ФЕДЕРАЛЬНОЕ АГЕНТСТВО

ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

ГОСТ Р 56498— 2015/ IEC/PAS 62443-3: 2008

СЕТИ КОММУНИКАЦИОННЫЕ ПРОМЫШЛЕННЫЕ

Защищенность (кибербезопасность) сети и системы

Часть 3

Защищенность (кибербезопасность) промышленного процесса измерения и управления

(IEC/PAS 62443-3:2008, IDT)

Издание официальное

Москва
Стандартинформ
2019

gost.e-ecolog.ru

Предисловие

1 ПОДГОТОВЛЕН Негосударственным образовательным частным учреждением «Новая Инженерная Школа» (НОЧУ «НИШ») на основе официального перевода на русский язык англоязычной версии указанного в пункте 4 документа, 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. № 775-ст

4 Настоящий стандарт идентичен международному документу IEC/PAS 62443-3:2008 «Промышленные коммуникационные сети. Защищенность (кибербезопасность) сети и системы. Часть 3. Защищенность (кибербезопасность) промышленного процесса измерения и управления» (IEC/PAS 62443-3:2008, «Industrial communication networks — Network and system security — Part 3: Security for industrial process measurement and control», IDT).

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, сведения о которых приведены в дополнительном приложении ДБ

5 ВВЕДЕН ВПЕРВЫЕ

6 ПЕРЕИЗДАНИЕ. Январь 2019 г.

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

*Правила применения настоящего стандарта установлены в статье 26 Федерального закона от 29 июня 2015 г. № 162-ФЗ «О стандартизации в Российской Федерации». 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 (*gost.e-ecolog.ru

© Стандартинформ, оформление, 2015, 2019

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
4 Введение и нормативно-правовое соответствие . . . 6
5 Принципы и базовые модели . . . 7
5.1 Общие положения . . . 7
5.2 Модель угроз-рисков . . . 7
5.3 Жизненный цикл безопасности . . . 9
5.4 Политика . . . 10
5.5 Типовые эталонные конфигурации . . . 12
5.6 Модели защиты . . . 15
6 Политика безопасности промышленной системы управления — основные сведения . . . 20
7 Политика безопасности промышленной системы управления — принципы и допущения . . . 21
7.1 Политика безопасности промышленной системы управления — принципы . . . 21
7.2 Политика безопасности промышленной системы управления — допущения и исключения . . . 22
7.3 Политика безопасности промышленной системы управления — организация и управление . . . 24
8 Политика безопасности промышленной системы управления — меры . . . 28
8.1 Управление доступностью . . . 28
8.2 Управление целостностью . . . 30
8.3 Управление логическим доступом . . . 32
8.4 Управление физическим доступом . . . 35
8.5 Управление сегментом . . . 36
8.6 Управление внешним доступом . . . 37
Приложение А (справочное) Готовящееся к публикации новое издание МЭК 62443 . . . 40
Приложение ДА (справочное) Алфавитный указатель терминов . . . 42
Приложение ДБ (справочное) Сведения о соответствии ссылочных международных стандартов национальным стандартам . . . 44
Библиография . . . 45

Введение

Ранее изолированные автоматизированные системы все больше объединяются в сети общего пользования и, следовательно, растет уязвимость таких систем перед атаками. Стандартные механизмы обеспечения IT-безопасности имеют цели и стратегии защиты, которые могут быть неприменимы для автоматизированных систем. Настоящий стандарт описывает концепцию обеспечения безопасности доступа к промышленным системам и внутри них, чтобы при этом гарантировалось своевременное срабатывание, которое может быть крайне важно для функционирования производственного объекта.

Для прикладных систем безопасности и систем в фармацевтических или других узкоспециализированных отраслей промышленности могут быть применимы дополнительные стандарты, директивы, определения и условия. Например, МЭК 61508, GAMP (ISPE), правило 21 CFR (FDA) для соответствия GMP и Стандартный регламент Европейского агентства лекарственных средств (SOP/INSP/2003).

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

СЕТИ КОММУНИКАЦИОННЫЕ ПРОМЫШЛЕННЫЕ

Защищенность (кибербезопасность) сети и системы

Часть 3

Защищенность (кибербезопасность) промышленного процесса измерения и управления

Industrial communication networks. Network and system security.
Part 3. Security for industrial process measurement and control

Дата введения — 2016—01—01

1 Область применения

Настоящий стандарт устанавливает концепцию обеспечения безопасности аспектов информационно-коммуникационных технологий систем измерений и управления в производственных процессах, включая сети таких систем и устройства в составе таких сетей, на этапе эксплуатации жизненного цикла производственного объекта.

Настоящий стандарт устанавливает методологическую основу для формулирования требований к безопасности эксплуатации производственного объекта и предназначен прежде всего для владельцев/операторов автоматизированных систем, отвечающих за эксплуатацию систем управления, используемых в промышленности (ICS).

Кроме того, эксплуатационные требования, установленные в настоящем стандарте, могут быть использованы теми, кто имеет отношение к ICS, в том числе:

a) разработчики автоматизированных систем;

b) изготовители (поставщики) устройств, подсистем и систем;

c) сборщики подсистем и систем.

PAS учитывает следующие вопросы:

- постепенный перенос/эволюция существующих систем;
- достижение целей безопасности с помощью существующих коммерческих технологий и продуктов;
- гарантия надежности/доступности защищенных коммуникационных сервисов;
- применимость к системам любых размеров и с любыми рисками (универсальность);
- совместимость требований защиты, нормативно-правового соответствия и функциональности автоматики с требованиями безопасности.

Примечание 1 — Производственные объекты и системы могут содержать компоненты и устройства, крайне важные для безопасности. Любые компоненты, относящиеся к безопасности, могут быть сертифицированы в рамках МЭК 61508 и в соответствии с его уровнями целостности безопасности (SIL). Настоящий стандарт не гарантирует, что ее технические требования полностью или частично соответствуют или достаточны для безопасности таких компонентов и устройств, важных для безопасности.

Примечание 2 — Настоящий стандарт не включает в себя требований к оценке и проверке обеспечения безопасности.

Примечание 3 — Меры, предусматриваемые настоящим стандартом, скорее привязаны к процессам и носят общий характер, в отличие от специальных, или носят характер директив, определяя технические контрмеры и конфигурации.

Примечание 4 — Положения настоящего стандарта описаны языком, привычным для владельца/оператора производственного объекта.

Издание официальное

Примечание 5 — Настоящий стандарт не распространяется на процессы жизненного цикла формулирования концепции, проектирования и реализации, т. е. устанавливает требования к разработке будущего продукта изготовителя управляющего оборудования.

Примечание 6 — Настоящий стандарт не распространяется на интеграцию компонентов и подсистем в систему.

Примечание 7 — Настоящий стандарт не распространяется на материально-техническое снабжение для интеграции в существующую систему, то есть требования к материально-техническому снабжению для владельца/операторов производственного объекта.

Примечание 8 — В рамках МЭК 62443 предусмотрена разработка трех частей, которые включают в себя большинство положений, изложенных в примечаниях 1—7. В приложении А приведен планируемый объем и содержание разрабатываемых стандартов.

2 Нормативные ссылки

Стандарты, ссылки на которые приведены в настоящем разделе, обязательны при применении настоящего стандарта. Для датированных ссылок применяют только указанное издание. Для недатированных ссылок применяют последнее издание ссылочного стандарта (включая любые изменения).

ISO/IEC 15408 (all parts), Information technology — Security techniques — Evaluation criteria for IT security (Информационная техника. Технологии безопасности. Критерии оценки для безопасности IT)

ISO/IEC 27002:2005, Information technology — Security techniques — Code of practice for IT security management (Информационная техника. Технологии безопасности. Свод правил для управления IT-безопасностью)

ISO/IEC Guide 73:2002, Risk management — Vocabulary — Guidelines for use in standards (Управление риском. Терминология. Директивы к использованию в стандартах)

3 Термины, определения и сокращения

3.1 Термины и определения

В настоящем стандарте применены следующие термины с соответствующими определениями:

3.1.1 **управление доступом** (access control): Предупреждение о несанкционированном использовании служебного ресурса, в том числе о его использовании без авторизации.

[ИСО/МЭК 18028-2:2006, изменен]

3.1.2 **источник угрозы** (adversary): Логический объект, совершающий атаку на систему или представляющий для нее угрозу.

[RFC 2828]

3.1.3 **сигнал тревоги** (alert): Текущая индикация, указывающая на то, что информационная система и сеть могут подвергнуться атаке или находиться в опасности вследствие аварии, сбоя или ошибки людей.

[ИСО/МЭК 18028-1:2006]

3.1.4 **имущественный объект** (asset): Что-либо, представляющее ценность для организации.

