средой устройства. Идеальные результаты будут получены при тестировании офлайнового устройства, идентичного рабочей IACS. Если это невозможно, необходимо рассмотреть альтернативные подходы, которые включают в себя тестирование в виртуальной среде или в контролируемом развертывании патча для работающей IACS.

Имея данные об уязвимостях, полученные от разработчика операционной системы, данные о совместимости патчей от разработчика IACS, данные о совместимости от разработчика IACS, информацию об использовании устройства IACS и, наконец, о тестировании пользователей, пользователь принимает решение о полевом развертывании патча.

А.3.4.2.5.3 Использование дополнительных контрмер

Для решения задач, связанных с неустраненными уязвимостями от патчей или уязвимостями, появившимися в результате изменений в промышленных операциях, могут потребоваться дополнительные контрмеры. Потребность в таких контрмерах определяется путем оценки SL (достигнутый) и его сравнения с SL (цель) для зоны.

В некоторых случаях бизнес-риск, с которым связана работа по повышению SL (достигнутый), в краткосрочной или долгосрочной перспективе может привести к существенным затратам. В этом случае лица, принимающее техническое решение, должны документально представить:

- риски;
- использованные контрмеры;
- контрмеры, рассматриваемые и отклоненные, и соответствующие причины;
- рекомендации для бизнес-лидеров по принятию риска на определенный период времени до того момента, когда можно будет установить, протестировать и внедрить наиболее приемлемую контрмеру или решение в области обеспечения безопасности.

Бизнес-лидеры должны официально и в письменном виде оформить согласие на принятие данной стратегии.

А.3.4.2.5.4 Плановый контроль защищенности

Комплексная CSMS включает в себя компонент соответствия, в который входит периодическая оценка использования защитных практик и контрмер, определенных в корпоративной политике безопасности и стандартах, и их эффективности в снижении риска и достижения SL (цель). Это еще один инициирующий фактор для этапа поддержки модели жизненного цикла обеспечения безопасности.

В ходе аудита безопасности измеряется степень соответствия определенным политикам и стандартам, что позволяет получить данные, необходимые для поддержания безопасности. Кроме проверки соответствия требуемым практикам организация периодически (и с учетом инициирующих факторов, указанных на рисунке А.18) должна проводить анализ того, в какой степени SL (достигнутый) соответствует или превосходит SL (цель) в зонах IACS.

А.3.4.2.6 Вспомогательные практические методы

А.3.4.2.6.1 Основные практические методы

К основным практическим методам относятся следующие действия:

a) определение и подтверждение правильности политик безопасности. В детальных положениях политик безопасности определяется цель операционного уровня по снижению каждого из рисков безопасности во время оценки риска;

b) разработка процедур с подробным описанием действий, необходимых для предупреждения, обнаружения и реагирования на угрозы;

c) адаптация стандартов международных организаций в сфере информационной безопасности для использования в среде IACS организации;

d) разработка сервисов для защиты образов операционной системы и общих приложений для обеспечения безопасной работы IACS;

e) определение инструментов и продуктов безопасности для внедрения компонентов политики безопасности. Несмотря на то, что инструменты и продукты безопасности, такие как файерволы и VPN-соединения, могут применяться в средах IT и IACS, регламенты и применение таких типов инструментов и продуктов могут существенно отличаться из-за различных рисков, связанных с такими средами;

f) определение формальной методики принятия риска, включая соответствующее одобрение на уровне руководства, разработанной на основе сферы применения и документации;

g) внедрение политик, процедур, инструментов и т. п. способом, позволяющим минимизировать административные накладные расходы и расходы конечного пользователя без ущерба для эффективности. В хорошо спроектированных средствах контроля часто остается фактор аудита, которым можно пользоваться в дальнейшем для выполнения верификации;

h) документирование причин, по которым были выбраны или не выбраны определенные контрмеры безопасности, и риски, для которых они предназначены в соответствии с положением о применимости контрмер (SoA). Хорошо составленная документация о средствах контроля действий по снижению рисков может быть использована в процессе принятия решений и информирования о таких решениях, а также является основной для обучения персонала по вопросам реагирования на инциденты и угрозы и для самостоятельной оценки или аудитов на предмет соответствия контрмерам.

A.3.4.2.6.2 Дополнительные практические методы

Примечание 1 — В IEC/TR 62443-3-1 [6] и МЭК 62443-3-3 [8] будут рассматриваться соответствующие практики, как только работа над этими стандартами будет завершена.

Примечание 2 — Разработчики настоящего стандарта принимают во внимание, что имеется много различных видов доступных контрмер. Они также принимают во внимание, что если сюда включить перечень различных контрмер, то пользователь столкнется со слишком большим объемом информации для понимания, которая будет приведена недостаточно подробно для того, чтобы пользователь мог с точностью применять средства контроля в отношении IACS. Поэтому разработчики приняли решение о том, что вопрос рассмотрения дополнительных практик безопасности IACS, связанных с контрмерами, должен изучаться в рамках других документов, в которых пользователи смогут ознакомиться с более глубоким анализом различных контрмер и способов их правильного применения к среде IACS.

A.3.4.2.7 Использованные ресурсы

Данный элемент частично основан на материалах [23], [24], [27], [28], [29], [30], [31], [33].

A.3.4.3 Элемент «Разработка и поддержка системы»

A.3.4.3.1 Описание элемента

Элемент «Разработка и поддержка системы» представляет собой вспомогательные методы, необходимые для разработки и поддержки информационных систем IACS, которые влияют на CSMS и сами являются объектом воздействия CSMS. В нем рассмотрены такие аспекты информационной безопасности, как документы, касающиеся требований, проектирования, закупки, тестирования, управления изменениями, управления патчами, процессов резервирования и восстановления.

В основном, этот элемент дает представление, каким образом такие методы необходимо применять с точки зрения обеспечения информационной безопасности. Этот подход используется не для того, что воспроизвести документацию, в которой описаны основные положения таких методов, а для того, чтобы объяснить, почему вопросы безопасности являются неотъемлемой частью процессов разработки и поддержки системы. Вопросам безопасности необходимо уделять внимание в ходе нормальной реализации всех процессов разработки и поддержки систем.

A.3.4.3.2 Документы, касающиеся требований

В A.3.4.2 приведена концепция целевого уровня безопасности (целевого SL). Понятие «требования» относится к возможностям и/или характеристикам данной системы или устройства. Требования могут быть связаны с различными характеристиками в различных контекстах: требования к системам или ПО, продуктам или промышленной эксплуатации, функциональные или нефункциональные требования. Но для целей данного элемента понятие «Требования к системе» определяется как характеристики целевого SL, а понятие «Требования к устройству» — как характеристики контрмер, необходимых для устройств в пределах зоны для достижения нужного целевого SL. Учитывая, что требования к системе определяют целевой SL, их можно устанавливать на этапе управления риском и принятия мер. Эти требования к системе часто называются требованиями высокого уровня. Требования к устройству могут изменяться в зависимости от результатов этапа проектирования.

Например, требование к системе для зоны управления может заключаться в ограничении всего сетевого трафика до аутентичного трафика управления и автоматизации. Требование к устройству для панели управления может заключаться в деактивации всех неиспользуемых протоколов сетевого взаимодействия и передачи данных. В этом случае такое требование к устройству может лишь частично достигать требование уровня системы. Для выполнения требований к системе может потребоваться несколько требований к устройству.

Детально проработанный и доступный к проверке комплекс требований к системе и устройству служит основой методов тестирования, верификации и валидации процессов проектирования, закупки, управления изменениями и управления патчами. Крайне сложно сказать, будет ли нарушение целевого SL с точки зрения проектирования, закупки, изменений в системе или патчей, если не будут определены специфические возможности, необходимые для достижения такого уровня.

A.3.4.3.3 Проектирование

Информационная безопасность должна встраиваться в IACS на этапе проектирования. Такую цель необходимо учитывать при поставке и разработке системы, а также на этапе ее поддержки. Имеются многочисленные

документы, в которых описаны надежные процессы проектирования систем. Однако стоит иметь в виду, что важнейшим аспектом процесса проектирования является необходимость привязки специфических контрмер к каждому из требований к системе, что позволяет гарантировать, что устройства и системы как единое целое соответствуют целевому SL.

Процесс проектирования охватывает не только подготовку спецификации проекта, но также включает в себя планирование подхода к осуществлению контроля и первоначальный контроль, позволяющий убедиться в том, что проект отвечает заявленным требованиям. Первоначальная проверка может выполняться на этапе анализа документов. Окончательная проверка выполняется в ходе тестирования системы.

Следует принимать во внимание, что новые проекты открываются и реализуются постоянно. Чтобы не было оснований для последующей доработки, когда такие новые проекты будут завершены и введены в эксплуатацию, операционные группы и разработчики, отвечающие за реализацию проектов, должны владеть информацией о применимых отраслевых стандартах в области информационной безопасности, а также о соответствующих корпоративных политиках и процедурах.

А.3.4.3.4 Закупка

Процесс закупки имеет особо важное значение для достижения желательного целевого SL. При описании нового или обновленного оборудования разработчику важно включать требования к информационной безопасности. Если есть специфические требования к устройству, необходимые для выполнения требований к системе, то о них нужно открыто заявлять в процессе закупки таких устройств. Также может потребоваться оговорить такие требования к устройству, в соответствии с которыми разработчик или специалист-интегратор не имеет права совершать определенные действия. Имеется несколько стандартных практик для разработчиков устройств или интеграторов, которые они могут реализовать в своих устройствах, в результате чего могут появиться нежелательные слабые места в системе безопасности и система может не достигнуть целевого SL. Например, разработчики в своих продуктах предусматривали способы входа (лазейки), облегчающие работу по устранению неисправностей и позволяющие сократить время реагирования на клиентские запросы. Такие неофициальные способы входа являются уязвимостью, которыми могут воспользоваться злоумышленники. Торговый представитель может даже и не иметь представления о том, что в продукте предусмотрены такие возможности, которые не должны допускаться, кроме случаев, когда они открыто включаются в требования к закупке.

Тема описания процесса закупки в рамках информационной безопасности слишком обширна для того, чтобы ее рассматривать в настоящем стандарте. Ею занимаются другие группы, которые могут предоставить более подробную информацию по этому вопросу (например, [58]).

А.3.4.3.5 Тестирование

А.3.4.3.5.1 Общие положения

Программа тестирования проводится с целью, чтобы гарантировать выполнение системой заявленных требований по проекту. В случае правильно спроектированной системы необходимо предусмотреть выполнение операционных требований и требований к безопасности. Одним из самых первых решений при разработке программы тестирования является степень обеспечения гарантии, требуемой от разработчиков и интеграторов, относительно информационной безопасности устройств или систем. Степень обеспечения гарантии, требуемая для конкретного устройства или системы, будет определять вид необходимого тестирования. Разработчик может руководствоваться рекомендованной стратегией тестирования для конкретного устройства или системы, но пользователь должен определить, достаточна ли такая стратегия тестирования для подтверждения правильности требований к безопасности.

В идеале, система проходит тестирование во всех возможных состояниях, что позволяет гарантировать, что выполнено каждое условие безопасности или хотя бы известен остаточный риск. Несмотря на то, что полное тестирование системы теоретически возможно, для большинства спецификаций это недостижимо ввиду финансовых и кадровых ограничений. В связи с этим задача заключается в том, чтобы определить допустимый уровень риска и затем выполнить достаточное тестирование, сопоставимое с допустимым риском.

После первоначального планирования тестирования для каждого этапа тестирования необходимо подготовить письменные планы и процедуры. В них должны быть определены планы и ожидаемые результаты, а также должна входить конфигурация системы, входные и выходные параметры системы, допустимые диапазоны погрешностей. Во время тестирования важно выполнять хотя бы поверхностную проверку результатов, позволяющую убедиться в том, что они соответствуют ожиданиям или определить, требуется ли предпринять какое-либо корректирующее действие. После завершения каждого этапа тестирования требуется выполнить оценку результатов. После валидационного испытания системы составляется окончательный отчет, в котором анализируются результаты всех тестов и делаются выводы.

А.3.4.3.5.2 Типы тестирования

Тестирование информационной безопасности, как и тестирование в отношении других аспектов, включает в себя верификационные и валидационные тесты. В соответствии с моделью зрелости процессов разработки ПО [39]: *«Верификация позволяет подтвердить, что рабочие продукты надлежащим образом отражают требования, предъявляемых к ним. Другими словами, она гарантирует, что «вы все сделали правильно». Валидация подтверждает, что продукт в поставленном виде будет выполнять свое предназначение. Другими словами, она гарантирует, что «вы создали правильный продукт».* В итоге, верификация определяет, насколько реализация удовлетворяет требования спецификации, а валидация — насколько спецификация отвечает требованиям.

Вид того или иного тестирования будет зависеть от уровня требуемого теста, компонента или системы, проходящей тестирование, а также от вида тестирования, требуемого для системы или компонента. Тестирование информационной безопасности обычно выполняется в три этапа: тестирование компонента, интеграционное тестирование и тестирование системы. Верификационное тестирование проводится на этапе тестирования компонентов и интеграции, но и валидационный тест также может пригодиться. Оба теста проводятся на этапе тестирования системы.

A.3.4.3.5.3 Тестирование компонентов

Тестирование компонентов должно проводиться разработчиками и проверяться владельцем системы. Компонентом может быть ПО, аппаратное обеспечение, встроенное ПО или любые их комбинации. Компонент должен пройти тестирование, позволяющее установить, насколько он отвечает специфическим операционным требованиям и требованиям к безопасности. Тестирование компонента обычно проводится в рабочей среде и требуется с целью получения гарантии того, что когда компоненты будут собраны в систему, каждый отдельный компонент будет функционировать, как и предполагается.

A.3.4.3.5.4 Интеграционное тестирование

Интеграционное тестирование проводится специалистом-интегратором и проверяется владельцем системы. Такое тестирование включает в себя операционное тестирование и тестирование с точки зрения безопасности различных компонентов, возможно от различных разработчиков, собранными воедино в рабочей среде или на вспомогательном тестовом стенде с целью получения гарантии того, что все компоненты будут функционировать правильно до того, как будут помещены в среду IACS. Интеграционное тестирование может включать использование дополнительных тестовых инструментов, например, инструменты сетевого управления и администрирования, которые не требовались на этапе тестирования компонентов.

В редких случаях тестовый стенд будет иметь точную конфигурацию системы управления, действующей на рабочем объекте. В основном для этапа тестирования компонентов и интеграционного тестирования при разработке или лабораторной настройке лучше всего подходит упрощенная система или ее копия. Интеграционные тесты должны разрабатываться с учетом особенностей такого тестового стенда. Необходимо учитывать различия между условиями проведения интеграционного теста и средой IACS, а также любые дополнительные инструменты, которые могут потребоваться для того, чтобы продукт, который не прошел полное интеграционное тестирование, прошел такое тестирование на этапе тестирования системы. По этой причине, особенно на этапе интеграционного тестирования, полезно размещать упрощенную систему или ее копию рядом с площадкой, на которой установлена OS.