[ИСО/МЭК 13335-1:2004]

3.1.5 **надежность** (assurance): Характеристика соответствующих действий или процессов, дающая уверенность в том, что результат удовлетворяет требованиям безопасности.

[ИСО/МЭК/ТО 15443-1]

3.1.6 **атака** (attack): Попытки уничтожить, подвергнуть опасности, преобразовать или вывести из строя информационную систему и/или содержащуюся в ней информацию или иным образом затронуть политику безопасности.

[ИСО/МЭК 18043]

3.1.7 **поверхность атаки** (attack surface): Совокупность ресурсов системы, которые напрямую или косвенно подвержены потенциальному риску атаки.

3.1.8 **аудит** (audit): Официальные запрос, исследование или сравнение фактических результатов с ожидаемыми в целях подтверждения соответствия их установленным требованиям и совместимости между стандартами.

[ИСО/МЭК 18028-1]

3.1.9 **проведение аутентификации, аутентификация** (authenticate, authentication): Проверка заявляемой идентичности логического объекта.

[ИСО/МЭК 19792]

3.1.10 **доступность** (availability): Свойство быть доступным и используемым по запросу со стороны уполномоченного логического объекта.

[ИСО 7498-2]

3.1.11 **коммерчески доступные продукты** (Commercial off the shelf, COTS): Продукты, изготовленные и распределенные в промышленном масштабе для многократного применения и/или множества потребителей; могут быть изготовлены на заказ для специального применения.

Примечание — COTS следует отличать от продуктов, которые разрабатываются исключительно для специального применения.

3.1.12 **утечка информации** (compromise): Несанкционированное использование, рассекречивание, преобразование или замена в каждом из случаев — данных, программ или конфигурации системы, то есть в результате и после несанкционированного проникновения.

3.1.13 **конфиденциальность** (confidentiality): Свойство, указывающее на то, что информация не была доступна или раскрыта неавторизованным лицам, логическим объектам или процессам.

[ИСО/МЭК 13335-3]

3.1.14 **регистрационные данные** (credentials): Средство подтверждения того, что нечто или некто является тем, за кого себя выдает, причем такое абстрактное средство может представлять собой учетные IT-данные доступа к информационному сервису или ресурсу.

[ИСО/МЭК 24760]

3.1.15 **демилитаризованная зона** (demilitarized zone, DMZ): Хост безопасности или небольшая сеть (называемая также защищенной подсетью), располагаемые между сетями в качестве «нейтральной зоны».

[ИСО/МЭК 18028-3]

Примечание — Данная зона образует буферную зону безопасности (ИСО/МЭК 18028-3).

3.1.16 **отказ в обслуживании (атака)** [denial of service (attack)]: Атака на систему, направленная на ограничение ее доступности.

[ИСО/МЭК 18028-4]

3.1.17 **событие** (event): Событие в системе, относящееся к ее безопасности.

[RFC 2828, изменен]

3.1.18 **незащищенный, незащищенность** (exposed, exposure): Состояние уязвимости и отсутствия защиты против атаки.

3.1.19 **внешний** (external): Находящийся за пределами либо на внешней границе периметра безопасности промышленной сети управления (ICN), то есть относящийся к внешней организационной или общедоступной сети.

3.1.20 **шлюз внешних подключений** (external connectivity gateway; ECG): Специальный шлюз безопасности (SGW) на внешней границе периметра безопасности ICN, как правило, с дополнительными функциями для выполнения специальных запросов, то есть для подключения внешних устройств.

3.1.21 **внешняя сеть** (external network; EN): Сеть, внешняя по отношению к ICN, либо входящая в состав организации, к которой принадлежит ICN, либо принадлежащая третьей стороне, либо общедоступная, т. е. Интернет.

3.1.22 **экспертиза** (forensic): Действия по объяснению прошедшего события в официальном порядке и с возможностью перепроверки для возложения ответственности последовательным и логичным образом.

3.1.23 **шлюз, шлюз безопасности** (gateway, security gateway; SGW): Точка соединения между сетями или сети с подсетями и внешними сетями, предназначенная для защиты сети или подсети в соответствии с установленной политикой безопасности.

[ИСО/МЭК 18028-3, изменен]

Примечание — Шлюз безопасности включает в себя не только межсетевые экраны. Термин охватывает также маршрутизаторы и переключатели, которые обеспечивают функции управления доступом и при необходимости — шифрования (ИСО/МЭК 18028-3).

3.1.24 **усилить защиту, усиление защиты** (harden, hardening): Удаление ненужных функций для уменьшения физических, логических и/или организационных уязвимостей.

3.1.25 **человеко-машинный интерфейс** (human-machine-interface; HMI): Функция оборудования, направленная на предоставление выходной информации оператору и прием вводимой информации от оператора, в результате чего человек, например оператор, становится неотъемлемой частью процесса.

3.1.26 **инцидент** (incident): Событие безопасности или комбинация множественных событий безопасности, ставящие под угрозу безопасность.

3.1.27 **промышленная сеть управления** (industrial control network; ICN): Сеть, связывающая между собой оборудование промышленной системы управления (ICS). На территории одного и того же завода могут иметься различные ICN, которые могут быть связаны с удаленным оборудованием и ресурсами, находящимися за пределами завода.

3.1.28 **промышленная система управления** (industrial control system; ICS): Система, состоящая из хостов, устройств и оборудования для вычислений и управления производственными процессами, интегрированных между собой для управления промышленным производством, передачей информации или распределением ресурсов.

Примечание — В рамках настоящего стандарта термин ICS обозначает автоматизированные системы в целом, включая системы диспетчерского контроля и сбора данных (SCADA).

3.1.29 **инсайдер, в пределах, внутренний** (insider, inside, internal): Логический объект, находящийся в пределах периметра безопасности; инсайдер — это логический объект, уполномоченный на доступ к ресурсам системы.

Примечание — Атака инсайдером относится к использованию ресурсов системы на несанкционированной основе.

3.1.30 **целостность** (integrity): Гарантия точности и полноты информации и методов обработки информации.

[ИСО/МЭК 21827]

Примечание — Целостность может относиться непосредственно к данным (целостность данных) или к действующей ICS (целостность системы).

3.1.31 **интранет, интрасеть** (intranet): Компьютерная сеть, которая основана, в частности, на технологии общедоступной сети, используется организацией в собственных внутрикорпоративных, обычно приватных целях и недоступна для аутсайдеров.

3.1.32 **несанкционированное проникновение** (intrusion): Инцидент, при котором неуполномоченный логический объект, то есть злоумышленник, получает или явно пытается получить доступ к служебным ресурсам системы.

[RFC 2828, изменен]

3.1.33 **детектирование несанкционированных проникновений** (intrusion detection): Сервис безопасности, который позволяет отслеживать и анализировать системные события с целью выявления и уведомления в режиме реального или почти реального времени о попытках получения несанкционированного доступа к ресурсам системы.

[RFC 2828]

3.1.34 **криптографический или физический ключ** [(cryptographic or physical) key]: Устройство, носитель информации или открытый текст, связанные с методами аутентификации или криптографии, а также привилегиями управления доступом.

3.1.35 **протоколировать, протоколирование** (log, logging): Сбор данных о событиях информационной безопасности с целью ее проверки и анализа и текущий мониторинг.

[ИСО/МЭК 18028-1]

3.1.36 **вредоносные программы** (malware): Вредоносное программное обеспечение, такое как вирус или троянский конь, созданное специально для повреждения системы или вывода ее из строя.

[ИСО/МЭК 18028-1]

3.1.37 **контрмера** (countermeasure): Действие, устройство, процедура или стратегия, ослабляющие угрозу, уязвимость или противодействующие атаке путем ее отражения или предотвращения, или минимизации ущерба, который она способна нанести, или путем ее обнаружения и сообщения о ней, чтобы могло быть предпринято корректирующее действие.

[RFC 2828]

3.1.38 **сообщение** (message): Упорядоченная последовательность октетов (или бит), служащая для передачи информации.

[ИСО/МЭК 2382, изменен]

3.1.39 **отслеживать** (monitor): Прослеживать текущие действия и события в целях подтверждения информации о том, что было прослежено.

[ИСО/МЭК 13888-1, изменен]

3.1.40 **защита от непризнания участия** (non-repudiation): Свойство действия, допускающее многократную последующую проверку того, что это действие было выполнено данным участником или исходило от него.

[RFC 2828, изменен]

3.1.41 **владелец/оператор** (owner/operator): Хозяйствующий субъект, отвечающий за эксплуатацию системы ICS или SCADA.

3.1.42 **сегмент, сегментирование** (partition, partitioning): Ограниченная физическая или логическая зона, в которой предоставление доступа к ресурсам или отказ в данном доступе регулируются правилами доступа и механизмами контроля.

[CCOPP v0.5, изменен]

Примечание — Сегмент имеет четкую границу с другими сегментами. Политика безопасности сегмента, как правило, укреплена совокупностью механизмов, имеющихся как на периферии сегмента, так и внутри него. Сегменты могут иметь иерархическую структуру.

3.1.43 **периметр** (perimeter): Границы сегмента или зоны сети, обычно защищаемые механизмами в соответствии с политикой безопасности или принятым регламентом на управление доступом.

3.1.44 **ворота физического доступа** (physical access gate; PAG): Точка физического доступа, предназначенная для управления авторизацией, например, персонала и оборудования при их проникновении внутрь периметра безопасности завода и/или физического сегмента ICS или покидании пределов указанного периметра.

3.1.45 **открытый текст** (plaintext): Данные, которые человек или машина способны прочитать и понять, то есть входные данные, подлежащие преобразованию методом шифрования, или выходные данные, полученные методом расшифровки.

[RFC 2828, изменен]

3.1.46 **завод** (plant): Производственное помещение, которое обычно имеет физически защищенный периметр и на территории которого осуществляется физический процесс и расположены ICS и ее ICN.

3.1.47 **привилегия** (privilege): Право или разрешение, предоставляемые в явной форме отдельным пользователям или устройствам, а также определенной группе пользователей или устройств, на выполнение определенных действий, входящих в состав должностных обязанностей и объединенных между собой по отличительным признакам.

3.1.48 **прокси** (сервер) [proxy (server)]: Компьютерный процесс, который перенаправляет протокол между клиентской и серверной компьютерными системами, представляясь клиенту от имени сервера, а серверу — от имени клиента.

[RFC 2828, изменен]

3.1.49 **в режиме реального времени** (real-time): Относящийся к времени реагирования вычислительных устройств, которое настолько мало, что реагирование кажется мгновенным и без задержек.

3.1.50 **резервирование** (redundancy): Дублирование важнейших компонентов безопасности системы с целью повышения ее доступности.

Примечание — При резервировании возрастает доступность, но побочным результатом при этом обычно является повышение уязвимости, что относится, например, к коммуникационному каналу.

3.1.51 **остаточный риск** (residual risk): Риск, сохраняющийся после реализации контрмер.

[RFC 2828]

3.1.52 **риск** (risk): Сочетание вероятности события и его последствия, где вероятность — это количественная оценка возможности того, что это событие произойдет.

[ИСО/МЭК Руководство 73:2002]

Примечание — Последствием называется ущерб для имущественных объектов.

3.1.53 **защищенный, защищенность** (secure, security): Продукт, система или сервис считаются защищенными в такой степени, что их пользователи могут рассчитывать на то, что они функционируют (или будут функционировать) надлежащим образом. Это понятие обычно рассматривают в контексте оценки фактических или ощущаемых угроз.

[ISO/IEC/TR 15443-1]

3.1.54 **центр безопасности** (security centre): Надежный ресурс для мониторинга, исправления, обновления, обработки подписей и оповещения в рамках обеспечения безопасности ICN. Внешний центр безопасности расположен за пределами периметра безопасности ICN.

3.1.55 **система управления (информационной) безопасностью** [(information) security management system (ISMS)]: Часть общей системы управления, основанной на концепции делового риска, для создания, внедрения, эксплуатации, мониторинга, анализа, поддержки и улучшения организационной безопасности.

[ИСО/МЭК 27001, изменен]

3.1.56 **мера безопасности** (security measure): Мера защиты против возможного нарушения безопасности защищенной системы.

3.1.57 **политика безопасности** (security policy): Набор правил и методик, которые регламентируют или регулируют способ предоставления сервисов безопасности системой или организацией для защиты ее конфиденциальных и особо важных ресурсов.

[RFC 2828]

3.1.58 **значимость для безопасности/значимый для безопасности** (security relevance/relevant): Отдельное явление, то есть действие или событие, способное нарушить безопасность.

3.1.59 **нарушение безопасности** (security violation): Акт или событие, которое приводит к нарушению или иному несоблюдению политики безопасности.

[RFC 2828]

3.1.60 **эффективность функции** (strength of function): Качество функции безопасности, отражающее минимальные усилия, которые предположительно необходимы для преодоления ее ожидаемых характеристик безопасности путем непосредственной атаки на базовые механизмы безопасности.

[ИСО/МЭК 15408-1, изменен]

3.1.61 **доверие, доверять** (trust, trusted): Ожидание того, что для выполнения конкретной задачи сегмент, хост или устройство будут функционировать согласно прогнозу при определенных условиях функционирования и в соответствии с четко сформулированной политикой безопасности.

3.1.62 **угроза** (threat): Потенциальная возможность для нарушения безопасности при наличии обстоятельства, средства, действия или события, способных нарушить безопасность и нанести ущерб.

[RFC 2828]

3.1.63 **пользователь** (user): Лицо, организационная единица или автоматический процесс, получающие доступ в систему как на санкционированной, так и несанкционированной основе.

[RFC 2828]

3.2 Сокращения

В настоящем стандарте применены следующие обозначения и сокращения:

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

DMZ — демилитаризованная зона (Demilitarized zone);

ECG — шлюз внешних подключений (External connectivity gateway);

EN — внешняя сеть (External network);

GPH — универсальный хост (General purpose host);

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

ICS — промышленная система управления (Industrial control system);

IDS — система обнаружения вторжений (Intrusion detection system);

ISMS — система управления (информационной) безопасностью [(Information) security management system];

O/S — операционная система (Operating system);

PAG — ворота физического доступа (Physical access gate);

ICN — промышленная сеть управления (Industrial control network);

PSM — портативный носитель данных (Portable storage medium);

SED — автономное внешнее устройство (Stand-alone external device);

SGW — шлюз безопасности (Security gateway).

4 Введение и нормативно-правовое соответствие

Использование методик и стандартов IT-безопасности стало обычным явлением в офисной среде и выражено в форме повсеместного свода правил для управления информационной безопасностью (ИСО/МЭК 27002, ранее известный как ИСО/МЭК 17799), для эксплуатационной безопасности, а также в форме критериев оценки IT-безопасности (ИСО/МЭК 5408) при разработке продуктов.

Интернет и беспроводные сети уже появились на производстве. Проблемы безопасности автоматизированных систем все больше находят отражение в заголовках специализированных изданий. Однако общепризнанная практика и соответствующие стандарты запаздывают, и это несмотря на повышенный интерес в сфере автоматизированных систем. Это чревато возможными материальными производственными убытками и ущербом для здоровья, человеческой жизни и окружающей среды.

По аналогии тому, как ранее были предусмотрены методологические принципы для эксплуатационной безопасности в офисной среде, настоящий стандарт — это начальная попытка предусмотреть методологические принципы для безопасности эксплуатации автоматизированных систем.

Однако методики и стандарты из офисной среды не могут быть непосредственно применены к автоматизированным системам. Исследование, проведенное EWICS [15], показало, что широко применяемый ИСО/МЭК 27002 необходимо значительно расширить, чтобы он был применим к системам управления, используемым в промышленности. Несмотря на то что 189 пунктам в указанном исследовании была дана оценка от применимых до абсолютно применимых, 85 % или 45 % были признаны как требующие дополнительной методологической основы.

Настоящий стандарт содержит рекомендуемые нормы, установленные специалистами-практиками на основе практического опыта, но разработанные независимо от ИСО/МЭК 27002.

Примечание — Несмотря на то что желательно было бы согласовать структуру и терминологию настоящего стандарта с ИСО/МЭК 27002, на данный момент этого не сделано.

Предполагается, что настоящий стандарт заполнит существующий в настоящее время пробел, пока планируются дальнейшие действия по укреплению методологической основы в последующем издании МЭК 62443, как отмечено в приложении А.

Соответствие политике настоящего стандарта — вопрос частный. Это соответствие может быть указано в качестве примечания ко всем положениям политики ICS или к некоторым из них или к ее специальной версии.

Некоторые меры, описанные в настоящей политике, могут быть не применимы одновременно в конкретный момент времени для конкретной конфигурации в конкретном контексте безопасности. Политика допускает такое блочное исполнение и адаптацию.

Также, в зависимости от конкретной ICS, может быть признано необходимым или желательным, например, с точки зрения компромисса между риском и затратами, не реализовывать определенные меры, регламентированные настоящей политикой. В зависимости от характера безопасности это может быть сделано лишь временно во исполнение политики ICS, с использованием ее положений по управлению ошибками.

5 Принципы и базовые модели

5.1 Общие положения

В настоящем стандарте описаны рекомендуемые нормы в отношении технических и организационных мер безопасности для защиты ICS и ICN на ее основе, включая обычно существующие подсети ICN.

В настоящем пункте описаны соответствующие базовые модели.

Пользователи настоящего стандарта должны по возможности приспособить эти модели к конкретной задаче, чтобы увязать положения настоящей политики безопасности с конкретными требованиями.