В некоторых случаях допускается выполнить непроизводственное интеграционное тестирование, позволяющее установить, насколько хорошо контрмеры безопасности будут работать в комплексе и как они будут взаимодействовать с операционными свойствами. Например, контрмеры безопасности, состоящие из дискретных аппаратных/программных средств, могут подключаться через лабораторную сеть тестового стенда. В других случаях такая интеграция невозможна. План интеграционного тестирования должен разрабатываться с учетом плюсовых особенностей схемы тестового стенда, конфигурация которого может быть разработана таким образом, что позволяет тестировать комбинации рабочих условий, присутствующих в операционной системе.

A.3.4.3.5.5 Тестирование системы

Верификационное и валидационное тестирование системы должен проводить владелец системы. Валидационное тестирование проводится с применением соответствующих техник, процедур и процедурных изменений (по мере необходимости) с целью демонстрации того, что управление, операционные и технические контрмеры IACS внедряются правильно, эффективны в своем применении и гарантируют, что новые защитные контрмеры системы в поставленном виде и после ее установки отвечают необходимым требованиям.

Тестирование системы может включать в себя тест на возможность проникновения в систему, позволяющий гарантировать, что компоненты безопасности могут защищать систему от различных угроз в соответствии с требованиями обеспечения уровня защищенности для каждой зоны. Такое тестирование позволяет определить, где именно известное лицо пытается обойти защитные механизмы и попасть в систему при поиске слабых мест и уязвимостей, которыми можно воспользоваться либо для получения доступа, либо для контроля системы. Многие компании специализируются в тестировании на возможность проникновения в традиционные IT-системы. Может быть намного сложнее найти группу, которая понимает особые требования IACS.

Для проведения фактического тестирования имеется большое количество разнообразных тестовых инструментов, например, сценарии тестирования, базы данных переменных значений, базовые конфигурации с предполагаемой датой начала тестирования, метрические показатели и калибровочные инструменты. Также в распоряжении имеются коммерческие и свободно распространяемые инструменты с заранее заданной конфигурацией, позволяющей выполнять диагностические операции и симулировать шлюзы и подключенные устройства.

При проведении тестов на возможность проникновения в систему, помимо результатов теста необходимо фиксировать производительность системы во время таких тестов. Скорее всего будет отмечаться некоторое ухудшение производительности системы или компонентов из-за проводимого теста. Эти изменения необходимо регистрировать для дальнейшего использования.

Следует отметить, что к контрмерам безопасности также могут относиться специалисты, работающие с политиками и процедурами, и неавтоматизированные проверки безопасности. Например, контрмера может включать

в себя инженера системы управления, устанавливающего патч, выпущенный для аппаратного или ПО. План тестирования может строиться на основе последовательности холостого прогона установки патча с определением других факторов, на которые он влияет.

A.3.4.3.5.6 Разделение сред разработки и тестирования

Разработка и тестирование могут привести к серьезным проблемам, например, нежелательному изменению файлов или системной среды или даже отказу системы. В связи с этим важно проводить тестирование информационной безопасности в системах, которые не являются операционными системами, что позволит снизить риск случайного изменения или неавторизованного доступа к операционным программам и коммерческим данным в результате получения разработчиком несанкционированного доступа. Если персонал по разработке и тестированию имеет доступ к операционной системе и ее данным, он может ввести несанкционированный и непроверенный код или изменить операционные данные. В результате действий разработчиков и специалистов по тестам могут возникнуть непредвиденные изменения в ПО и информации, если у них одна вычислительная среда.

Предпочтительный способ устранения таких проблем — это использование системы, отделенной от операционной системы, в которой будет выполняться первоначальная разработка и тестирование. Если это невозможно, необходимо обеспечить, чтобы в системе использовалась правильно настроенная система управления изменениями, которая документально фиксирует любые изменения, выполненные в системе, и предусматривает возможность отмены таких изменений.

A.3.4.3.6 Управление изменениями

В зависимости от регулятивных требований в некоторых отраслях применяются системы управления изменениями для SIS. В случае полной CSMS системы управления изменениями должны использоваться для всех IACS. Процесс управления изменениями проводится после разделения должностных принципов во избежание конфликта интересов. Это означает, что один человек не имеет право одобрять изменение и реализовывать его. Компетентный в техническом плане специалист должен изучать предлагаемые изменения в IACS на предмет их потенциального влияния на риски HSE и риски информационной безопасности, руководствуясь четко определенными политиками. Если изменение нарушает одну из политик, то может потребоваться пересмотреть предлагаемое изменение силами другого компетентного персонала, который подтвердит, что оно допустимо, или отклонит такое изменение.

Для того, чтобы управление изменениями было эффективным, необходимо вести подробную регистрацию устанавливаемых программ, которая будет служить основной для предлагаемых изменений. Система управления изменениями работает на основе проверенной и документально оформленной процедуры резервирования и восстановления. Необходимо обеспечить, чтобы все системные обновления, патчи и изменения политик внедрялись в соответствии с процедурами системы управления изменениями.

A.3.4.3.7 Управление патчами

Инсталляция патчей, обновлений и изменения политик, которые выглядят безвредными по отдельности, может привести к серьезным последствиям для информационной безопасности. Равно как и ситуации, когда такие патчи и обновления не устанавливаются. Необходимо разработать способ, позволяющий определить связь и критичность уязвимостей, для которых предназначены новые патчи. Такой метод должен определять влияние на способность поддержания целевого SL, если патч устанавливается и если он не устанавливается.

Примечание — IEC/TR 62443-2-3 [5] — это плановый технический отчет об управлении патчами.

A.3.4.3.8 Резервирование и восстановление

С особым вниманием следует относиться к тому, чтобы гарантировать совместимость процессов резервирования и восстановления с целевым SL для системы. В целом, процесс резервирования и восстановления должен обеспечивать подтверждение того, что резервные копии защищены в той же степени, что и оригиналы. Для этого могут потребоваться особые процедуры, позволяющие гарантировать, что резервные копии не были повреждены и что механизмы, указывающие на успешное резервирование или восстановление, не были подвержены рискам. Устойчивость резервных копий должна постоянно проверяться с целью обеспечения гарантии того, что состояние носителя, на котором содержатся файлы, не ухудшилось и что данные на таком носителе все еще считываются и пригодны к использованию. Может потребоваться хранение неподдерживаемого оборудования в местах, в которых старые резервные копии не считываются на новом оборудовании.

A.3.4.3.9 Вспомогательные практические методы

A.3.4.3.9.1 Основные практические методы

К основным практическим методам относятся следующие действия:

a) документальное оформление требований безопасности (угрозы/контрмеры/планы тестирования);

b) привязка контрмер безопасности к требованиям безопасности;

c) определение ожидаемых ответных действий в случае неисправности;

d) определение, разработка и тестирование функциональности компонента с целью обеспечения достижения системой целевого SL;

e) проверка и валидация информационной безопасности во время тестирования компонента, интеграции и системы;

f) включение маршрута авторизации, системы резервирования и восстановления, системы управления патчами и процедуры защиты от вирусных и вредоносных программ в систему управления изменениями.

A.3.4.3.9.2 Дополнительные практические методы

К дополнительным практическим методам относятся следующие действия:

a) внедрение отдельных сред разработки, тестирования и эксплуатации;

b) применение независимых процедур верификации и валидации компонентов;

c) применение независимых верификационных и валидационных процедур для этапа интеграции;

d) применение независимых процедур верификации и валидации системы;

e) интеграция процедур управления изменениями IACS с существующими процедурами PSM.

A.3.4.3.10 Использованные ресурсы

Данный элемент частично основан на материалах [23], [38], [39].

A.3.4.4 Элемент «Управление информацией и документацией»

A.3.4.4.1 Описание элемента

Управление информацией и документацией является процессом классификации всех данных, защиты информации, управления документами и обеспечения доступности информации, связанной с IACS и CSMS. Управление документами IACS может быть включено в общую систему организации по хранению данных и управлению документацией. Управление информацией и документацией гарантирует, что данные будут доступны на протяжении требуемого периода времени в зависимости от внутренних (например, политики организации и обслуживание устройств) или внешних (например, правовых, регулятивных или политических) требований.

A.3.4.4.2 Аспекты управления информацией и документацией

Информация, связанная с CSMS организации, является важной, а зачастую секретной, поэтому необходимо осуществлять надлежащий контроль и управление такой информацией. В связи с этим организациям необходимо использовать комплексные политики управления информацией и документацией, относящейся к CSMS. Информация, связанная с разработкой и внедрением CSMS, анализы рисков, исследования последствий для бизнеса, профили допустимости рисков и аналогичная информация может являться секретной для организации и нуждаться в защите, наряду с контрмерами, принципами и стратегиями внедрения. Кроме того, меняются условия бизнеса, что требует актуализации анализов и исследований. Необходимо уделять внимание защите этой информации, а также сохранению необходимых версий. Существенной здесь является система классификации информации, которая позволяет обеспечивать надлежащий уровень защиты информационных ресурсов.

Одним из первых шагов создания системы управления информацией и документацией IACS является определение уровней классификации информации. Необходимо определить классы информации (например, конфиденциальная, для ограниченного доступа и общедоступная) для управления доступом и контролем информационных ресурсов. Уровни и соответствующие практические методы должны включать совместное использование, копирование, передачу и распространение информационных ресурсов в соответствии с требуемыми уровнями защиты.

После определения основных уровней информация, связанная с IACS (например, информация о строении системы управления, оценки уязвимости, сетевые схемы и программы производственного управления), должна быть классифицирована для определения требуемого уровня защиты. Такой уровень защиты определяется на основе секретности информации и возможных последствий ее распространения. Уровень по классификации должен указывать на необходимость и приоритетность информации, а также на ее секретность. Политики и процедуры доступа к информации и документации должны быть связаны с процедурами контроля доступа, указанными в A.3.3.5—A.3.3.7.

Для этой цели должен быть разработан и реализован процесс управления документацией жизненного цикла. Данный процесс должен включать подтверждение безопасности, доступности и пригодности конфигурации системы управления. Сюда входит логика, использованная при разработке конфигурации или программировании жизненного цикла IACS. Данный процесс также должен включать механизм обновления при внесении изменений.

Должны быть разработаны политики и процедуры, детализирующие хранение, защиту, уничтожение и утилизацию информации компании, включая письменные и электронные записи, оборудование и другие носители, содержащие информацию, с учетом выполнения нормативно-правовых требований. Политики и процедуры, разработанные для системы управления информацией и документацией IACS, должны соответствовать и быть включены в корпоративные системы управления информацией и документацией. Необходимо проводить юридическую проверку политики хранения на предмет соответствия законодательству и нормативными требованиями. Необходимо выявлять документы, требующие хранения, и документально определять период хранения.

Также необходимо принимать надлежащие меры для обеспечения того, чтобы записи, хранящиеся длительное время, могли быть извлечены (т. е. конвертировать данные в более новые форматы, сохранять устаревшее оборудование, которое может считать данные). Следует разработать методы и процедуры для предотвращения повреждения резервных копий данных. Резервные копии должны сохраняться на регулярной основе. Такие резервные копии необходимо проверять на предмет их читаемости. Также необходимо регулярно проверять и проводить испытания процедур восстановления.

Следует проводить периодический анализ уровней классификации информации и документации. Во время такого анализа должна оцениваться необходимость в принятии специальных мер контроля или особого обращения с конкретной информацией или документацией. Также необходимо разрабатывать методы повышения или снижения уровня классификации конкретной информации или документации.

Кроме того, должен проводиться периодический анализ системы управления информацией и документацией в целом. Это обеспечивает выполнение владельцами информации или документации соответствующих политик, стандартов и других требований, установленных организацией.

А.3.4.4.3 Вспомогательные практические методы

А.3.4.4.3.1 Основные практические методы

К основным практическим методам относятся следующие действия:

a) определение уровней классификации информации (т. е. конфиденциальной, с ограниченным доступом и общедоступной) для доступа и контроля, включая совместное использование, копирование, передачу и распространение в соответствии с требуемым уровнем защиты;

b) классификация всей информации (например, информация о строении системы управления, оценки уязвимости, сетевые схемы и программы производственного управления) для определения необходимости, приоритетности и требуемого уровня защиты, исходя из ее секретности и последствий;

c) регулярный анализ информации, требующей особого контроля или обращения, для подтверждения актуальности таких мер;

d) разработка и включение политик и процедур, детализирующих обновление, хранение, уничтожение и утилизацию информации, включая письменные и электронные записи, оборудование и другие носители, содержание информацию. Необходимо учитывать любые нормативно-правовые требования при разработке таких политик и процедур;

e) разработка и применение методов предотвращения повреждения данных путем резервирования и записи;

f) подтверждение безопасности, доступности и пригодности для использования конфигурации системы управления. Данное действие включает в себя логику, использованную при разработке конфигурации или программировании жизненного цикла IACS.

А.3.4.4.3.2 Дополнительные практические методы

К дополнительным практическим методам относятся следующие действия:

a) реализация соответствующих мер, гарантирующих возможность извлечения информации, хранящейся длительное время (т. е. конвертирование данных в более новые форматы или сохранение устаревшего оборудования, считывающего данные).

Пример — Данные о выбросах, записанные более десятилетия назад в системе, которой более не существует, или в проприетарном формате;

b) проведение периодической проверки выполнения политики управления информацией и документацией;

c) проведение юридической проверки политики хранения информации для обеспечения выполнения законодательства и нормативных требований;

d) шифрование обмена информацией в Интернете, включающего передачу конфиденциальной информации, с помощью протокола SSL или шифрования аналогичного уровня.

А.3.4.4.4 Использованные ресурсы

Данный элемент основан частично на материалах [6], [23], [24], [26].

А.3.4.5 Элемент «Планирование и реагирование на инциденты»

А.3.4.5.1 Описание элемента

Планирование и реагирование на инциденты относится к постоянному отслеживанию инцидентов кибербезопасности, а также быстрого выявления и реагирования на такие инциденты. Не имеет значения, насколько хорошо защищена система. Всегда существует возможность нежелательных проникновений, которые могут подвергнуть систему риску. Уязвимости в технологии остаются, а количество и сложность внешних угроз продолжает расти, создавая необходимость в надежной стратегии планирования и реагирования. Планирование и реагирование на инциденты позволяет организации заранее определить, каким образом она будет определять инциденты в сфере кибербезопасности и реагировать на них. Это позволяет организации предпринимать предупреждающие меры по программе кибербезопасности вместо реагирования на произошедшие события.

Планирование и реагирование на инциденты предоставляет организации возможность планировать инциденты в сфере безопасности, а затем реагировать на них согласно установленным практикам. Цели планирования и реагирования на инциденты очень схожи с целями планирования непрерывности бизнеса, но обычно они относятся к менее масштабным и более приближенным по времени инцидентам. Часть плана инцидентов должна включать процедуры реагирования организации на инциденты, включая процессы оповещения, документирования, расследования и последующего контроля. Реагирование на аварийные ситуации, обеспечение безопасности персонала и восстановление работоспособности системы являются составляющими процесса реагирования на инцидент. Раннее выявление инцидента и соответствующее реагирование может ограничить ущерб/последствия события.