Информация, представленная в настоящем стандарте, может нуждаться в дополнении другими моделями и соответствующей политикой, то есть анализом угроз-рисков, общей политикой безопасности и ISMS.

5.2 Модель угроз-рисков

5.2.1 Обзор

На рисунке 1 приведена общая модель угроз-рисков, относящаяся к безопасности. Из рисунка следует:

- угрозы используют уязвимости ICS;
- без контрмер они могут представлять недопустимый риск (для имущественных объектов);
- в общем случае для минимизации риска (для имущественных объектов) необходимы контрмеры.

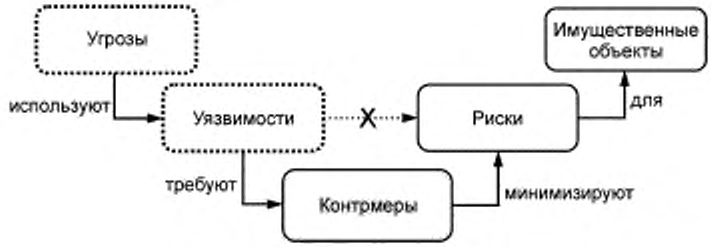


Рисунок 1 — Взаимосвязь угроз-рисков

Контрмеры общедоступны в виде общих методик, подробных регламентов и в некоторых случаях — подробных спецификаций.

Настоящий стандарт предусматривает контрмеры в виде методик, оформленных в предлагаемую политику.

5.2.2 Угрозы

Угрозы — это потенциальные нежелательные события безопасности, причиняющие ущерб, то есть финансовый убыток. В ICS могут произойти с той или иной вероятностью следующие события:

- атаки вандалов и террористов;
- сбой в ICS, за которым следует событие безопасности;
- атаки типа «отказ в обслуживании»;
- нарушение конфиденциальности, например утечка производственной информации;
- нарушение законодательных норм;
- нежелательное событие вследствие непреодолимой силы, например экстремальные погодные условия (шторм или торнадо).

Возможны и другие события, которые могут быть характерны для конкретной организации.

В типичном случае о наступлении таких событий должно быть доложено руководству, при этом от того, как быстро будет доложено, соответствующее действие и уровень задействования руководства зависят от их серьезности.

Такое событие, известное также как инцидент безопасности, можно представить себе как фигурирующее в газетном заголовке.

5.2.3 Риск

В ИСО/МЭК Guide 73 риск определен как «комбинация вероятности события и его последствий», то есть как ущерб или последствие инцидента безопасности. Наступление инцидента может привести к одному или более последствиям, а также спровоцировать другие события.

Ущерб, который может быть понесен в ICS, включает в себя:

- потерю дохода;
- непредвиденные расходы;
- невозможность частичного или полного ведения финансово-хозяйственной деятельности;
- потерю денежной стоимости зданий и содержимого;
- инцидент безопасности;
- штрафные санкции за нарушение законодательных требований, например касающихся контроля выбросов;
- последствия из-за нарушения нормативно-правовых требований, таких как стандарты GAM0;
- неудовлетворенность клиента;
- негативное освещение в прессе;
- судебное разбирательство против сотрудника или самого хозяйствующего субъекта.

Фактом является то, что защитные действия требуют денежных затрат на технологические, физические и организационные меры. Поэтому последствие неблагоприятного события безопасности обычно необходимо выражать в денежном выражении.

Риск для объектов ICS требует фиксации ценности объектов и их уязвимости перед атакой. Как правило, это очень трудно и субъективно, например, если рассматривать в качестве последствия потерю репутации организации.

5.2.4 Анализ угроз-рисков

Анализ угроз-рисков (TRA) предполагает оценку риска и соответствующих ему незащищенных объектов, угроз и уязвимостей. TRA — это предпосылка к выбору и детальной спецификации защитных мер.

TRA, в частности применительно к электронной атаке на компьютерные системы, соединенные с незащищенными или недоверенными сетями, в настоящее время не доступен для математико-статистического анализа, то есть атаки со стороны лиц-злоумышленников целенаправленны и не обладают статистическим свойством событий случайного сбоя. Таким образом, экстраполяция статистических данных (как обычно возможно при случайных отказах) не может прогнозировать будущую вероятность атаки со стороны человека. По этой причине вычисление вероятности наступления событий безопасности, возможно, позволит навсегда избежать чисто статистического подхода.

Несмотря на то что доступно множество моделей TRA, ни одна из них не общепризнанна. Количественные методы обманчивы. Обычно риск безопасности анализируют штатные эксперты или консультанты, после чего следует его оценка относительно критериев риска владельца/оператора ICS.

В связи с изложенным в настоящем стандарте методы TRA не представлены.

5.2.5 Обработка, принятие и информирование о рисках

После анализа рисков их, как правило, могут счесть неприемлемыми без обработки.

Риски обрабатывают с помощью мер, предложенных в настоящем стандарте, мер, которые могут быть отнесены в настоящем стандарте к предварительным условиям, а также мер, которые не приведены в настоящем стандарте, но которые владелец/оператор ICS, регламентирующий орган или законодатель могут счесть необходимыми.

Меры безопасности должны быть по возможности:

- эффективными, результативными и достаточно жесткими, чтобы противодействовать выявленным угрозам;
- прогнозируемыми в отношении прилагаемых усилий для их учреждения;
- простыми во внедрении и применении;
- лишены обратного эффекта в отношении существующего процесса производства;
- не требовать сопровождения.

Большинство требований настоящего стандарта допускают варианты, различающиеся объемом прилагаемых усилий и достигаемым уровнем защиты, для соответствия допустимому риску. Эффективность мер должна быть по возможности сбалансирована таким образом, чтобы защита, достигнутая с помощью одной меры, не могла быть ослаблена недостатком защиты, достигаемой с помощью другой меры.

Меры должны быть логически полными, то есть не оставлять слабых мест в системе безопасности. Действуя совместно, меры должны быть по возможности независимы друг от друга и, предпочтительно, поддерживать друг друга. Особое внимание следует уделить тому, чтобы гарантировать, что меры не препятствуют друг другу.

Меры — это расходы. Поэтому выбранные меры должны быть сбалансированы между собой для получения рентабельного решения. Если организация не может понести расходы, то может потребоваться процесс оптимизации, включающий в себя изменение конфигурации ICS, ограничение коммуникаций и дополнительные организационные мероприятия.

Кроме того, риск должен быть принят заинтересованными лицами и доведен до сведения всех заинтересованных сторон до реализации мер и при каждой существенной их корректировке.

Примечание — Ранее действующие и настоящий стандарт не затрагивают формальное установление доверия, требующее оценки безопасности с помощью признанных критериев и методологии, например ИСО/МЭК 15408 и/или ИСО/МЭК 27001.

5.3 Жизненный цикл безопасности

Положения настоящего стандарта основаны на модели жизненного цикла безопасности, приведенной на рисунке 2.

При обеспечении безопасности ICS необходимо учитывать следующие категории угроз и контрмер:

- социальные и организационные угрозы и меры, то есть злоумышленники-инсайдеры и несоответствующий мониторинг персонала;
- физические и естественные угрозы и меры, то есть злоумышленники-аутсайдеры и управление физическим доступом;
- электронные и логические угрозы и меры, то есть электронная почта и антивирусные программы.

В настоящем стандарте приведены в основном электронные и логические категории, что отмечено на рисунке 2 крупными галочками.

Примечание — Там, где требуется специальный прикладной жизненный цикл (например, жизненный цикл безопасности), такой регламент управления жизненным циклом должен по возможности объединять в себе аспекты IT-безопасности настоящего стандарта.

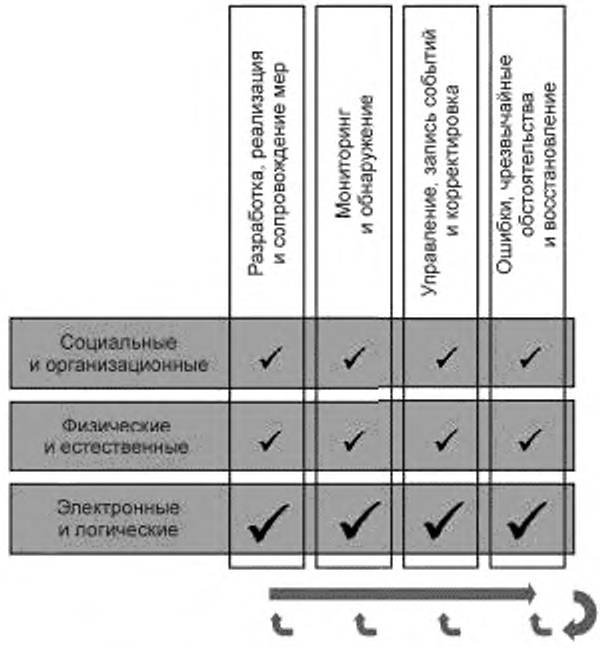


Рисунок 2 — Жизненный цикл безопасности

Модель предполагает четыре сферы особого внимания:

- разработка, реализация и сопровождение мер по предотвращению риска, включая управление обновлениями и патчами;
- мониторинг созданной и сопровождаемой таким образом системы безопасности, то есть для обнаружения любого несанкционированного проникновения;
- управление системой, включая запись событий и корректирующие воздействия, пока несанкционированные проникновения поддаются управлению;
- управление ошибками при чрезвычайных обстоятельствах и восстановлением, когда происходят более серьезные инциденты, в том числе управление непредвиденными обстоятельствами в случае наихудших сценариев.

На рисунке 2 прямая стрелка показывает, что четыре сферы, логически вытекающие друг из друга по своему принципу, могут быть введены последовательно, по меньшей мере на начальном этапе запуска ICS после обеспечения ее безопасности.

Важно принимать во внимание, что в противоположность обычным техническим дисциплинам техника обеспечения безопасности — это по сути бесконечный процесс. Этот процесс требует, чтобы все сферы вводились постоянно или периодически для приспособления ICS к постоянно меняющимся технологическим и угрожающим средам.

5.4 Политика

5.4.1 Обзор

Политика — это свод основополагающих принципов и мер безопасности. Меры группируются по аспектам безопасности, которые привязаны к общепризнанным концепциям безопасности.

Меры, предлагаемые в соответствии с настоящей политикой, остаются базовыми и допускают масштабируемость, свободу выбора соответствующих доступных технологий и будущие усовершенствования.

Политика имеет иерархическую структуру в виде четырех уровней, как показано на рисунке 3. В центре внимания настоящего стандарта — оперативная политика, которая в общем случае имеет характер методик. Оперативную политику следует понимать в рамках полной политики.



Рисунок 3 — Уровни политики

5.4.2 Руководящая политика безопасности

Политика на самом верхнем уровне организации санкционирует программу безопасности и обозначает направление. Она устанавливает общие цели безопасности организации.

Формулировка политики высшим руководством должна быть достаточно продуманна и оставаться актуальной и точной при изменениях в структуре организации, в технологии системы и безопасности и в характере угроз безопасности. Будучи продуманной, политика может быть стабильной и будет нуждаться в переработке только в случае изменения исходной позиции организации в отношении безопасности. Однако формулировка политики является однозначной. Она четко определяет, что требуется.

Политика безопасности верхнего уровня организации определяет общие сферы ответственности и подотчетности для организационных сфер.

Примечание — Например, политика может определять взаимоотношения между руководством корпоративным IT-отделом и ICS и их соответствующие обязанности. Политика может разграничивать цели безопасности системы управления от целей безопасности корпоративной сети. Например, важнейшим аспектом безопасности корпоративной сети может быть сохранение конфиденциальности, в то время как важнейшим аспектом безопасности системы управления может быть обеспечение бесперебойной работы.

Кроме того, организационная политика безопасности может определять конкретные стандарты и нормы, применимые к организации в целом.

Руководству следует доводить политику безопасности до сведения всей организации, чтобы все сотрудники понимали эту политику, а также могли регистрировать последствия ее нарушений.

Политику безопасности этого уровня периодически пересматривают. Периодичность пересмотра может варьироваться в соответствии с требованиями руководства и быть чаще на первых этапах после внедрения.

Данный уровень политики безопасности ICS приведен в разделе 7.

5.4.3 Оперативная политика

Оперативные политики разрабатывают на нижних уровнях организации для определения того, как необходимо реализовывать положения корпоративной политики безопасности в соответствующих организационных сферах.

Эти политики определяют, что необходимо предпринять в отдельно взятой организационной сфере для достижения целей корпоративной политики. Они подчиняют себе регламенты безопасности, расположенные уровнем ниже.

Регламенты должны по возможности затрагивать все необходимые этапы жизненного цикла программы безопасности с точки зрения отдельно взятой организационной единицы:

- разработку системы;
- материально-техническое снабжение;
- технологический процесс;
- сопровождение системы;
- персонал;
- аудит.

В типичном случае политику на этом уровне пересматривают периодически и по определенным поводам, например каждый раз при внедрении нового, корректировке существующего бизнес-процесса или его ликвидации.

Особое внимание в настоящем стандарте уделено эксплуатации и обслуживанию ICS. Настоящий стандарт не предусматривает методологической основы по таким вопросам, как беспроводные устройства и датчики, персонал, политика субподряда и материально-техническое снабжение.

Соответствующий уровень политики безопасности ICS отражен в 7.3.5, который затрагивает следующие сферы управления:

- целостностью;
- логическим доступом;
- физическим доступом;
- сегментами;
- доступностью;
- администрированием, аудитом и нештатными ситуациями;
- внешним доступом.

5.4.4 Рабочие регламенты

Регламенты должны по возможности устанавливаться владельцем/оператором и воплощать оперативную политику, представленную в настоящем стандарте, определяя степень их вовлеченности и подотчетность за действие, пересмотр и обновление таких документов.

Рабочие регламенты устанавливают порядок исполнения оперативной политики. Они устанавливают необходимые действия и могут ссылаться на соответствующие методы и справочные документы, в том числе стандарты.

Политику на этом уровне пересматривают каждый раз при утверждении, корректировке или отклонении оперативной политики.

В подпунктах подраздела 7.3 приведен ряд аспектов, которые должен по возможности устанавливать регламент.

Примечание — Регламенты содержат также информацию о порядке изменения других регламентов.

5.4.5 Рабочая методика

Рабочая методика должна по возможности содержать конкретные измеримые требования и конкретизировать регламенты, учитывая конкретные инструкции от владельца/оператора. В связи с тем, что они еще более привязаны к организации и организационной сфере, в настоящем стандарте они могут быть приведены только как примеры.

Политику на этом уровне изменяют периодически, по мере изменения в планах и технологиях руководства общей инфраструктурой. Сама по себе она временна и может подлежать пересмотру в любое время.

Все меры должны по возможности рассматриваться каждым конкретным пользователем настоящего стандарта и адаптироваться к его конкретным требованиям и ситуации риска.

5.5 Типовые эталонные конфигурации

5.5.1 Промышленная система управления (ICS)

ICS обычно состоит из электронного оборудования, то есть хостов и устройств, и может включать в себя сети, подсети и соединения «один к одному», как показано на рисунке 4. Как правило, система включает в себя ICN и соединенные с ней оборудование и подсети, а во многих случаях — еще и внешние хосты и устройства внешних сетей, подключенные к данной сети через средства сетевого взаимодействия.

В современной ICS, как правило, используются внешние коммуникации, чтобы получать доступ к внешним ресурсам и быть доступной для них, как показано на рисунке 4.

Внутренние устройства и операторы ICS могут нуждаться в доступе к внешним ресурсам, например для обновлений или управляющей информации.

Внешние операторы и устройства ICS могут получать доступ к ICN, например, в целях диагностики, обслуживания, разработки и/или управления.

Примечание — Внутриобъектовое подключение внешнего оборудования, привнесенного на производственный объект обслуживающим персоналом, причислено к внешним коммуникациям.

Внешние коммуникации могут служить для соединения ICN с системами, хостами и устройствами, такими как:

- внешний(е) центр(ы) безопасности;
- внешняя(ие) система (ы) поддержки изготовления и управления;
- обособленное(ые) стационарное(ые) устройство(а);
- интерактивный(е) пульт(ы)/хост(ы) интерактивного удаленного доступа;
- пульт(ы)/центр(ы) удаленного доступа;
- портативная(ые) рабочая(ие) станция(и) инженера;
- портативный(е) носитель(и) информации.