Планирование и реагирование на инциденты являются ключевым элементом системы управления для любого типа риска организации, включая риски кибербезопасности. Разумные практики управления информацией признают необходимость официального планирования и реагирования на инциденты на месте.

Существуют три основные стадии планирования и реагирования на инциденты: планирование, реагирование и восстановление. Стадия планирования включает первичную разработку программы для системы и многовариантное планирование. Стадия реагирования подразумевает способность реагирования на фактические инциден-

ты. На стадии восстановления система промышленной автоматики и контроля восстанавливается до предшествующего рабочего состояния.

А.3.4.5.2 Стадия планирования

Для распознавания инцидентов и реагирования на них в среде IACS необходимо разработать программу. Такая программа должна включать письменный план, документирующий типы рассматриваемых инцидентов и ожидаемые действия при реагировании на каждый из таких инцидентов.

План инцидентов должен включать в себя типы инцидентов, которые могут произойти, и ожидаемые действия при реагировании на такие инциденты. Должны быть выявлены и классифицированы типы инцидентов, которые могут вызвать проникновение в систему, по воздействию и вероятности, чтобы для каждого возможного инцидента была выработана надлежащая стратегия реагирования. План должен включать пошаговые действия, предпринимаемые различными организациями. Если существуют требования по сообщению об инциденте, они должны быть указаны наряду с тем, куда следует сообщать об инциденте, а также с указанием телефонных номеров для уменьшения дезорганизации при сообщении. Во время составления плана реагирования на инциденты различные заинтересованные стороны должны предоставить информацию, включая информацию о деятельности, управлении, правовых вопросах и безопасности. Такие заинтересованные стороны также подписывают и утверждают план.

План инцидентов должен включать многовариантные планы, включающие полный спектр последствий возможного выхода из строя программы кибербезопасности IACS. Многовариантные планы должны включать в себя процедуры отделения IACS от всех несущественных кабелей, которые могут являться векторами атак, процедуры защиты важных кабелей от последующих атак и процедуры восстановления IACS до предыдущего известного состояния в случае инцидента. Также необходимо проводить периодическую проверку планов в целях обеспечения их выполнения.

Еще одним важным типом информации, который должен включаться в план инцидентов, является контактная информация для всего персонала, ответственного за реагирование на инциденты в организации. При возникновении инцидента могут возникнуть трудности с определением местонахождения этой информации.

После составления плана инцидентов организации необходимо разослать его копии соответствующим группам персонала в организации, а также за ее пределами. Весь соответствующий персонал и организации должны быть осведомлены о своих обязанностях, выполняемых до, во время и после инцидентов.

Кроме передачи плана всем соответствующим организациям, план необходимо периодически проверять для обеспечения его актуальности. Организация должна проводить практическую отработку плана реагирования на инциденты и анализировать ее результаты. Любые проблемы, выявленные во время отработки, должны быть решены, а план должен быть актуализирован.

А.3.4.5.3 Стадия реагирования

Существует несколько способов реагирования на инциденты безопасности. Они ранжируются от отсутствия каких-либо действий до полной остановки системы. Конкретный тип реагирования зависит от типа инцидента и его влияния на систему. Необходимо составить письменный план на стадии планирования, в котором будут четко указаны типы инцидентов, которые могут произойти, и ожидаемый тип реагирования на такие инциденты. Такой план будет служить руководством при возникновении замешательства или стресса из-за инцидента.

Организации необходимо разработать процедуры для выявления и уведомления об инцидентах. Эти процедуры должны являться руководством в отношении того, что необходимо считать инцидентом, каким образом о возможных инцидентах необходимо сообщать и каким образом их классифицировать. Такое руководство должно включать в себя информацию о распознавании и уведомлении о необычных событиях, которые могут быть инцидентами в системе кибербезопасности. Процедуры также должны включать в себя любые особые обязанности (например, методы идентификации, требования сообщения об инцидентах и конкретные действия), о которых персонал должен быть осведомлен при разрешении инцидентов в системе кибербезопасности.

При обнаружении инцидента необходимо зафиксировать информацию о таком инциденте с указанием самого инцидента, предпринятых действий, сделанных выводов и любых действий, предпринятых для модификации CSMS ввиду такого инцидента. Информацию об инциденте необходимо сообщить всем соответствующим группам в организации (например, руководству и отделам IT, технологической безопасности, проектирования систем автоматизации и управления и производства) и любым сторонним организациям, на которые повлиял инцидент. Необходимо обеспечить своевременное предоставление такой информации, чтобы помочь организации предотвратить последующие инциденты.

Учитывая, что не все инциденты могут быть первоначально распознаны или обнаружены, в организации должны существовать процедуры для определения неудачных и удачных попыток нарушения кибербезопасности. В зависимости от масштабов ущерба, причиняемого конкретным инцидентом, может возникнуть необходимость в консультации экспертов для определения корневой причины инцидента, оценки эффективности реагирования и в случае международного ущерба для сохранения цепочек свидетельств — для судебного преследования преступника. Если в критически важной IACS происходит инцидент, приводящий к прерыванию непрерывности бизнеса, целью, возможно, будет являться восстановление рабочего состояния оборудования в кратчайшие сроки. Это может подразумевать переформатирование жестких дисков и полную перезагрузку OS и приложений, что, возможно, удалит все данные для экспертной оценки. Определение приоритетов и практик реагирования на инциденты имеет первостепенное значение для понимания всем персоналом целей и методов.

A.3.4.5.4 Стадия восстановления

Результаты инцидента могут быть незначительными или могут вызывать большое количество проблем в системе. Пошаговые действия по восстановлению должны быть документированы, чтобы система вернулась к нормальной работе в кратчайшие сроки и в безопасном режиме.

Важным компонентом стадии восстановления является восстановление систем и информации (т. е. данных, программ и наборов параметров) до рабочего состояния. Это требует наличия системы резервирования и восстановления, достаточной для работы с целой IACS. Она может состоять из одного или нескольких физических устройств резервирования и восстановления, которые должны работать совместно для восстановления IACS.

В организации должен быть определен процесс анализа инцидентов для решения выявленных проблем и обеспечения их исправления. Результаты процесса анализа должны быть отражены в соответствующих политиках и процедурах кибербезопасности, технических контрмерах и планах реагирования на инциденты. Инциденты, относящиеся к кибербезопасности, можно разделить на три категории:

- вредоносные коды, например, вирусы, черви, боты, руткиты и трояны;
- случайная утрата доступности, целостности или конфиденциальности информации (включая эксплуатационную готовность);
- несанкционированное проникновение, включая физический доступ.

Управление инцидентами в первых двух категориях обычно осуществляется за счет процесса реагирования на инциденты IT-безопасности. Управление третьей категорией обычно осуществляется при содействии специалистов по охране труда, технике безопасности и охране окружающей среды, а также руководства площадки.

A.3.4.5.5 Вспомогательные практические методы

A.3.4.5.5.1 Основные практические методы

К основным практическим методам относятся следующие действия:

a) создание процедур для всей организации в целях распознавания и сообщения о необычных событиях, которые могут являться инцидентами кибербезопасности;

b) создание процедур планирования и реагирования на инциденты, включая:

- назначение лица, ответственного за реализацию плана при возникновении необходимости;
- определение структуры вызываемой группы реагирования на инциденты, включающей специалистов по IT-безопасности и IACS и дополнительный персонал;
- определение ответственности за координирование защиты и реагирования на инцидент;
- рассмотрение инцидента от возникновения до окончательного анализа;
- создание процедур выявления и определения категории и приоритетности инцидентов;
- создание процедур для различных типов инцидентов, например, атак DoSa, взлома системы, вредоносного кода, несанкционированного доступа и ненадлежащего использования;

c) определение профилактических мер для автоматического выявления инцидентов на ранней стадии;

d) предплановое реагирование на сценарии угроз, выявленные оценкой уязвимости и рисков;

e) сообщение об инцидентах в системе промышленной автоматики и контроля всем соответствующим организациям, включая организации, занимающиеся IT, безопасностью производственной деятельности, проектированием систем автоматизации и контроля и эксплуатацией, для их осведомленности.

f) сообщение о количественных показателей и инцидентах исполнительному руководству;

g) выполнение регулярного анализа прошлых инцидентов для совершенствования CSMS;

h) фиксирование информации об инцидентах, сделанных выводов и любых действий, которые были предприняты для модификации CSMS в отношении инцидента;

i) практическая отработка плана. Проведение совещаний после отработки для выявления областей совершенствования.

A.3.4.5.5.2 Дополнительные практические методы

К дополнительным практическим методам относятся следующие действия:

a) разработка внутренних или внешних средств судебной экспертизы для IACS;

b) разработка процесса немедленного сообщения об инцидентах кибербезопасности. Обеспечение связи процесса с группой кризисного управления организации. Обучение персонала на примерах регистрируемых инцидентов, чтобы он мог более тщательно выполнять требования по сообщению об инцидентах;

c) понимание любых возможных связей между IT, безопасностью и IACS и использование этих знаний в комплексных процедурах реагирования на инциденты безопасности;

d) разработка, испытание, применение и документирование процесса расследования инцидентов;

e) разработка корпоративных политик сообщения об инцидентах кибербезопасности и предоставления информации об инцидентах отраслевым группам и государственным органам, если это допускается корпортивными политиками;

f) определение ролей и обязанностей в отношении выполнения местного законодательства и/или других важных заинтересованных сторон в программах внутреннего и совместного расследования инцидентов;

g) расширение рамок расследования инцидента, исходя из возможного результата инцидента, а не только фактического результата, признания того, что киберинцидент может включать злой умысел. Может потребоваться повышение уровня расследования инцидента в зависимости от его серьезности;

h) разработка методов и механизмов определения корректирующих действий по результатам инцидента кибербезопасности или проведения практической отработки;

i) обучение реагированию на инциденты в сфере безопасности учебных групп, включающих специалистов разного профиля;

j) анализ окончательных результатов расследования инцидента совместно со всем персоналом, выполняющим служебные функции, имеющие отношение к результатам расследования. Анализ инцидента с учетом тенденций и его регистрация для использования при последующем анализе тенденций;

k) развитие взаимного сотрудничества между конкурирующими компаниями и компаниями отрасли для изучения чужого опыта оценки, реагирования, расследования, сообщения и коррекции инцидентов кибербезопасности;

l) выявление непредвиденных последствий, в особенности тех, которые могут повлиять на будущую реализацию плана. Инциденты могут включать рисковые события, угрозы серьезного инцидента и неисправности. Также необходимо включать обнаруженные или подозреваемые слабые стороны системы или риски, которых ранее могло не быть;

m) включение планирования реагирования на аварийные ситуации в процесс планирования реагирования на инциденты.

A.3.4.5.6 Использованные ресурсы

Данный элемент частично основан на материалах [26] и [36].

A.4 Категория «Контроль и совершенствование системы управления кибербезопасностью»

A.4.1 Описание категории

CSMS включает все меры, необходимые для создания и реализации программы кибербезопасности. Объем и уровень этих работ зависит от целей организации, границ допустимости рисков и степени завершенности программы кибербезопасности. Система управления должна включать в себя требования, методы, устройства, интерфейсы и описание персонала, необходимого для реализации программы кибербезопасности.

Контроль и совершенствование CSMS подразумевает обеспечение использования системы, а также анализ эффективности самой системы. На рисунке A.19 представлены две составляющих категории:

- выполнение норм;
- анализ, совершенствование и поддержание CSMS.



Рисунок A.19 — Графическое представление категории «Контроль и совершенствование CSMS»

A.4.2 Элемент «Выполнение норм»

A.4.2.1 Описание элемента

Выполнение норм является процессом подтверждения выполнения организацией разработанной программы кибербезопасности. Успешность CSMS всецело зависит от способности организации следовать ей. Организация должна нести ответственность за выполнение политик и процедур, являющихся частью CSMS, в противном случае, система управления будет неэффективной. Подтверждая соответствие CSMS, организация может использовать встроенные процессы системы для совершенствования всей системы в будущем.

В процесс подтверждения соответствия CSMS входят запланированные и незапланированные мероприятия. Периодический анализ CSMS считается запланированным мероприятием, а реагирование на инцидент кибербезопасности с большей вероятностью будет считаться незапланированным мероприятием.

Определение ключевых показателей эффективности (KPI) дает организации возможность измерять эффективность CSMS. Использование KPI, соответствующих лучшим решениям отраслевых групп или других организаций, позволяет проводить сравнительный анализ CSMS.

A.4.2.2 Запланированные и незапланированные мероприятия

Многие подпункты CSMS включают идею периодического анализа какой-либо позиции для контроля или совершенствования CSMS во времени. Такой анализ является частью модели развитости программы безопасности, рассмотренной в IEC/TS 62443-1-1. Анализы, проводимые в рамках CSMS, не позволяют системе деградировать со временем из-за появления новых угроз, уязвимостей или ситуаций, которых не существовало на момент разработки системы.

Могут также существовать критические угрозы, уязвимости и ситуации, которые необходимо разрешать до следующего запланированного периода анализа. Эти действия относятся к незапланированным мероприятиям и могут потребовать повторной оценки CSMS для обеспечения эффективности.

Периодические анализы и аудиты CSMS позволяют выявить, были ли требуемые политики, процедуры и контрмеры реализованы надлежащим образом и выполняются ли они, так как предполагалось. В среде IACS аудиторам необходимо полностью ознакомиться с политиками и процедурами кибербезопасности и конкретными рисками охраны труда, техники безопасности и охраны окружающей среды, связанными с конкретным предприятием и/или промышленной деятельностью. Необходимо обеспечивать, чтобы аудит не вмешивался в функции управления, выполняемые оборудованием IACS. Может понадобиться отключение системы перед проведением аудита. В ходе аудита необходимо проверить следующее:

- политики, процедуры и контрмеры, имевшиеся во время приемочных испытаний системы, все еще установлены и надлежащим образом функционируют в OS;
- OS не содержит угроз для безопасности.

Примечание — При возникновении инцидента должны создаваться записи о характере и масштабах инцидента;

- процедура управления изменениями программы строго соблюдается, при этом имеется журнал контроля с указанием всех проверок и одобрений изменений.

Добавление или удаление имущественных объектов из IACS может быть незапланированным действием, приводящим к проверке CSMS. Распространенной практикой во время технического обслуживания или переоборудования системы является добавление, модернизация или удаление оборудования или ПО из IACS. Четко определенный и выполняемый процесс управления изменениями зафиксирует это, что может привести к проверке или аудиту CSMS. Такая проверка или аудит обеспечит отсутствие негативного влияния такого изменения на кибербезопасность IACS. Еще одним примером незапланированного действия является реагирование на вирусную атаку на предприятие. После того, как CSMS была использована для реагирования и восстановления после инцидента необходимо провести проверку или аудит CSMS, чтобы определить, какая неисправность привела к возможности распространения вируса.

Проверка или аудит (внутренний или внешний) кибербезопасности предоставляет организации ценные данные для совершенствования CSMS. Результаты таких проверок или аудитов должны включать необходимое количество подробной информации, чтобы обеспечить выполнение всех правовых и нормативных требований, а также внесение всех изменений, предписанных проверкой или аудитом. Результаты направляются всему соответствующему персоналу (т. е. заинтересованным сторонам, руководителям и персоналу, занимающемуся безопасностью).