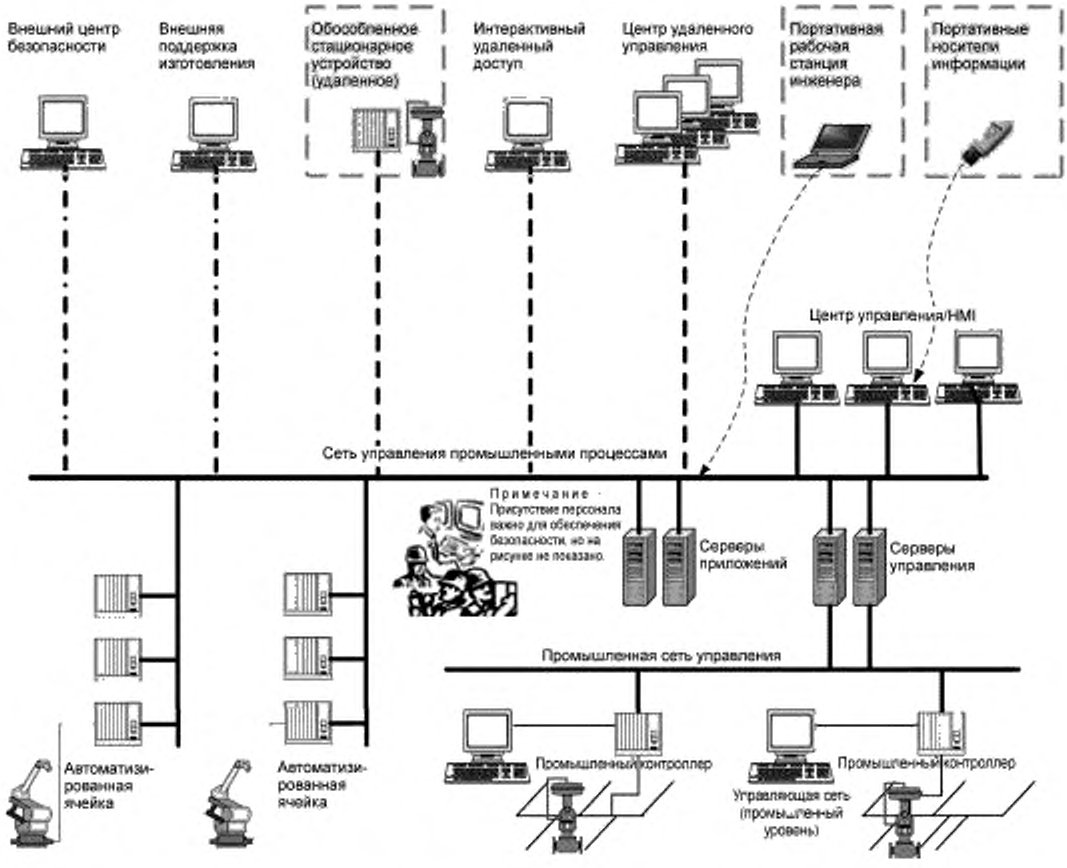


Рисунок 4 — Промышленная система управления (ICS)

5.5.2 Промышленная сеть управления (ICN)

ICN может быть образована путем интегрирования устройств со значительным разнообразием, включая:

- хосты, прокси-серверы, шлюзы, концентраторы, маршрутизаторы;
- периферийное IT-оборудование;
- технологическое контрольно-измерительное оборудование, исполнительные механизмы, преобразователи и т. д.

Хосты ICN могут функционировать как серверы приложений, серверы управления и другие специальные HMI.

ICN соединена непосредственно или опосредованно с выделенными сетями, то есть автоматизированными ячейками и/или сетями периферийных устройств.

Многие из этих хостов и устройств, за исключением простого оборудования, соединены между собой через сетевую аппаратуру и кабели, образуя ICN. ICN может включать в себя выделенные сети, соединенные с ней непосредственно или опосредованно, в частности автоматизированные ячейки и/или сети периферийных устройств.

Частью парка оборудования являются также устройства, которые содержат ресурсы обработки и хранения данных. Указанные устройства являются лишь временной частью парка. Особое внимание следует уделять устройствам, вносимым и уносимым с производственного объекта, таким как портативные компьютеры или портативные накопители.

5.5.3 Универсальный хост (GPH) промышленной системы управления

Настоящий стандарт применяют к хостам, которые могут быть аналогичны GPH ICS. Конфигурация GPH, представленная на рисунке 5, иллюстрирует его ключевые компоненты:

- центральный процессор с его неотъемлемыми компонентами, такими как накопитель большой емкости и интерфейсы;
- пульт оператора с устройствами ввода и отображения данных;
- интерфейс/накопитель для считывания информации с внешних носителей данных, таких как USB-накопители и гибкие магнитные диски;
- интерфейс и кабели связи с устройством управления/периферийным устройством;
- интерфейс связи с ICN.

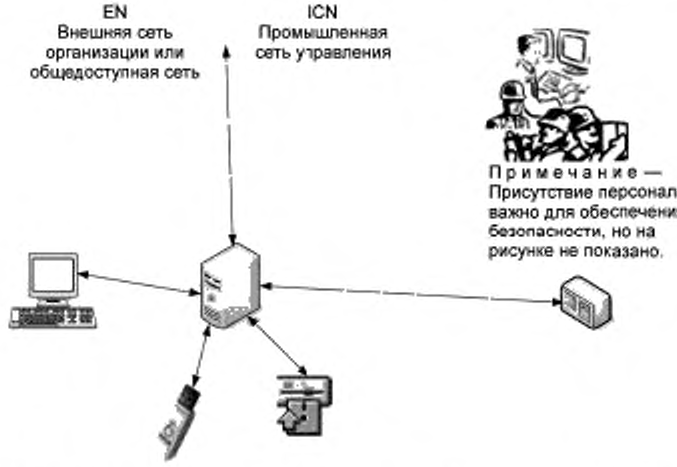
GPH может представлять собой также простую ICS, не содержащую ICN. Такая система может быть впоследствии соединена:

- с внешней общедоступной сетью, такой как Интернет;
- с внешней организационной сетью.

Эталонная конфигурация GPH, приведенная на рисунке 5, даст представление:

- о простейшей ICS без ICN;
- об отдельных хостах в составе ICS как обособленных элементах;
- о любом программируемом/программном устройстве как компоненте ICS в целом;
- об интерфейсе и кабелях связи с внешней сетью, такой как Интернет или корпоративная сеть.

На рисунке 5, а также на других рисунках отмечено присутствие людей. Люди — это часть практически любой системы, даже если они осуществляют только удаленное обслуживание или управляющие воздействия, и именно люди являются основной причиной и инициаторами угроз.



Примечание 1 — Могут использоваться и беспроводные соединения, например, взамен кабелей связи с сетью или устройствами.

Примечание 2 — Конфигурация хоста, приведенная на рисунке, является лишь наглядным примером и не предназначена для задания какой-либо топологии сети.

Рисунок 5 — Эталонная конфигурация GPH — GPH ICS с внешними устройствами

5.6 Модели защиты

5.6.1 Целостность и защита доступа

Основные принципы безопасного управления доступом и обеспечения целостности можно рассмотреть, используя типовую конфигурацию простого GPH (см. рисунок 5).

Зоны защиты применительно к GPH представлены на рисунке 6.

Рисунок дает представление о том, что угрозы, исходящие от ICS и ее среды, могут быть пресечены на физической границе комнаты, шкафа или на электрической границе центрального процессора (CPU) и интерфейсов хоста.

Логическая граница вокруг GPH может быть создана мерами по обеспечению целостности — усилением защиты за счет конфигурирования O/S, приложений и служб (на рисунке 6 соответствующие компоненты помещены в круги, обозначенные пунктиром).

Усиление защиты кабелей передачи на коротких расстояниях может быть осуществлено физическими средствами. На больших расстояниях следует использовать криптографические средства (показано пунктирными линиями, идущими параллельно кабелю).

Меры по обеспечению целостности и управлению доступом применяются по общему образцу к сценариям, в которых:

- для операторов и внутренних устройств ICS может быть необходимо подключение к ICN;
- сеть ICN подключена к другим сетям ICN и/или подсетям.

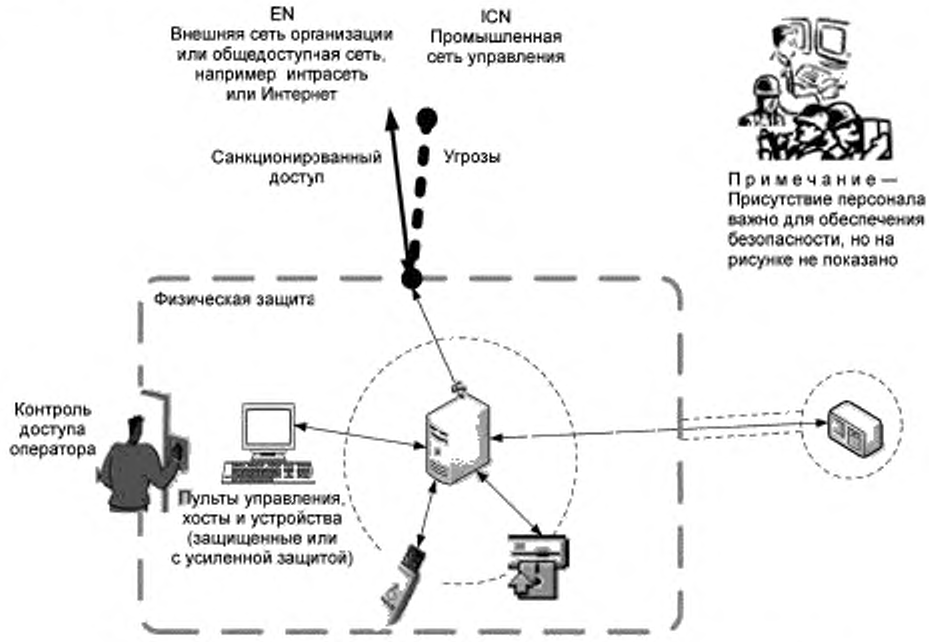


Рисунок 6 — Защита устройства — усиление защиты и управление доступом

5.6.2 Защита сегментов

Архитектура принципа обеспечения безопасности сегмента основана на предположении, что топологическая структура промышленной сети может быть разделена на отдельные сегменты безопасности. На этом же уровне различные сегменты могут быть соединены друг с другом магистральной сетью, например в основной ICN, каждый сегмент может иметь единственную точку входа в магистральную сеть.

Рассмотрение сегментов в основном выполняется для:

- самой сети ICN;
- сегментов подсети ICN;
- специальных сегментов сети ICN, например шлюзов SGW в конфигурации DMZ.

Примечание — ICN определена таким образом, что фактически сама не содержит сегментов внешней сети EN. Ее общая защита от внешних устройств и/или сетей обеспечивается шлюзами внешних подключений (ECG).

Дополнительно могут быть созданы специальные (несетевые) сегменты внутри физических хостов и устройств, обеспечивающие соответствующее управление доступом для защиты, например:

- самого хоста или устройства от угроз ICN;
- ядра операционной системы и сетевых служб от приложений и инструментов;
- критичных приложений от менее критичных;
- мониторинга безопасности и приложений администрирования от приложений управления.

Основными мерами защиты для сетей с высокой безопасностью являются:

a) иерархическая или ступенчатая структура сегментов;

b) строго суженный набор интерфейсов (вплоть до минимально необходимого, например использование ограниченного набора функций/адресов);

c) строгие меры управления доступом (например, применение специальной схемы привилегий, блокирование несанкционированных изменений, намеренный отказ от служб контрмер).

Примечание — Для сети или сегментов сети, связанных с приложениями эксплуатационной безопасности, в соответствии с МЭК 61508 (МЭК 61511), особое внимание следует уделять соответствию приложений мониторинга излучений требованиям действующего местного законодательства и приложений контроля качества действующим в промышленности соглашениям, таким как GAMP 0. В этом случае эта сеть или сегмент сети могут считаться сетью с высокой безопасностью.

При иерархической структуре сегментов каждый подчиненный сегмент вследствие сегментации получает дополнительную защиту и «эшелонированную оборону», так как защищенная граница каждой подчиненной сети представляет собой дополнительную линию обороны.

Примечание — Сеть, расположенная снаружи сегмента, даже если она находится внутри ICN, может рассматриваться как «ненадежная с исключениями» по отношению к типам трафика сети и объемам, а также намерениям и возможностям пользователей.

Успешная дополнительная защита на пути атаки снаружи на внутреннюю сеть не состоит только из одной обороны границы, она также предполагает обнаружение и реагирование.

На рисунке 7 приведен пример принципа эшелонированной обороны, которую обеспечивает иерархическая сегментация. Показано, например, что угрозы из интернета пресекаются на границе внешней сети организации. Однако политика безопасности ICS считает эту внешнюю сеть организации ненадежной и требует также пресечения угроз и на границе ICN.

Если атака не будет пресечена на границе ICN, атакующий может преодолеть дальнейшие меры, принятые на отдельных устройствах и серверах, а также на границе критичной автоматизации и сетей, управляемых в поле. Благодаря сочетанию ступенчатого подхода с другими соответствующими мерами владелец/оператор завода может быть уверен в том, что при всех обстоятельствах ICS в достаточной степени защищена от атаки.

Внутри сети ICN любой сегмент подсети защищен шлюзом SGW на ее границе. Подобно этому устройства защищены некоторым функционалом безопасности, который показан на рисунке 7 (круги вокруг устройств, выделенные пунктиром).

Следует иметь в виду, что, в зависимости от анализа угроз и рисков, других требований владельца/оператора, могут существовать меры, применяемые к соответствующим подмножествам и надмножествам сегментов.

Примечание — Любая политика безопасности должна требовать баланса мер усиления, так как обеспечение требуемой защиты одного канала доступа может привести к ухудшению защиты другого канала. Поэтому логическое разделение на сегменты, описанное в настоящем подпункте, должно дополняться адекватной физической защитой, в том числе правилами вноса/выноса портативных устройств на завод и его сегменты.

Применение принципа эшелонированной обороны, приведенного на рисунке 7, например сценария (адаптированного из рисунка 4), показывает пример сегментации ICS, представленный на рисунке 8.

В этой модели защиты периметр ICN защищен шлюзом внешних подключений (ECG) и воротами физического доступа (PAG).

Шлюз ECG является выделенным шлюзом безопасности (SGW) с дополнительным функционалом, удовлетворяющим требованиям конкретной политики, например, для внешних устройств.

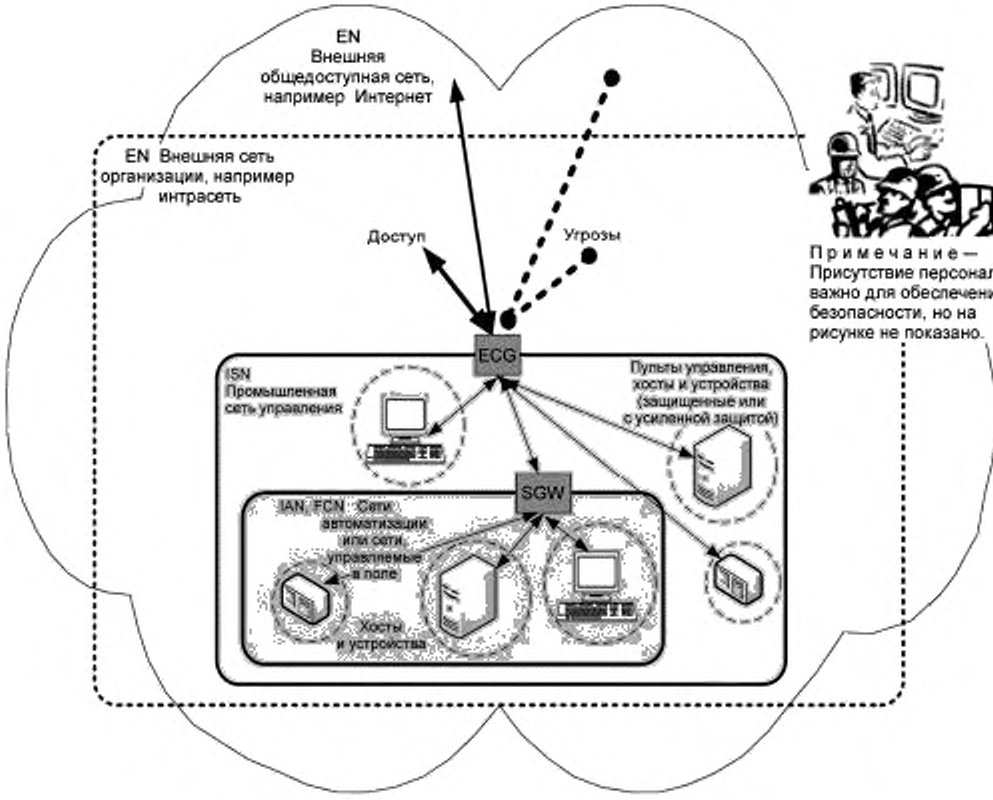


Рисунок 7 — Эшелонированная оборона за счет использования сегментации

PAG представляют собой пункт физического доступа, который должно пройти устройство при вносе/выносе через периметр безопасности ICN, гарантирующий, что политики безопасности ICS не будут нарушены, например, из-за передачи конфиденциальной информации или вноса вредоносного программного обеспечения.

Могут использоваться дополнительные сегменты от подсетей до конкретных устройств с усиленной защитой, рассматриваемые как сегмент.

Примеры

- защищенный хост сети управления;

- принцип управления сетью на верхнем/нижнем уровне;

- сеть внутри ICN, содержащая все хосты с операционными системами общего назначения;

- конкретные устройства с усиленной защитой (например, хосты), для которых сегмент соответствует одному устройству. Данные устройства формируют защитный периметр.