A.4.2.3 Ключевые показатели эффективности

KPI позволяют организации определить, насколько эффективно функционирует CSMS, а также направить ресурсы в области, которые необходимо усовершенствовать. KPI должны представлять собой, по возможности, количественные показатели (т. е. цифры и процентные доли), указывающие насколько эффективно функционирует определенная часть CSMS относительно ожидаемых условий.

Учитывая, что результаты проверок или аудитов CSMS выражаются с использованием KPI, большое значение имеет выбор показателей, которые являются актуальными, значимыми и соответствующими CSMS и другим требованиям организации. Результаты периодических запланированных действий могут быть выражены в виде показателей эффективности по сравнению с набором заданных показателей для отражения эффективности и тенденций безопасности. Результаты незапланированных действий могут быть выражены в виде эффективности работы CSMS при возникновении незапланированного события или инцидента.

Данные о кадрах должны являться частью показателей эффективности. Компании должны отслеживать процентную долю персонала, назначенного для работы с IACS, и процентную долю персонала, прошедшего обучение и соответствующего квалификационным требованиям для выполнения соответствующей роли. Несмотря на то, что такие данные могут показаться непонятными, с их помощью системные проблемы могут быть обнаружены ранее, чем с помощью результатов некачественного аудита.

Сравнительный анализ KPI и результатов проверок или аудитов по сравнению с другими организациями или требованиями является хорошим методом подтверждения эффективности CSMS. Если сравнительные данные собираются за определенный период времени, организация может определить тенденции угроз или контрмер. Такие тенденции могут указывать на места, в которых CSMS должна быть проанализирована в рамках подпункта об анализе, совершенствовании и поддержании системы (см. A.4.3).

A.4.2.4 Вспомогательные практические методы

A.4.2.4.1 Основные практические методы

К основным практическим методам относятся следующие действия:

a) получение гарантий пригодности среды управления и выполнения общих целей кибербезопасности. Определение влияния на безопасность добавления, модернизации или устранения объектов (т. е. патчи ПО, модернизация приложений и изменение оборудования);

b) подтверждение, что в течение конкретного периода между аудитами все аспекты CSMS функционируют надлежащим образом. Должно быть запланировано достаточное число аудитов, чтобы задачи аудита были равномерно распределены в течение выбранного периода. Руководство должно обеспечивать периодическое проведение аудитов. Руководство должно также обеспечивать информацию о том, что существует подтверждение:

- проверки выполнения документированных процедур и достижения требуемых целей;

- установки и надлежащей и непрерывной работы технических средств контроля (т. е. брандмауэров и средств контроля доступа).

А.4.2.4.2 Дополнительные практические методы

К дополнительным практическим методам относятся следующие действия:

a) построение программы количественных показателей кибербезопасности на основе ключевых действий, описанных ниже:

1) определение цели (целей) программы количественных показателей;

2) принятие решения о том, какие количественные показатели должны быть предусмотрены для измерения степени внедрения и выполнения политик и процедур, определенных в CSMS:

- предварительная оценка любых возможных уязвимостей безопасности (например, процент слабых сторон безопасности, выявленных аудитом, которые должны быть исправлены к конкретной дате);
- отслеживание реализации и использования мер безопасности и превентивных мер (например, процент выполнения стандартов безопасности);

3) разработка стратегий определения количественных показателей;

4) определение контрольных показателей и целей;

5) определение того, каким образом и кому предоставляется информация о значениях количественных показателей;

6) создание и выполнение плана действий;

7) создание официального плана анализа/доработки программы;

b) анализ результатов аудитов, самостоятельно проведенных оценок, отчетов об инцидентах кибербезопасности и обратной связи, регулярно предоставляемой ключевыми заинтересованными сторонами для определения эффективности CSMS;

c) проведение анализов операционной безопасности IACS с помощью инженеров, прошедших обучение по безопасности IACS. Кроме того, вопросы безопасности подвергаются более обширному анализу государственным органом.

А.4.2.5 Использованные ресурсы

Данный элемент был частично основан на материалах [24], [26], [35], [49], [50].

А.4.3 Элемент «Анализ, совершенствование и поддержание системы управления кибербезопасностью»

А.4.3.1 Описание элемента

Процесс непрерывного мониторинга и анализа CSMS позволяет организации получить подтверждение, что она достигает целей и выполняет политики и процедуры, заложенные в CSMS. KPI, определенные при разработке CSMS, используются для оценки эффективности CSMS во время процесса анализа выполнения норм. Элемент «Выполнение норм» предназначен для проверки того, что CSMS функционирует надлежащим образом, в то время как настоящий элемент предназначен для проверки того, что требования, использованные для разработки CSMS, соответствуют целям по кибербезопасности организации.

Методы внутренней проверки, например, аудиты соответствия и расследование инцидентов, позволяют организации определить эффективность системы управления и соответствие ее работы ожиданиям. Также важно определить, выполняет ли система управления цели и задачи, установленные во время процесса планирования. Если существуют отклонения от первоначальных целей и задач, может понадобиться внесение системных изменений в систему управления.

Поскольку угрозы и технологии обеспечения безопасности находятся в постоянном развитии, программа кибербезопасности организации тоже должна развиваться с учетом новых угроз и доступных возможностей. Организации должны отслеживать, проверять и совершенствовать мероприятия по обеспечению безопасности персонала, имущества, продукции, производственной деятельности, данных и информационных систем.

Общей целью является обеспечение того, чтобы CSMS оставалась эффективной при внесении изменений, основаных на появлении новых угроз, возможностей и регулярных анализов. Непрерывное внимание к безопасности является для персонала показателем того, что кибербезопасность является основной ценностью компании.

А.4.3.2 Анализ соответствия CSMS

Соответствие CSMS рассматривалось в одном из предыдущих элементов. Оно предназначено для проверки выполнения организацией политик и процедур, заложенных в CSMS. В рамках процесса определения соответствия были установлены ключевые показатели эффективности для измерения эффективности CSMS организации. Неудовлетворительные значения KPI в одном цикле анализа могут указывать на одиночную проблему, которая может быть исправлена простыми способами. Неудовлетворительные значения многих KPI или у одного и того же KPI при повторных проверках могут указывать на системные проблемы в CSMS. Это может указывать также на необходимость повышения уровня обучения или контроля выполнения, недостаточное количество ресурсов или нецелесообразность реализованных процедур. Принятие указанных решений входит в процесс управления CSMS. Для решения указанных вопросов необходимо проконсультироваться с организацией, действия которой контролируются вне зависимости от того, оценивается ли KPI в ходе независимого или внутреннего аудита.

Важно, чтобы CSMS включала в себя требования по улучшению результатов проверки соответствия. Необходимо назначить ответственное лицо для разработки долговременной стратегии совершенствования в целях обеспечения последовательного и экономически целесообразного совершенствования во времени.

A.4.3.3 Оценка и анализ эффективности CSMS

Оценка эффективности CSMS включает в себя анализ информации об инцидентах. Чем больше у организации возможностей выявления успешных и неудачных попыток нарушения кибербезопасности и фиксирования таких инцидентов, тем больше возможность оценки эффективности CSMS при снижении риска. Информация об инциденте включает количество инцидентов, тип или класс инцидентов и экономические последствия инцидентов. Такая информация является чрезвычайно важной для понимания текущего экономического воздействия угроз кибербезопасности и для оценки эффективности конкретных применяемых контрмер.

В то время, как анализ информации об инциденте позволяет оценить эффективность CSMS в прошлом, управление системой также предназначено для поддержания эффективности системы в будущем. Для достижения этого необходимо контролировать изменение факторов, которые могут повысить или уменьшить эффективность в перспективе. Ключевыми факторами контроля являются:

- уровень риска, который может измениться в связи с изменением угроз, уязвимости, последствий или вероятности;
- границы допустимости рисков организации;
- внедрение новых или измененных систем или производственной деятельности;
- отраслевые практики;
- доступные технические и нетехнические контрмеры;
- правовые и нормативные требования.

CSMS организации должна регулярно проверяться с целью оценки ее эффективности в прошлом и будущих перспектив. Такая проверка должна включать периодическую оценку политик и процедур кибербезопасности для подтверждения того, что такие политики и процедуры существуют, функционируют и соответствуют правовым, нормативным и внутренним требованиям безопасности. В соответствующих обстоятельствах также выполняется оценка политик и процедур бизнес-партнеров организации, например, поставщиков продукции и услуг, совместных предприятий или заказчиков.

Помимо регулярных проверок, проверки соответствующих аспектов CSMS могут вызвать значительные изменения перечисленных выше факторов. Организация должна определить набор триггеров и пороговых значений изменений, приводящих к проверкам. Триггеры могут включать следующие факторы:

- внутренние: исходя из эффективности CSMS и значений KPI и других подходящих внутренних показателей (например, допустимости рисков, изменений в управлении и т. д.);
- внешние: изменения в среде угроз, передовых отраслевых практиках, имеющихся решениях и правовых требованиях могут указывать на необходимость или возможность совершенствования CSMS.

Организация, назначенная для управления изменениями в CSMS, должна нести ответственность за анализ триггеров и пороговых значений для изменений и использования их для начала процесса проверки.

A.4.3.4 Правовые и нормативные последствия для CSMS

Нормативные и правовые требования, под которые подпадает организация, могут изменяться со временем. Организация может выполнять первоначальные требования к CSMS, но CSMS может не соответствовать действующим нормативным и правовым требованиям.

Организация должна периодически анализировать действующие нормативные и правовые требования и определять области, которые могут оказывать влияние на CSMS. Также при внесении значительных изменений в нормативные и правовые требования необходимо проводить проверку CSMS на соответствие новым требованиям.

A.4.3.5 Управление изменениями в CSMS

Для того, чтобы создать скоординированную систему, необходимо назначить организацию/группу специалистов для управления и координирования оптимизации и реализации изменений CSMS. Такая организация/группа специалистов, вероятно, будет организацией матричного типа, привлекающей ключевых специалистов из различных деловых организаций. Для внесения и реализации изменений такая группа специалистов должна использовать определенный метод.

Необходимость изменений CSMS обусловливается рядом внутренних и внешних факторов. Управление этими изменениями требует координирования действий с различными заинтересованными сторонами. При внесении изменений в систему управления необходимо оценить возможные побочные последствия, относящиеся к работе и безопасности системы. При совершенствовании безопасности IACS также необходимо учитывать различные организации, практики и требования реагирования на инциденты.

Для управления изменениями CSMS необходимо разработать письменные процедуры. Этот процесс может включать следующие действия:

a) Изучение существующей системы управления

До улучшения CSMS необходимо изучить и понять существующую систему управления. Все политики, относящиеся к кибербезопасности, должны быть проанализированы, чтобы все заинтересованные стороны четко понимали действующую политику и способ ее реализации. Кроме того, должны быть определены все имущественные объекты и процедуры, относящиеся к CSMS;

b) Определение процедур внесения предложений и оценки изменений CSMS

После рассмотрения существующей системы управления она должна быть проверена на соответствие и эффективность, как указано выше. Должны быть выявлены слабые стороны или разрывы в системе управления и предложены корректирующие действия. Оценка системы управления должна выявлять области, где могут

потребоваться изменения. Кроме того, необходимо рассмотреть передовые отраслевые практики и требования, описанные в настоящем стандарте, при определении изменений, усиливающих CSMS. Выбор новых контрмер должен проводиться в соответствии с принципами, указанными в элементе «Управление рисками и реализация» настоящего стандарта (см. А.3.4.2). После определения предлагаемых изменений они должны быть кратко задокументированы для предоставления другим заинтересованным сторонам;

c) Выдвижение предложений и оценка изменений CSMS

После выявления и документирования изменений они должны быть предоставлены заинтересованным сторонам. Необходимо провести анализ предлагаемых изменений, чтобы определить, оказывают ли они какое-либо негативное или непредвиденное побочное воздействие. Они также должны быть оценены для определения, имеется ли необходимость во внесении каких-либо изменений в CSMS по сравнению с первоначальными требованиями и сериями испытаний. По мере появления новых возможностей многие организации внедряют новейшие технологии в систему. В среде IACS необходимо проверить технологию или решение кибербезопасности перед внедрением;

d) Реализация изменений в CSMS

После согласования изменения заинтересованными сторонами изменения они должны быть реализованы в CSMS. Изменения в политики должны вноситься в соответствии с процедурой компании, относящейся к внесению изменений в политики, и такие изменения должны быть, как минимум, задокументированы с получением письменного одобрения ключевых заинтересованных сторон. Особое внимание необходимо уделять испытанию и проверке системы, а также участию поставщика средств управления;

e) Контроль изменений в CSMS

После внедрения новой или пересмотренной CSMS необходимо контролировать и оценивать ее эффективность. Необходимо проводить проверку системы управления на регулярной основе, а также при внесении любых изменений в систему.

А.4.3.6 Вспомогательные практические методы

А.4.3.6.1 Основные практические методы

К основным практическим методам относятся следующие действия:

a) использование метода инициации проверки уровня остаточного риска и допустимости риска при возникновении изменений в организации, технологии, целях бизнеса, производственной деятельности или внешних событиях, включая выявленные угрозы и изменения в социальном климате;

b) анализ, фиксирование и сообщение информации о функционировании для оценки эффективности CSMS;

c) анализ результатов периодических проверок и аудитов CSMS для определения необходимости в изменениях;

d) выявление неэффективных политик и процедур CSMS для определения ключевых причин системных проблем. Необходимо определить мероприятия не только для решения проблемы, но и для минимизации и предотвращения повторений;

e) анализ потенциальных угроз и последствий на регулярной основе для определения требуемых контрмер;

f) выявление действующих и измененных норм и законодательства, а также контрактных обязательств и требований по кибербезопасности;

g) участие ключевых заинтересованных сторон в организации определения областей дальнейшего исследования и планирования. К ключевым заинтересованным сторонам относится персонал из всех групп, на которые оказывает влияние CSMS (т. е. IT, IACS и безопасность);

h) определение уместных корректирующих и превентивных мероприятий для дальнейшего совершенствования функционирования;

i) определение приоритета улучшений CSMS и разработка планов для реализации таких улучшений (т. е. планирование бюджетов и проекта);

j) реализация всех изменений с помощью процесса управления изменениями в организации. Особое внимание необходимо уделять испытанию и проверке систем и участию поставщика средств управления в связи с последствиями, связанными с охраной труда, техникой безопасности и охраной окружающей среды, для среды IACS;

k) проверка реализации согласованных действий, определенных предыдущими аудитами и проверками;

l) предоставление планов действий и областей совершенствования всем заинтересованным сторонам и соответствующему персоналу.

А.4.3.6.2 Дополнительные практические методы

К дополнительным практическим методам относятся следующие действия:

a) построение программы количественных показателей кибербезопасности на основе ключевых действий, описанных ниже:

1) определение цели (целей) программы количественных показателей;

2) принятие решения о том, какие количественные показатели должны быть пересмотрены для измерения степени внедрения и выполнения политик и процедур, определенных в CSMS.

Примечание — Рекомендуется провести ретроспективную оценку готовности системы безопасности, отслеживая количество и серьезность прошлых инцидентов системы безопасности, включая шаблонные незначительные события;

3) разработка стратегий определения количественных показателей;

4) определение контрольных показателей и целей;

5) определение того, каким образом и кому предоставляется информация о значениях количественных показателей;

6) создание и выполнение плана действий;

7) создание официального плана анализа/доработки программы;

b) применение большого количества разных стратегий, способствующих постоянному совершенствованию мероприятий обеспечения кибербезопасности. Стратегии должны быть соизмеримы с риском и зависеть от корпоративной культуры, существующих систем, размера и сложности цифровых систем. К потенциальным стратегиям относятся следующие:

- проведение сравнительного анализа в сфере безопасности в пределах отрасли и за ее пределами, включая использование внешних проверок для содействия при утверждении изменений;
- обеспечение обратной связи от персонала в форме предложений по безопасности и донесение до высшего руководства соответствующих недостатков и возможностей повышения эффективности;
- использование стандартных корпоративных бизнес-методик, например, методики «Six Sigma™», для измерения, анализа, совершенствования и подтверждения совершенствования кибербезопасности.

A.4.3.7 Использованные источники

Данный элемент частично основан на материалах [24], [26], [35], [49].

Приложение В
(справочное)

Процесс разработки системы управления кибербезопасностью

В.1 Обзор

В разделе 4 и приложении А настоящего стандарта рассмотрены отдельные элементы, связанные с комплексной CSMS. Разработка функционирующей CSMS представляет собой процесс, который может занять месяцы или даже годы. Настоящее приложение описывает упорядочивающий и повторяющейся характер мероприятий, связанных с разработкой элементов CSMS. Целями настоящего приложения являются:

- обеспечение понимания того, как успешные организации определяют последовательность таких мероприятий и рассмотрение наиболее распространенных заблуждений, относящихся к порядку создания элементов CSMS;
- предоставление пошагового руководства, которым организация может пользоваться в начале процесса создания CSMS;
- предоставление пошагового руководства по использованию настоящего стандарта.

В.2 Описание процесса

На рисунке В.1 показано шесть мероприятий верхнего уровня CSMS и взаимосвязь между ними. На рисунках, представленных далее в настоящем приложении, эти элементы будут показаны более подробно. В то время, как на рисунке В.1 показаны взаимосвязи между всеми мероприятиями, не все из этих взаимосвязей будут подробно показаны далее в настоящем приложении. Это было сделано для сбалансирования краткости изложения с полнотой рассматриваемых тем.

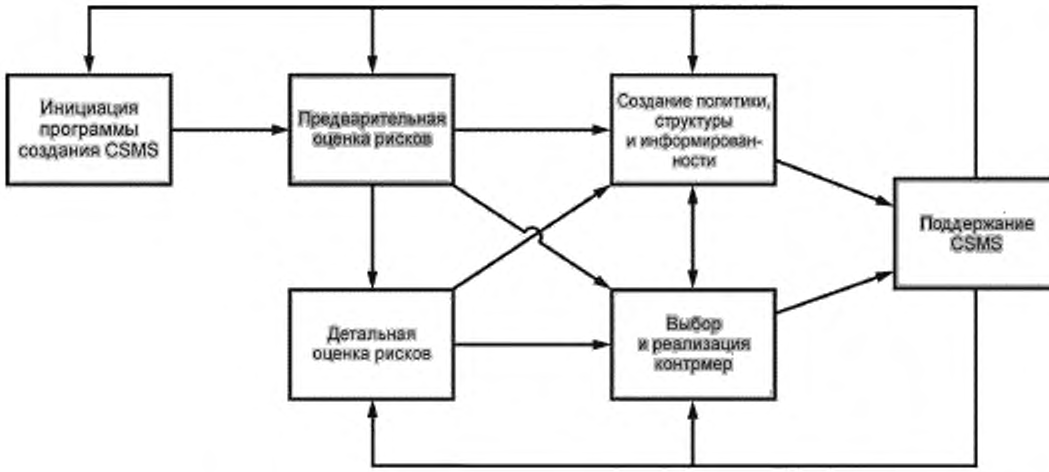


Рисунок В.1 — Мероприятия верхнего уровня для создания CSMS

Мероприятие «Инициация программы создания CSMS» создает прочную основу для программы путем определения цели, организационной поддержки, ресурсов и масштабов системы. Первоочередная реализация данного мероприятия максимизирует эффективность работ аналогично любой программе с широким влиянием. Начальный масштаб может быть меньше, чем необходимо, но он может увеличиваться по мере развития программы.

Содержание CSMS определяется оценкой рисков. Мероприятие «Предварительная оценка рисков» включает описание угроз, вероятности их материализации, общих типов уязвимостей и последствий. Детальная оценка рисков добавляет подробную техническую оценку уязвимости в общую картину рисков. Распространенным заблуждением является использование ресурсов на ранней стадии для проведения детальной оценки уязвимости и последующее получение апатичной реакции на эти результаты, поскольку не был определен общий контекст общей укрупненной оценки рисков.

Мероприятия «Создание политики, структуры и информированности» и «Выбор и реализация контрмер» напрямую снижают риск для организации. Эти мероприятия применяют как решения, принятые на нижнем уровне, так и решения, принятые на высшем уровне, и зависят от предварительной и детальной оценки рисков. Мероприятие «Создание политики, структуры и информированности» включает в себя создание политик и процедур, распределение организационных обязанностей, а также планирование и проведение обучения. Мероприятие «Выбор и реализация контрмер» определяет и внедряет технические и нетехнические средства защиты кибербезопасности организации. Реализация этих двух основных мероприятий должна быть скоординирована, поскольку в большинстве случаев для эффективности контрмер существенными являются соответствующие политики и процедуры, обучение и распределение ответственности.

Мероприятие «Поддержание CSMS» включает задачи определения выполнения организацией политик и процедур CSMS, эффективности системы управления кибербезопаностью при выполнении целей организации в сфере кибербезопасности, а также необходимости изменения таких целей с учетом внутренних или внешних событий. Это мероприятие определяет, когда требуется провести пересмотр предварительной или детальной оценки рисков, или может ускорить изменение первоначальных параметров программы. Оно также может предоставить информацию для задействования политик, процедур, организационных решений или обучения в максимизации эффективности контрмер или выявлении слабых сторон, которые должны быть усилены при реализации выбранных контрмер. По сообщениям организаций реализация мероприятия «Поддержание CSMS» является очень трудоемкой, поскольку первоначальный энтузиазм в отношении программы может угаснуть и могут появиться другие приоритеты. Однако, без уделения достаточного внимания этому мероприятию положительные результаты программы будут в конечном итоге утеряны, поскольку среда, в которой функционирует программа, не является статичной.

Оставшаяся часть настоящего приложения дает читателю более четкое представление о шести мероприятиях CSMS верхнего уровня. Номер элемента или подэлемента указывается для помощи пользователю настоящего стандарта при поиске более подробной информации по конкретной теме.

B.3 Мероприятие «Инициация программы создания CSMS»

На рисунке B.2 показаны шаги по реализации мероприятия «Инициация программы создания CSMS».

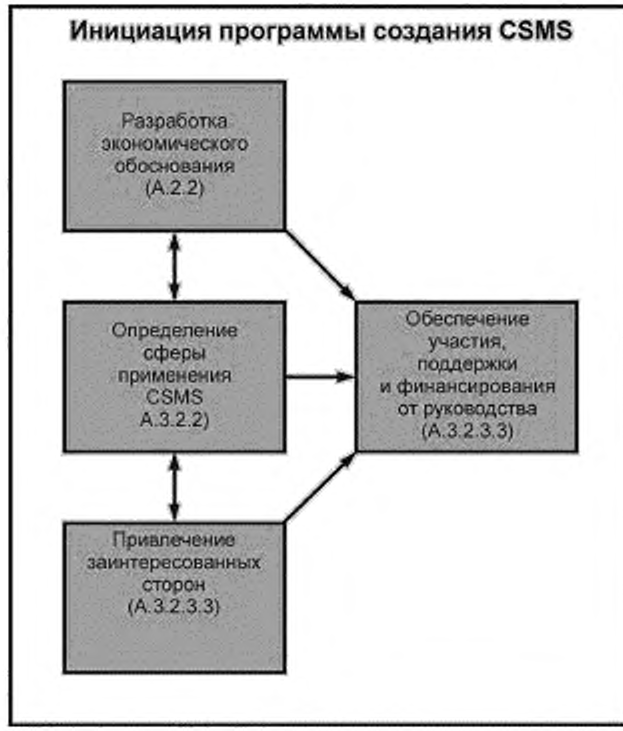


Рисунок B.2 — Действия и взаимосвязи мероприятия «Инициация программы создания CSMS»

Желательным результатом мероприятия «Инициация программы создания CSMS» является обеспечение участия, поддержки и финансирования создания CSMS со стороны руководства. Для достижения этого первыми шагами, как показано на рисунке В.2, является разработка экономического обоснования, которое будет оправдывать создание программы для руководства, и предполагаемой сферы применения программы. Одновременно с этими шагами на основе обоснования и сферы применения программы определяются и привлекаются лица, являющиеся заинтересованными сторонами. Наиболее эффективным является необходимость заранее определить эти заинтересованные стороны при появлении такой возможности и вовлечь их в работу по обеспечению участия в программе руководства. Затем может быть построена организационная структура безопасности. Распространенным заблуждением является попытка инициировать создание CSMS даже без предварительного обоснования, соотносящего кибербезопасность с конкретной организацией и ее миссией. Мероприятия по обеспечению кибербезопасности требуют получения ресурсов от организации, и, несмотря на то, что программа может быть начата при всеобщем мнении о том, что кибербезопасность необходима, в отсутствие экономического обоснования движущая сила может быть быстро потеряна перед более насущными потребностями.

В.4 Мероприятие «Предварительная оценка рисков»

На рисунке В.3 показаны шаги по реализации мероприятия «Предварительная оценка рисков».

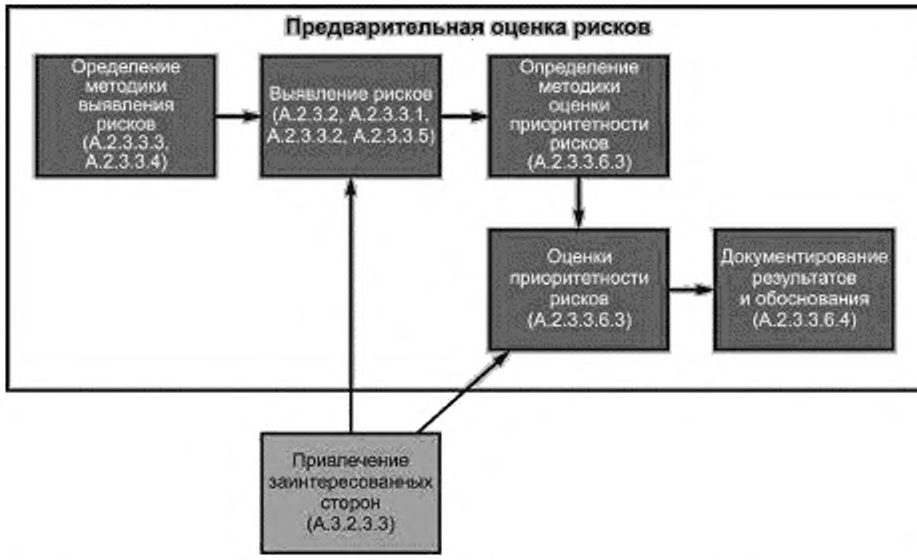


Рисунок В.3 — Действия и взаимосвязи для мероприятия «Предварительная оценка рисков»

Мероприятие «Предварительная оценка рисков» включает в себя выбор методик выявления и определения приоритетности рисков и последующее применение этих методик. Необходимо определить такие методики заранее, чтобы они образовали структуру для дальнейшей оценки рисков. На рисунке В.3 показана важность привлечения заинтересованных сторон, определенных во время проведения мероприятия «Инициация создания CSMS», к процессу выявления и оценки приоритета рисков. Последний шаг, заключающийся в документировании результатов и обоснования, имеет большое значение, поскольку эти записи являются бесценными при подтверждении или актуализации оценки рисков в будущем.

В.5 Мероприятие «Детальная оценка рисков»

Как показано на рисунке В.4, мероприятие «Детальная оценка рисков» обеспечивает более детальную оценку рисков путем, в первую очередь, проведения инвентаризации конкретных систем, сетей и устройств IACS. Ограничения ресурсов или временные ограничения могут не позволить провести подробное изучение всех этих имущественных объектов. В этом случае угрозы, последствия и типы уязвимостей, определенные при предварительной оценке рисков, используются при определении приоритетности конкретных систем, сетей и устройств, на которых необходимо сфокусироваться. Другие факторы, например, непосредственная поддержка или история проблем, также способствуют определению ориентиров для детальной оценки рисков. Детальное определение уязвимостей зависит от типов уязвимостей, определенных при предварительной оценке рисков, но не ограничивается этими

типами. Таким образом, при детальной оценке уязвимости можно обнаружить не только новые типы уязвимостей, но также, возможно, новые угрозы и соответствующие последствия, которые не были выявлены при предварительной оценке рисков, т. е. новые риски. В этом случае необходимо актуализировать предварительную оценку рисков для их включения. Все обнаруженные уязвимости связываются с конкретным риском (угроза, вероятность и последствия) и их приоритет определяется в соответствии с методом, использованным при предварительной оценке рисков.

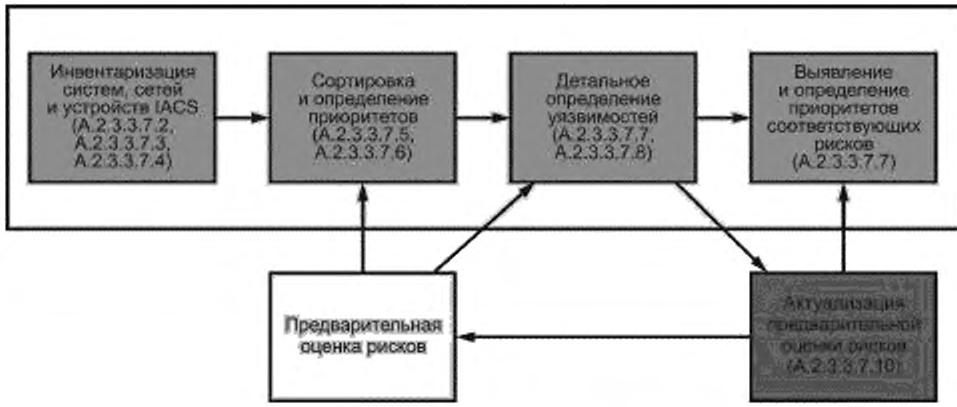


Рисунок В.4 — Действия и взаимосвязи для мероприятия «Детальная оценка рисков»

В.6 Мероприятие «Создание политики, организация и информированность в сфере безопасности»

Соответствующие политики для организации являются функциональным толкованием границ допустимости рисков для организации. Организация, создающая политику до определения своих рисков или границ допустимости рисков, может потратить ненужные усилия на выполнение и приведение в действие нецелесообразной политики или обнаружить, что ее политики не обеспечивают необходимый уровень снижения рисков. На рисунке В.5 показаны шаги по реализации мероприятия «Создание политики, организация и информированность».



Рисунок В.5 — Действия и взаимосвязи для мероприятия «Создание политики, организация и информированность в сфере безопасности»

Реализация политики включает в себя предоставление политики организации, проведение обучения персонала в организации и распределение обязанностей по выполнению политики. Политики и процедуры могут оказывать влияние на любые мероприятия в CSMS. Например, могут существовать политики в отношении обычных используемых контрмер, требующие разработки конкретных систем и процессов обслуживания или определения рисков, подлежащих повторной оценке. Таким образом, на рисунке В.5 показаны не все возможные типы воздействия политик и процедур на CSMS.

На рисунке В.6 показана более подробная разбивка мероприятий «Разработка мероприятий по обучению» и «Распределение организационных обязанностей». На нем показаны различные мероприятия по обучению, составляющие учебную программу, организационные обязанности, связанные с такими мероприятиями по обучению, и соответствующие мероприятия, относящиеся к частям программы создания CSMS. На этом рисунке не показаны все организационные обязанности или темы обучения, которые могут относиться к CSMS, а только основные аспекты, которые должны быть рассмотрены.

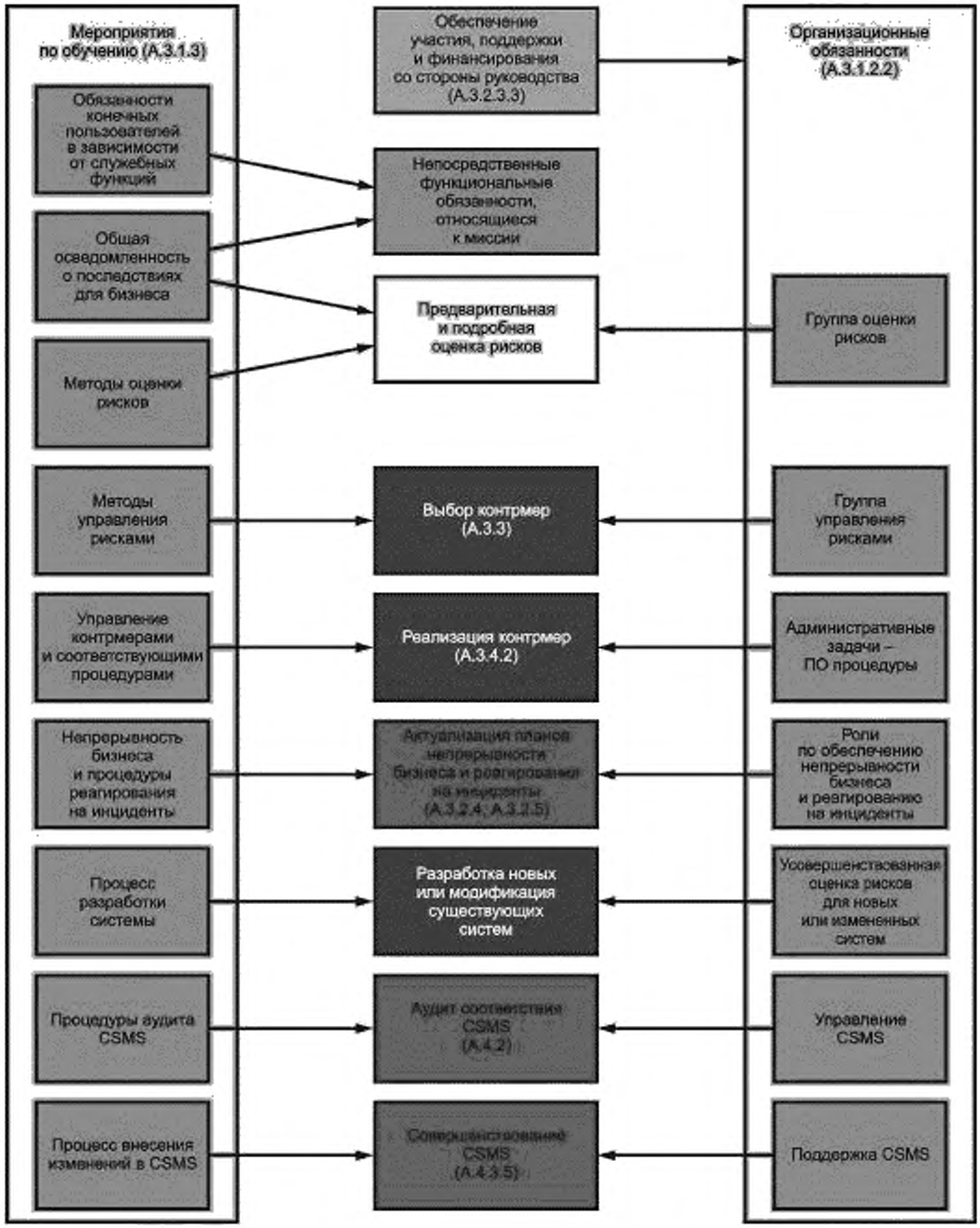


Рисунок В.6 — Обучение и распределение организационных обязанностей

B.7 Мероприятие «Выбор и реализация контрмер»

На рисунке B.7 показаны шаги по реализации мероприятия «Выбор и реализация контрмер».

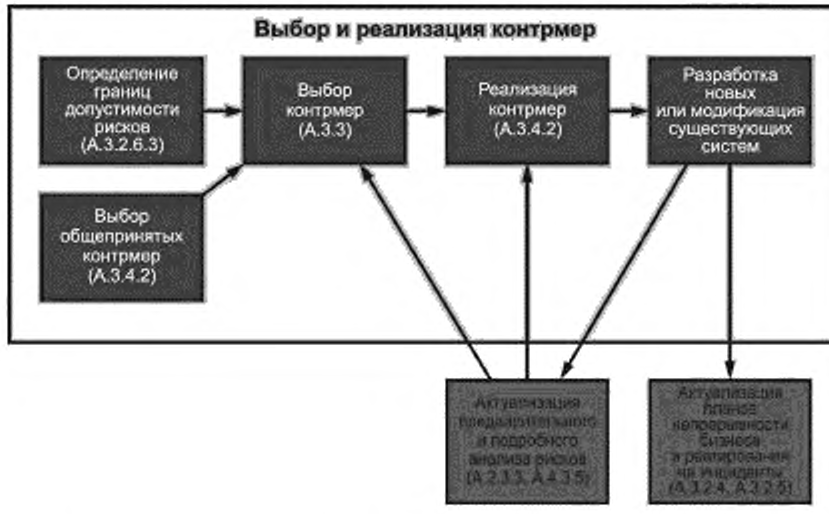


Рисунок B.7 — Действия и взаимосвязи для мероприятия «Выбор и реализация контрмер»

Выбор контрмер является техническим процессом управления рисками. Границы допустимости рисков организации, заранее выбранные общепринятые контрмеры и результаты предварительной и детальной оценок рисков определяют подход управления рисками к выбору контрмер. Если организация внедряет новую систему или изменяет существующую систему, это приводит к необходимости предварительной актуализации и детальной оценки рисков для сценария внедрения такой новой системы. Затем проводится выбор контрмер, относящихся к новой или измененной системе на основе обновленной информации о рисках. Разработка или модификация систем требует актуализации планов непрерывности бизнеса и реагирования на инциденты.

B.8 Мероприятие «Поддержание CSMS»

Как показано на рисунке B.8, мероприятие «Поддержание CSMS» требует проведения периодических проверок и улучшений системы на основе результатов анализа. Исходной информацией для такой проверки являются результаты мер повышения эффективности и аудитов соответствия при внутреннем контроле самой CSMS. Также исходной информацией является внешняя информация о доступных контрмерах, развивающихся отраслевых практиках и новых или измененных законах или нормах.

При проверке CSMS выявляются недостатки и предлагаются улучшения, что в свою очередь приводит к совершенствованию системы. Некоторые из этих изменений могут принимать форму контрмер или улучшения реализации контрмер. В других случаях это могут быть изменения политики и процедур или улучшение их реализации. Анализ результатов несоответствия может указывать на необходимость совершенствования обучения или распределения организационных обязанностей.

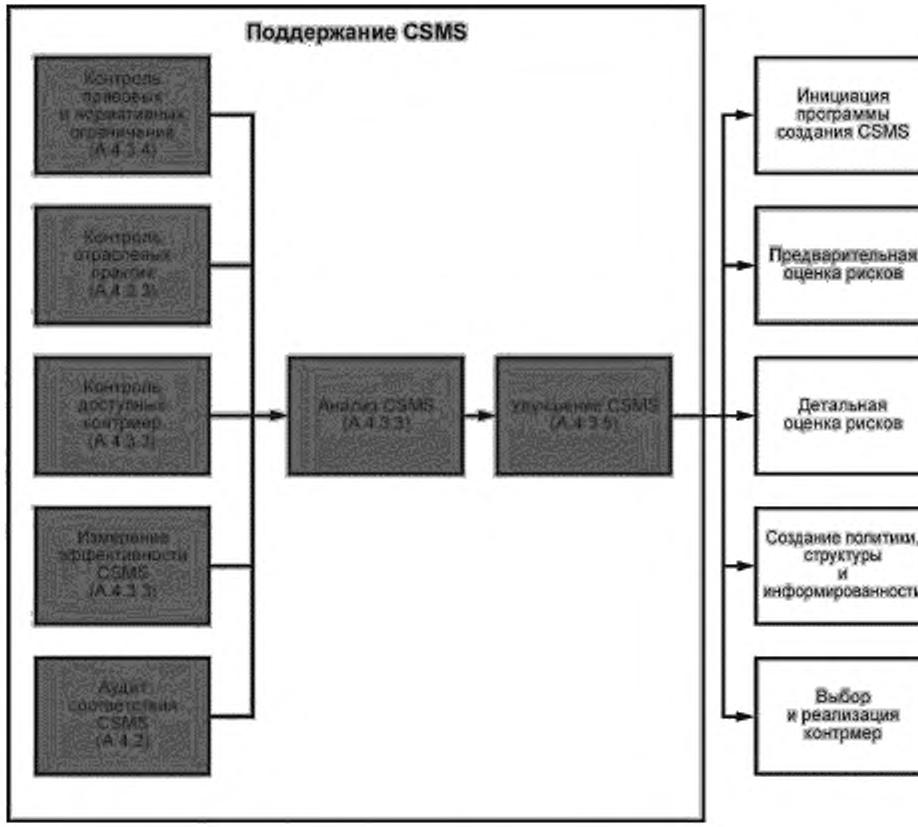


Рисунок В.8 — Действия и взаимосвязи для мероприятия «Поддержание CSMS»

Приложение С
(справочное)

Сопоставление требований настоящего стандарта с ИСО/МЭК 27001

С.1 Обзор

Требования, приведенные в настоящем стандарте очень схожи с требованиями ИСО/МЭК 27001 [24]. МЭК 62443-2-1 был разработан на основе ИСО/МЭК 27001 и содержит большое число перекрестных ссылок. Однако настоящий стандарт использует другую структуру для описания требований. Использованная альтернативная структура была тщательно разработана в результате изменений, внесенных при разработке стандарта в ответ на рецензии конечных пользователей IACS, для обеспечения удобства пользования им путем объединения аналогичных требований в более крупные подразделы и предоставления более информативного руководства в приложении А. Учитывая, что большинство работников, прошедших подготовку в сфере информационной безопасности, уже знакомы с ИСО/МЭК 27001, настоящее приложение было включено для облегчения понимания пользователями схожести требований двух стандартов читателями.

Примечание — В результате предоставления комментариев национального комитета МЭК по проекту стандарта для голосования нормативный орган, который будет подготавливать следующую редакцию настоящего стандарта, будет уделять большее внимание структуре ИСО/МЭК 27001 с добавлением требуемого руководства для конечных пользователей IACS, относящегося к справочным приложениям. Работа над следующей редакцией настоящего стандарта начнется после принятия настоящей редакции.

Настоящее приложение содержит две таблицы сопоставления требований. Первая таблица содержит требования настоящего стандарта и соответствующие ссылки, приведенные в ИСО/МЭК 27001. Вторая таблица содержит требования ИСО/МЭК 27001 и соответствующие ссылки, приведенные в настоящем стандарте. Сопоставление требований осуществляется на уровне подразделов и не является исчерпывающим анализом всех детальных требований. Более подробный анализ требований может быть проведен в последующей редакции настоящего стандарта.

С.2 Сопоставление требований настоящего стандарта с ИСО/МЭК 27001:2005

В таблице С.1 показано сопоставление требований в настоящем стандарте на уровне подразделов с частями ИСО/МЭК 27001:2005.

Примечание — Редакция ИСО/МЭК 27001 была разработана, но не была опубликована к моменту разработки настоящего стандарта. Сопоставление требований настоящего стандарта с более новыми версиями ИСО/МЭК 27001 не проводилось.

Таблица С.1 — Сопоставление требований настоящего стандарта со ссылками в ИСО/МЭК 27001

Требование МЭК 62443-2-1	Соответствующие ссылки в ИСО/МЭК 27001
4.2.2 Экономическое обоснование	4.2.1 e) Анализ и оценка рисков 5.2.1 Предоставление ресурсов
4.2.3 Выявление, классификация и оценка рисков	4.2.1 c) Подход к оценке рисков 4.2.1 d) Выявление рисков 4.2.1 e) Анализ и оценка рисков 4.3.1 Общие требования к документации A.6.2 Сторонние организации A.7.1 Ответственность за имущественные объекты
4.3.2.2 Сфера применения CSMS	4.2.1 a) Сфера применения и границы ISMS 4.3.1 Общие требования к документации

Продолжение таблицы С.1

Требование МЭК 62443-2-1	Соответствующие ссылки в ИСО/МЭК 27001
4.3.2.3 Организация безопасности	4.2.1 b) Политика ISMS 4.2.1 i) Получение разрешения руководства на внедрение и работу ISMS 4.2.2 a) Составление плана снижения рисков 4.2.2 b) Реализация плана снижения рисков 4.2.2 g) Управление ресурсами для ISMS 5.1 Обязательство по управлению 5.2.1 Предоставление ресурсов A.6.1 Внутренняя структура
4.3.2.4 Обучение персонала и повышение информированности о необходимости безопасности	4.2.2 e) Реализация программ обучения и повышения информированности 5.2.2 Обучение, информированность и компетенция A.8.2 Безопасность персонала — при найме
4.3.2.5 План непрерывности бизнеса	4.3.2 Контроль документации 4.3.3 Контроль записей A.9.1 Зоны безопасности A.9.2 Безопасность оборудования A.14.1 Аспекты управления непрерывностью бизнеса, связанные с безопасностью информации
4.3.2.6 Политики и процедуры в области безопасности	4.2.1 b) Политика ISMS 4.2.1 h) Получение разрешения руководства на внедрение и работу ISMS 4.2.1 i) Получение разрешения руководства на внедрение и работу ISMS 4.2.2 d) Определение метода измерения эффективности выбранных средств контроля 4.3.1 Общие требования к документации 4.3.2 Контроль документации 7.1 Проверка ISMS руководством
4.3.3.2 Безопасность персонала	A.6.1 Внутренняя структура A.6.2 Сторонние организации A.8.1 Безопасность персонала — перед наймом A.8.2 Безопасность персонала — при найме A.8.3 Безопасность персонала — при прекращении трудоустройства или смене работы A.10.1 Рабочие процедуры и обязанности
4.3.3.3 Физическая безопасность и защита от внешних воздействий	A.9.1 Безопасные зоны A.9.2 Безопасность оборудования A.10.7 Обращение с носителями информации
4.3.3.4 Сегментация сети	A.10.1 Рабочие процедуры и обязанности A.10.3 Планирование и приемка системы A.10.6 Управление безопасностью сети A.11.4 Контроля доступа к сети
4.3.3.5 Контроль доступа — администрирование учетных записей	A.11.1 Требования бизнеса к контролю доступа A.11.2 Управление пользовательским доступом

Продолжение таблицы С.1

Требование МЭК 62443-2-1	Соответствующие ссылки в ИСО/МЭК 27001
4.3.3.6 Контроль доступа: аутентификация	A.11.3 Обязанности пользователей A.11.4 Контроль доступа к сети A.11.5 Контроль доступа к операционной системе
3.3.7 Контроль доступа — авторизация	A.11.6 Контроль доступа к информации и приложениям A.11.7 Мобильные средства вычисления и телеобработки
4.3.4.2 Управление рисками и принятие мер	4.2.1d) Выявление рисков 4.2.1 e) Анализ и оценка рисков 4.2.1 f) Выявление и оценка вариантов снижения рисков 4.2.1 g) Выбор целей контроля и средств контроля для снижения рисков 4.2.1 h) Получение разрешения руководства на предполагаемые остаточные риски 4.2.1 j) Составление заявления о применимости 4.2.2 b) Реализация плана снижения рисков 4.2.2 c) Внедрение средств контроля 4.2.2 d) Определение метода измерения эффективности выбранных средств контроля 4.2.2 h) Процедуры внедрения и средства контроля для обнаружения и реагирования на события в сфере безопасности 5.2.1 Предоставление ресурсов
4.3.4.3 Разработка и поддержание системы	A.10.1 Рабочие процедуры и обязанности A.10.2 Управление оказанием услуг сторонними организациями A.10.3 Планирование и приемка системы A.10.4 Защита от вредоносных и мобильных кодов A.10.5 Резервирование A.10.6 Управление безопасностью сети A.10.8 Информационный обмен A.10.9 Электронные коммерческие услуги A.10.10 Мониторинг A.12.1 Требования к безопасности информационных систем A.12.2 Исправление обрабатывающих приложений A.12.3 Шифровальные средства контроля A.12.4 Безопасность системных файлов A.12.5 Безопасность процессов разработки и поддержки A.12.6 Управление техническими уязвимостями
4.3.4.4 Управление информацией и документацией	4.3.1 Общие требования к документации 4.3.2 Контроль документации 4.3.3 Контроль записей A.10.7 Обращение с носителями информации
4.3.4.5 Планирование и реагирование на инциденты	4.2.2 h) Реализация процедур и средств контроля для обнаружения и реагирования на события в сфере безопасности 4.3.2 Контроль документов A.13.1 Предоставление информации о событиях и слабых сторонах информационной безопасности A.13.2 Управление информацией об инцидентах и улучшениях безопасности

Окончание таблицы С.1

Требование МЭК 62443-2-1	Соответствующие ссылки в ИСО/МЭК 27001
4.4.2 Выполнение норм и требований	4.2.3 e) проведение внутренних аудитов ISMS с запланированной частотой 6 Внутренние аудиты ISMS A.10.10 Мониторинг A.15.1 Выполнение правовых требований A.15.2 Выполнение политик и стандартов безопасности и соответствие техническим условиям A.15.3 Аспекты проведения аудитов информационных систем
4.4.3 Анализ, совершенствование и поддержание CSMS	4.2.2 f) Управление работой ISMS 4.2.3 a) Проведение мониторинга и процедур проверки и других контрольных мероприятий 4.2.3 b) Проведение регулярных проверок эффективности ISMS 4.2.3 c) Изменение эффективности средств контроля 4.2.3 d) Анализ оценок рисков, остаточных рисков и приемлемых уровней рисков с запланированной частотой 4.2.3 f) Регулярная проверка ISMS для определения достаточности сферы применения системы и выявления улучшений ISMS 4.2.3 g) Совершенствование планов безопасности с помощью мероприятий по мониторингу и проверке 4.2.3 h) Фиксирование действий и событий, которые могут оказать влияние на эффективность ISMS 4.2.4 a) Реализация улучшений ISMS 4.2.4 b) Реализация соответствующих корректирующих и превентивных действий 4.2.4 c) Уведомление всех заинтересованных сторон о действиях и улучшениях 4.2.4 d) Обеспечение достижения поставленных целей с помощью улучшений 5.1 Обязательства руководства 6 Внутренние аудиты ISMS 7.1 Проверка ISMS руководством 7.2 Анализ исходной информации для проверки руководством 7.3 Анализ результатов проверки руководством 8.1 Непрерывное улучшение ISMS 8.2 Корректирующие действия 8.3 Превентивные действия A.13.2 Управление информацией об инцидентах и улучшениях в сфере безопасности

С.3 Сопоставление требований ИСО/МЭК 27001:2005 с настоящим стандартом

В таблице С.2 сопоставлены требования ИСО/МЭК 27001:2005 с настоящим стандартом в противоположность таблице С.1.

Таблица С.2 — Сопоставление требований ИСО/МЭК 27001 с настоящим стандартом

Требование ИСО/МЭК 27001	Соответствующие ссылки в МЭК 62443-2-1
4.2.1 a) Сфера и границы применения ISMS	4.3.2.2 Сфера применения CSMS
4.2.1 b) Политика ISMS	4.3.2.3 Организация безопасности 4.3.2.6 Политики и процедуры безопасности
4.2.1 c) Подход к оценке рисков	4.2.3 Выявление, классификация и оценка рисков
4.2.1 d) Выявление рисков	4.2.3 Выявление, классификация и оценка рисков 4.3.4.2 Управление рисками и принятие мер
4.2.1 e) Анализ и оценка рисков	4.2.2 Экономическое обоснование 4.2.3 Выявление, классификация и оценка рисков 4.3.4.2 Управление рисками и принятие мер
4.2.1 f) Выявление и оценка вариантов снижения рисков	4.3.4.2 Управление рисками и принятие мер
4.2.1 g) Выбор целей контроля и средств контроля для снижения рисков	4.3.4.2 Управление рисками и принятие мер
4.2.1 h) Получение одобрения руководства для предполагаемых остаточных рисков	4.3.2.6 Политики и процедуры безопасности 4.3.4.2 Управление рисками и принятие мер
4.2.1 i) Получение разрешения руководства для внедрения и работы ISMS	4.3.2.3 Организация безопасности 4.3.2.6 Политики и процедуры безопасности
4.2.1 j) Составление заявления о применимости	4.3.4.2 Управление рисками и принятие мер
4.2.2 a) Составление плана по снижению рисков	4.3.2.3 Организация безопасности
4.2.2 b) Реализация плана по снижению рисков	4.3.2.3 Организация безопасности 4.3.4.2 Управление рисками и принятие мер
4.2.2 c) Внедрение средств контроля	4.3.4.2 Управление рисками и принятие мер
4.2.2 d) Определение метода измерения эффективности избранных средств контроля	4.3.2.6 Политики и процедуры безопасности 4.3.4.2 Управление рисками и принятие мер 4.4.2 Выполнение норм и требований
4.2.2 e) Реализация программ обучения и повышения информированности	4.3.2.4 Обучение персонала и повышение информированности о необходимости безопасности
4.2.2 f) Управление работой ISMS	4.4.3 Анализ, совершенствование и поддержание CSMS
4.2.2 g) Управление ресурсами для ISMS	4.3.2.3 Организация безопасности
4.2.2 h) Внедрение процедур и средств контроля для обнаружения и реагирования на события в сфере безопасности	4.3.4.2 Управление рисками и принятие мер 4.3.4.5 Планирование и реагирование на инциденты
4.2.3 a) Проведение мониторинга и проверка процедур и других средств контроля	4.4.2 Выполнение норм и требований 4.4.3 Анализ, совершенствование и поддержание CSMS
4.2.3 b) Проведение регулярных проверок эффективности ISMS	4.4.3 Анализ, совершенствование и поддержание CSMS

Продолжение таблицы С.2

Требование ИСО/МЭК 27001	Соответствующие ссылки в МЭК 62443-2-1
4.2.3 c) Измерение эффективности средств контроля	4.4.2 Выполнение норм и требований 4.4.3 Анализ, совершенствование и поддержание CSMS
4.2.3 d) Проверка оценок рисков, остаточных рисков и приемлемых уровней рисков с запланированной частотой	4.4.3 Анализ, совершенствование и поддержание CSMS
4.2.3 e) Проведение внутренних аудитов ISMS с запланированной частотой	4.4.2 Выполнение норм и требований
4.2.3 f) Проверка ISMS с запланированной частотой для определения достаточности ее сферы применения и улучшений ISMS	4.4.3 Анализ, совершенствование и поддержание CSMS
4.2.3 g) Актуализация планов безопасности после мероприятий по мониторингу и проверке	4.4.3 Анализ, совершенствование и поддержание CSMS
4.2.3 h) Фиксирование действий и событий, которые могут оказать влияние на эффективность ISMS	4.4.3 Анализ, совершенствование и поддержание CSMS
4.2.4 a) Реализация улучшений ISMS	4.4.3 Анализ, совершенствование и поддержание CSMS
4.2.4 b) Реализация соответствующих корректирующих и превентивных действий	4.4.3 Анализ, совершенствование и поддержание CSMS
4.2.4 c) Уведомление всех заинтересованных сторон о действиях и улучшениях	4.4.3 Анализ, совершенствование и поддержание CSMS
4.2.3 h) Фиксирование действий и событий, которые могут оказать влияние на эффективность ISMS	4.4.3 Анализ, совершенствование и поддержание CSMS
4.2.4 a) Реализация улучшений ISMS	4.4.3 Анализ, совершенствование и поддержание CSMS
4.2.4 b) Реализация соответствующих корректирующих и превентивных действий	4.4.3 Анализ, совершенствование и поддержание CSMS
4.2.4 c) Уведомление всех заинтересованных сторон о действиях и улучшениях	4.4.3 Анализ, совершенствование и поддержание CSMS
4.2.4 d) Обеспечение достижения поставленных целей с помощью улучшений	4.4.3 Анализ, совершенствование и поддержание CSMS
4.3.1 Общие требования к документации	4.2.3 Выявление, классификация и оценка рисков 4.3.2.2 Сфера применения CSMS 4.3.2.6 Политики и процедуры безопасности 4.3.4.4 Управление информацией и документацией
4.3.2 Контроль документации	4.3.2.5 План непрерывности бизнеса 4.3.2.6 Политики и процедуры в области безопасности 4.3.4.4 Управление информацией и документацией 4.3.4.5 Планирование и реагирование на инциденты
4.3.3 Контроль записей	4.3.2.5 План непрерывности бизнеса 4.3.4.4 Управление информацией и документацией
5.1 Обязательство руководства	4.3.2.3 Организация безопасности 4.4.2 Выполнение норм и требований 4.4.3 Анализ, совершенствование и поддержание CSMS

Продолжение таблицы С.2

Требование ИСО/МЭК 27001	Соответствующие ссылки в МЭК 62443-2-1
5.2.1 Предоставление ресурсов	4.2.2 Экономическое обоснование 4.3.2.3 Организация безопасности 4.3.4.2 Управление рисками и принятие мер
5.2.2 Обучение, информированность и компетенция	4.3.2.4 Обучение персонала и повышение информированности о необходимости безопасности
6 Внутренние аудиты ISMS	4.4.2 Выполнение норм и требований 4.4.3 Анализ, совершенствование и поддержание CSMS
7.1 Проверка ISMS руководством	4.3.2.6 Политики и процедуры безопасности 4.4.3 Анализ, совершенствование и поддержание CSMS
7.2 Анализ исходной информации для проверки руководством	4.4.3 Анализ, совершенствование и поддержание CSMS
7.3 Анализ результатов проверки руководством	4.4.3 Анализ, совершенствование и поддержание CSMS
8.1 Непрерывное совершенствование ISMS	4.4.3 Анализ, совершенствование и поддержание CSMS
8.2 Корректирующие действия	4.4.3 Анализ, совершенствование и поддержание CSMS
8.3 Превентивные действия	4.4.3 Анализ, совершенствование и поддержание CSMS
А.5.1 Политика информационной безопасности	Ссылка в конкретном пункте отсутствует; политики безопасности системы управления толкуют и применяют общие политики к этой среде
А.6.1 Внутренняя структура	4.3.2.3 Организация безопасности 4.3.3.2 Безопасность персонала
А.6.2 Сторонние организации	4.2.3 Выявление, классификация и оценка рисков 4.3.3.2 Безопасность персонала
А.7.1 Ответственность за имущественные объекты	4.2.3 Выявление, классификация и оценка рисков
А.7.2 Классификация информации	Ссылка в конкретном пункте отсутствует; политики безопасности системы управления толкуют и применяют общие политики к этой среде
А.8.1 Безопасность персонала — до найма	4.3.3.2 Безопасность персонала
А.8.2 Безопасность персонала — при найме	4.3.2.4 Обучение персонала и повышение информированности о необходимости безопасности 4.3.3.2 Безопасность персонала
А.8.3 Безопасность персонала — при прекращении трудоустройства или смене работы	4.3.3.2 Безопасность персонала
А.9.1 Безопасные области	4.3.2.5 План непрерывности бизнеса 4.3.3.3 Физическая безопасность и защита от внешних воздействий
А.9.2 Безопасность оборудования	4.3.2.5 План непрерывности бизнеса 4.3.3.3 Физическая безопасность и защита от внешних воздействий

Продолжение таблицы С.2

Требование ИСО/МЭК 27001	Соответствующие ссылки в МЭК 62443-2-1
А.10.1 Рабочие процедуры и обязанности	4.3.3.2 Безопасность персонала 4.3.3.4 Сегментация сети 4.3.4.3 Разработка и обслуживание систем 4.4.2 Выполнение норм и требований
А.10.2 Управление оказанием услуг сторонними организациями	4.3.4.3 Разработка и обслуживание систем
А.10.3 Планирование и приемка системы	4.3.3.4 Сегментация сети 4.3.4.3 Разработка и обслуживание систем
А.10.4 Защита от вредоносных и мобильных кодов	4.3.4.3 Разработка и обслуживание систем
А.10.5 Резервирование	4.3.4.3 Разработка и обслуживание систем
А.10.6 Управление сетевой безопасностью	4.3.3.4 Сегментация сети 4.3.4.3 Разработка и обслуживание систем
А.10.7 Обращение с носителями информации	4.3.3.3 Физическая безопасность и защита от внешних воздействий 4.3.4.4 Управление информацией и документацией
А.10.8 Информационный обмен	4.3.4.3 Разработка и обслуживание систем
А.10.9 Электронные коммерческие услуги	4.3.4.3 Разработка и обслуживание систем
А.10.10 Мониторинг	4.3.4.3 Разработка и обслуживание систем 4.4.2 Выполнение норм и требований
А.11.1 Требования бизнеса к контролю доступа	4.3.3.5 Контроль доступа — администрирование учетных записей
А.11.2 Управление пользовательским доступом	4.3.3.5 Контроль доступа — администрирование учетных записей
А.11.3 Обязанности пользователей	4.3.3.6 Контроль доступа — аутентификация
А.11.4 Контроль доступа к сети	4.3.3.4 Сегментация сети 4.3.3.6 Контроль доступа — аутентификация
А.11.5 Контроль доступа к операционной системе	4.3.3.6 Контроль доступа — аутентификация
А.11.6 Контроль доступа к приложениям и информации	4.3.3.7 Контроль доступа — авторизация
А.11.7 Мобильные вычисления и телеобработка	4.3.3.7 Контроль доступа — авторизация
А.12.1 Требования к безопасности информационных систем	4.3.4.3 Разработка и поддержание систем
А.12.2 Коррекция обработки в приложениях	4.3.4.3 Разработка и обслуживание систем
А.12.3 Криптографические средства контроля	4.3.4.3 Разработка и обслуживание систем
А.12.4 Безопасность системных файлов	4.3.4.3 Разработка и обслуживание систем
А.12.5 Безопасность процессов разработки и поддержки	4.3.4.3 Разработка и обслуживание систем

Окончание таблицы С.2

Требование ИСО/МЭК 27001	Соответствующие ссылки в МЭК 62443-2-1
А.12.6 Управление техническими уязвимостями	4.3.4.3 Разработка и обслуживание систем
А.13.1 Уведомление о событиях и слабых сторонах информационной безопасности	4.3.4.5 Планирование и реагирование на инциденты
А.13.2 Управление инцидентами и улучшениями информационной безопасности	4.3.4.5 Планирование и реагирование на инциденты 4.4.3 Анализ, совершенствование и поддержание CSMS
А.14.1 Аспекты управления непрерывностью бизнеса, связанные с информационной безопасностью	4.3.2.5 План непрерывности бизнеса
А.15.1 Выполнение правовых требований	4.4.2 Выполнение норм и требований
А.15.2 Выполнение политик и процедур безопасности и технических условий	4.4.2 Выполнение норм и требований
А.15.3 Аспекты аудита информационных систем	4.4.2 Выполнение норм и требований

Приложение ДА
(справочное)

Алфавитный перечень терминов

Административные порядки (administrative practices)	3.1.2
Аппаратные требования (device requirements)	3.1.14
Аутентификация (authentication)	3.1.4
Важнейший (critical)	3.1.12
Вероятность возникновения (likelihood)	3.1.22
Границы допустимости риска (risk tolerance)	3.1.36
Заинтересованное лицо (stakeholder):	3.1.40
Имущественный объект (asset)	3.1.3
Инженер по организации производства (process engineer)	3.1.28
Информационная техника (information technology)	3.1.20
Инцидент (incident)	3.1.18
Консультант безопасности (gatekeeper)	3.1.15
Локальный пользователь (local user)	3.1.23
MAC-адрес (MAC-address)	3.1.25
Методика «шести сигм» (Six Sigma®)	3.1.38
Независимый аудит (independent audit)	3.1.19
Неподдерживаемая система (legacy system)	3.1.21
Оператор (operator)	3.1.26
Отслеживаемый удаленный доступ, отслеживание удаленного доступа (ushered access, shadowing)	3.1.43
Охрана труда, техника безопасности и охрана окружающей среды (здоровье, условия труда и экологическая безопасность) (health, safety and environment)	3.1.16
Оценка рисков (risk assessment)	3.1.34
Оценка уязвимости (vulnerability assessment)	3.1.44
План непрерывности бизнеса (business continuity plan)	3.1.6
Планирование непрерывности бизнеса (business continuity planning)	3.1.7
Последствие (consequence)	3.1.11
Программируемый логический контроллер (programmable logic controller; PLC)	3.1.30
Самостоятельная оценка (self-assessment)	3.1.37
Система управления горелкой (burner management system)	3.1.5
Система управления кибербезопасностью (cyber security management system)	3.1.13
Система управления производственными данными (process information management system)	3.1.29
Система управления производством (manufacturing execution system)	3.1.24
Системный администратор (system administrator)	3.1.41

Смягчение риска (risk mitigation)	3.1.35
Совместимость между стандартами (compliance)	3.1.9
Соответствие стандарту (conformance)	3.1.10
Социальная инженерия (social engineering)	3.1.39
Требования к системе (system requirements)	3.1.42
Удаленный доступ (remote access)	3.1.32
Удаленный пользователь (remote user)	3.1.33
Управление безопасностью процесса (process safety management)	3.1.31
Управление изменениями (change management)	3.1.8
Управление патчами (patch management)	3.1.27
Учетная запись доступа (access account)	3.1.1
Человеко-машинный интерфейс (human-machine interface; HMI)	3.1.17

Приложение ДБ
(справочное)

Сведения о соответствии ссылочных международных стандартов национальным стандартам Российской Федерации

Таблица ДА.1

Обозначение ссылочного международного стандарта	Степень соответствия	Обозначение и наименование соответствующего национального стандарта
IEC/TS 62443-1-1: 2009	IDT	ГОСТ Р 56205—2014/IEC/TS 62443-1-1: 2009 «Сети коммуникационные промышленные. Защищенность (кибербезопасность) сети и системы. Часть 1-1. Терминология, концептуальные положения и модели»

Примечание — В настоящей таблице использовано следующее условное обозначение степени соответствия стандартов:

- IDT — идентичный стандарт.

Библиография

Примечание — Данный библиографический список включает ссылки на источники, использованные при составлении настоящего стандарта, а также ссылки на источники, которые могут помочь читателю при получении общего представления о кибербезопасности и разработке системы управления. Не все ссылки в данном списке приведены в тексте настоящего стандарта. Ссылки разбиты на отдельные категории в зависимости от типа источника.

Ссылки на другие части стандартов серии МЭК 62443 как существующие, так и ожидаемые:

Примечание — Некоторые их этих ссылок являются ссылками на нормативные документы (см. пункт 2), опубликованные, разрабатываемые или ожидаемые документы. Они перечислены для дополнения ожидаемых частей стандартов серии МЭК 6244-3.

[1] IEC/TS 62443-1-1[1)], Industrial communication networks — Network and system security Part 1-1: Terminology, concepts and models

[2] IEC/TR 62443-1-2[2)], Industrial communication networks — Network and system security — Part 1-2: Master glossary of terms and abbreviations

[3] IEC/TR 62443-1-3, Industrial communication networks — Network and system security — Part 1-3: System security compliance metrics

Примечание — Настоящий стандарт называется МЭК 62443-2-1, Промышленные коммуникационные сети. Безопасность сетей и систем. Часть 2.1. Создание программы безопасности IACS.

[4] IEC 62443-2-2[3)], Industrial communication networks — Network and system security — Part 2-2: Operating an industrial automation and control system security program

[5] IEC/TR 62443-2-3[2)], Industrial communication networks — Network and systemsecurity — Part 2-3: Patch management in the IACS environment

[6] IEC/TR 62443-3-1, Industrial communication networks — Network and system security — Part 3-1: Security technologies for industrial automation and control systems

[7] IEC 62443-3-2[2)], Industrial communication networks — Network and system security — Part 3-2: Target security assurance levels for zones and conduits

[8] IEC 62443-3-3[2)], Industrial communication networks — Network and system security — Part 3-3: System security requirements and security assurance levels

[9] IEC 62443-3-4[2)], Industrial communication networks — Network and system security — Part 3-4: Product development requirements

[10] IEC 62443-4-1[2)], Industrial communication networks — Network and system security — Part 4-1: Embedded devices

[11] IEC 62443-4-2[2)], Industrial communication networks — Network and system security — Part 4-2: Host devices

[12] IEC 62443-4-3[2)], Industrial communication networks — Network and system security — Part 4-3: Network devices

[13] IEC 62443-4-4[2)], Industrial communication networks — Network and system security — Part 4-4: Application, data and functions

---

[1)] Настоящий стандарт разработан на основе AN SI/ISA 99.02.01:2009 и в полном объеме заменяет его для использования в любой стране мира. При этом понимается, что второе издание IEC/TS 62443-1-1 является международным стандартом, а не технической спецификацией (TS), т. к. в него были включены некоторые нормативные требования, в отношении которых возможно достижение соответствия.

[2)] В разработке.

[3)] Планируемый справочник к настоящему стандарту.

Ссылки на другие стандарты:

[14] IEC 61131-3, Programmable controllers — Part 3: Programming languages

[15] IEC 61512-1, Batch Control, Part 1: Models and terminology

[16] IEC 62264-1, Enterprise-Control System Integration, Part 1: Models and terminology

[17] ISO/IEC Directives, Part 2, Rules for the structure and drafting of International Standards

[18] ISO/IEC 10746-1, Information technology — Open distributed processing — Reference model: Overview

[19] ISO/IEC 10746-2, Information technology — Open distributed processing — Reference model: Foundations

[20] ISO/IEC 15408-1:2008, Information technology — Security techniques — Evaluation criteria for IT security — Part 1: Introduction and general model

[21] ISO/IEC 15408-2:2008, Information technology — Security techniques — Evaluation criteria for IT security — Part 2: Security functional components

[22] ISO/IEC 15408-3:2008, Information technology — Security techniques — Evaluation criteria for IT security — Part 3: Security assurance components

[23] ISO/IEC 17799, Information technology — Security techniques — Code of practice for information security management

[24] ISO/IEC 27001:2005, Information technology — Security techniques — Information security management systems — Requirements

[25] 29 CFR 1910.119 — U.S. Occupational Safety and Health Standards — Hazardous Materials — Process safety management of highly hazardous chemicals

Ссылки на отраслевые материалы:

[26] Guidance for Addressing Cyber Security in the Chemical Sector, Version 3.0, May 2006, American Chemistry Council's Chemical Information Technology Center (ChemITC), available at <gost.e-ecolog.ru gost.e-ecolog.ru

[27] Report on Cyber Security Vulnerability Assessments Methodologies, Version 2.0, November 2004, ChemITC, available at <http://gost.e-ecolog.ru >

[28] Cyber Security Architecture Reference Model, Version 1.0, August 2004, ChemITC, available at <gost.e-ecolog.ru gost.e-ecolog.ru >

[29] Report on the Evaluation of Cybersecurity Self-assessment Tools and Methods, November 2004, ChemITC, available at <http://www.chemicalcybersecurity.com/>

[30] U.S. Chemicals Sector Cyber Security Strategy, September 2006, available at <gost.e-ecolog.ru gost.e-ecolog.ru

Другие документы и опубликованные ресурсы:

[31] Carlson, Tom, Information Security Management: Understanding ISO 17799, 2001, available at <gost.e-ecolog.ru gost.e-ecolog.ru >

[32] Purdue Research Foundation, A Reference Model for Computer Integrated Manufacturing, 1989, ISBN 1-55617-225-7

[33] Purdue Research Foundation, A Reference Model for Computer Integrated Manufacturing, 1989, ISBN 1-55617-225-7

[34] NIST Special Publication 800-37, Guide for the Security Certification and Accreditation of Federal Information Systems, May 2004

[35] NIST Special Publication 800-55, Security Metrics Guide for Information Technology Systems, July 2003

[36] NIST Special Publication 800-61, Computer Security Incident Handling Guide, January 2004

[37] NIST Special Publication 800-82, Guide to Supervisory Control and Data Acquisition (SCADA) and Industrial Control System Security, March 2006, Draft

[38] NIST Process Control Security Requirements Forum (PCSRF), Industrial Control System — System Protection Profile (ICS-SPP)

[39] Carnegie Mellon Software Engineering Institute, Capability Maturity Model Integration (CMMI) for Software Engineering, v1.1, August 2002

Веб-сайты:

[40] NASA/Science Office of Standards and Technology (NOST), available at <gost.e-ecolog.ru gost.e-ecolog.ru

[41] Zachmann Enterprise Reference Model, available at <http://www.zifa.com/>

[42] Sarbanes — Oxley Web site, available at <http://www.sarbanes-oxley.com/>

[43] Sans Web site, available at <gost.e-ecolog.ru

[44] MIS Training Institute, available at <gost.e-ecolog.ru

[45] U.S. National Institute of Standards & Technology, available at <gost.e-ecolog.ru

[46] Information Systems Technology Audit Programs, available at <gost.e-ecolog.ru >

[47] NIST eScan Security Assessment, available at <https://gost.e-ecolog.ru >

[48] American National Standards Institute, available at <gost.e-ecolog.ru

[49] IDEAL Model, available at <gost.e-ecolog.ru >

[50] Control Objectives for Information and Related Technology (COBIT), available at <gost.e-ecolog.ru

[51] Corporate Governance Task Force «Information Security Governance- A call to action», available at <gost.e-ecolog.ru gost.e-ecolog.ru >

[52] Michigan State Cybersecurity Definitions, available at <gost.e-ecolog.ru gost.e-ecolog.ru

[53] The Free Internet Encyclopedia — Wikipedia, available at <gost.e-ecolog.ru >

[54] Bridgefield Group Glossary, available at <gost.e-ecolog.ru >

[55] Six Sigma Information, available at <gost.e-ecolog.ru >

[56] Carnegie Mellon Software Engineering Institute, available at <gost.e-ecolog.ru >

[57] Carnegie Mellon Software Engineering Institute, Computer Emergency Response Team (CERT), available at <gost.e-ecolog.ru

[58] SCADA and Control Systems Procurement Project, available at <gost.e-ecolog.ru >

[59] Interoperability Clearinghouse, available at <gost.e-ecolog.ru

[60] New York State Financial Terminology, available at <gost.e-ecolog.ru gost.e-ecolog.ru

[61] Search Windows Security, available at <gost.e-ecolog.ru >

[62] Chemical Sector Cyber Security Program, available at <gost.e-ecolog.ru >

[63] TechEncyclopedia, available at <http://www.techweb.com/encyclopedia/>

УДК 004.056.5:006.354

МКС 25.040.40
35.040

Ключевые слова: сети промышленные коммуникационные, защищенность, кибербезопасность, сети и системы, программа обеспечения защищенности, кибербезопасность, системы управления и промышленной автоматизации

Редактор *Л.А. Кудрявцева*
Технический редактор *В.Н. Прусакова*
Корректор *С.В. Смирнова*
Компьютерная верстка *Е.А. Кондрашовой*

Сдано в набор 25.11.2015. Подписано в печать 24.12.2015 Формат 60×84¼. Гарнитура Ариал.
Усл. печ. л. 16,28. Уч.-изд. л. 15,60. Тираж 32 экз Зак. 4281.

Издано и отпечатано во ФГУП «СТАНДАРТИНФОРМ», 123995 Москва, Гранатный пер., 4.
gost.e-ecolog.ru gost.e-ecolog.ru

gost.e-ecolog.ru