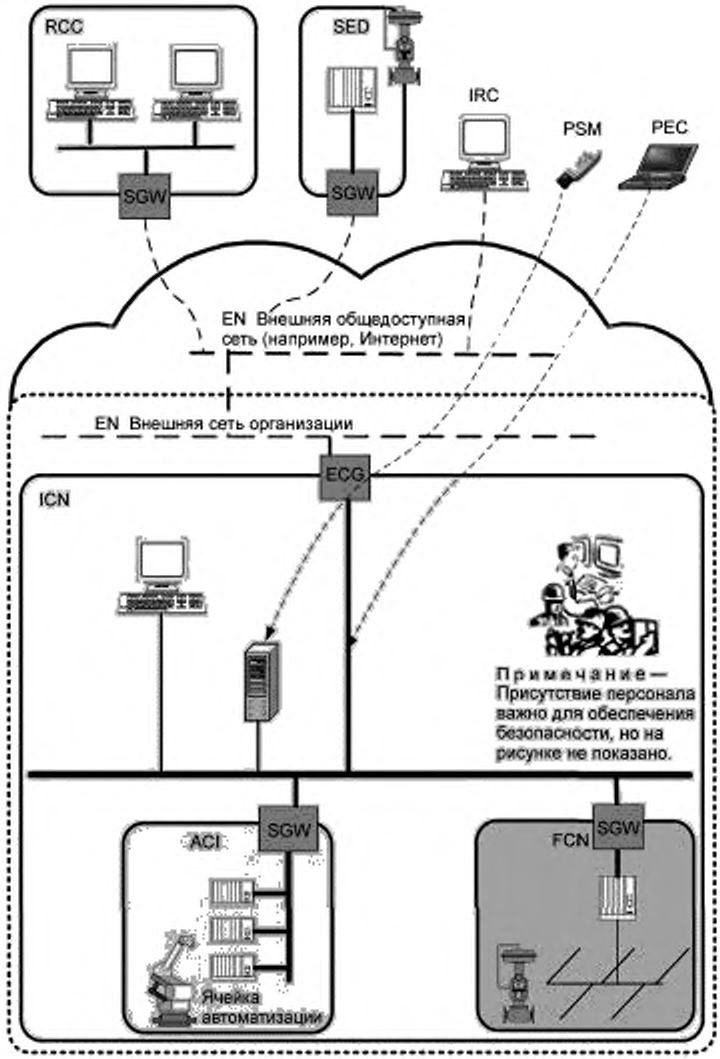


Рисунок 8 — Пример — сегментация ICS

5.6.3 Общие меры защиты внешнего доступа

С точки зрения ICN любая EN является ненадежной по отношению к типам и объему сетевого трафика, а также к намерениям и возможностям пользователя. Поэтому в настоящем стандарте описаны отдельные меры защиты сети для внешней границы ICN, выходящие за рамки мер, принимаемых внутри сети.

Хосты или устройства могут пытаться использовать общий внешний доступ, который обычно означает использование незащищенных сервисов интернета, например использование браузера, электронной почты (e-mail), передачи файлов и т. д. Общие внешние сервисы могут пытаться подключиться к незащищенным общим сервисам ICN.

Внутри ICS имеются два компонента, которые могут реагировать или отвечать на общий внешний доступ (см. рисунок 9):

- средства, обеспечивающие соединения при связи, в том числе интерфейсы, протоколы и сервисы (входящие и исходящие для ICS) на ECG;
- соответствующее внутреннее оборудование и приложения внутри ICS.

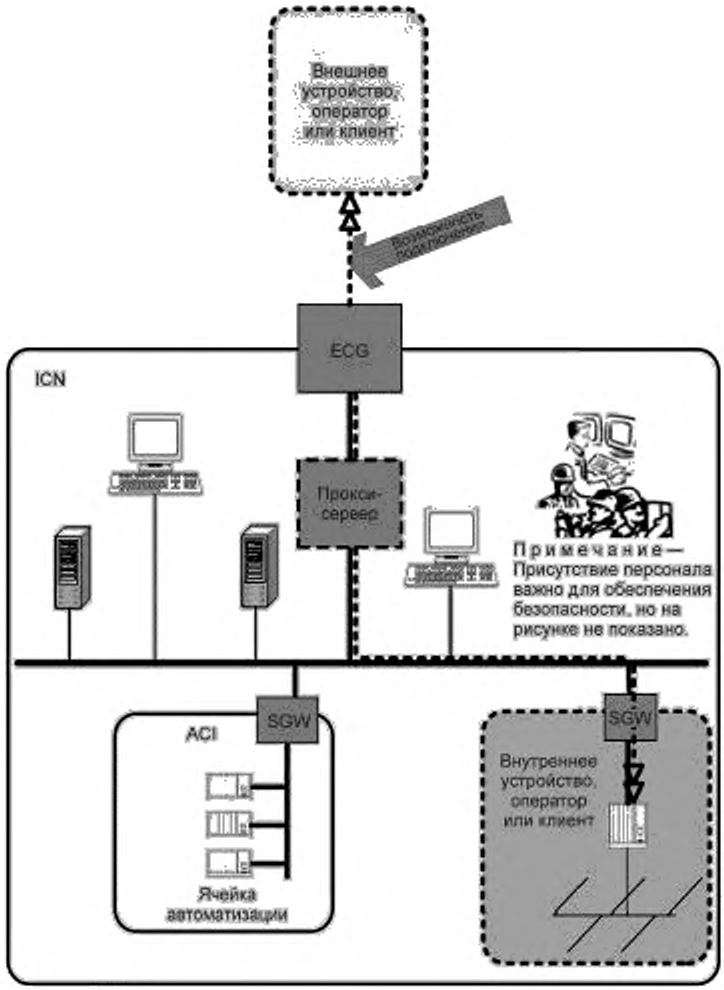


Рисунок 9 — Общие внешние соединения

Внутри корреспондентом может быть оборудование источника или назначения, связывающееся с внешней сетью напрямую или через оператора или через промежуточный прокси-сервер.

Снаружи партнеры по связи могут быть различными — от надежных до подозрительных.

Примечание — Общий внешний доступ не включает в себя специальных внешних промышленных клиентов управления, которые рассмотрены в 5.6.4.

Установленный общий внешний доступ и новые запросы этого типа соединений должны быть рассмотрены в целях безопасности, например является ли абсолютно необходимым общий web-доступ внутри ICN.

Даже при специальной связи с надежными внешними партнерами и соответствующим образом выполненными бизнес-требованиями требуются ECG, гарантирующие поддержку только требуемых сервисов и усиленные привилегии внешнего доступа.

5.6.4 Защита внешнего клиента

Если для работы с ICS требуется связь с удаленными (внешними) клиентами, связь с внешними сетями должна быть защищена. Внешние сети EN с точки зрения ICS являются ненадежными (см. 5.6.3). Безопасность должна быть распространена на архитектуру, реализацию и работу соединения.

Меры по защите внешнего клиента применяются на общих основаниях к сценариям, при которых:

- операторы и внутренние устройства ICS могут нуждаться в доступе к внешним ресурсам, например, для обновления или для получения информации управления;

- внешние операторы и устройства ICS могут получать доступ к ICN, например, для целей диагностики, обслуживания и/или управления.

В частности, политика ICS применима к защите внешнего клиентского оборудования и его приложений. Она также применима к важной проблеме оборудования, временно находящегося снаружи ICS и доставляемого на завод для прямого или косвенного подключения к ICN, например портативных устройств для обслуживания и носителей для обновления программного обеспечения.

Соответствующие каналы удаленного доступа должны быть в типичном случае защищены более сильными мерами, чем используемые внутри ICS. В отличие от общего доступа, каналы клиентов удаленного доступа могут, в дополнение к интернету, использовать набор номера определенного сотового телефона, вызов на радиочастоте, другие действия, выполняемые через операторов общего доступа или частных операторов связи.

Одним из основополагающих принципов для этой политики является, насколько это возможно, отделение технологии доступа от требуемых механизмов и мер безопасности.

Для внешних клиентов и прокси-серверов существует сильная зависимость от внутренних корреспондентов, использующих установленные специальные правила доступа и процедуры на стороне ICN и ECG. Тем не менее особое значение необходимо уделять безопасности внешнего клиента, находящегося за пределами досягаемости плана оператора и поэтому нуждающегося в особом внимании.

Повышение требований безопасности может потребовать связи с оборудованием ICS для транзита через прокси-сервер приложений внутри ICN, так как использование прокси-серверов существенно улучшает безопасность.

Альтернативное решение состоит в использовании сквозного шифрования с защитой целостности или применения технологии безопасных частных сетей.

6 Политика безопасности промышленной системы управления — основные сведения

Хосты ICS, сеть ICN, внутренние устройства, внешние хосты или устройства должны быть безопасными вместе с их клиентами, каналами доступа, используемыми хостами клиентов и устройствами для связи с ними.

Такая политика безопасности ICS предполагает меры по выполнению требований безопасности ICN при подключении к какой-либо внешней сети организации и/или общедоступной сети. Эти меры относятся к безопасности хостов, устройств, ICN и связи с внутренней частью ICS, а также в пределах внутренней части ICS, в том числе с подключенными хостами и устройствами, являющимися внешними по отношению к заводу или ICN, к повышению безопасности и обеспечению требований к безопасности эксплуатации.

Примечание — Политика также учитывает исключения, допуская управление ими и анализ рисков отклонения от политики.

Предлагаемые меры политики безопасности ICS сгруппированы по подпунктам соответствующего содержания:

- принципы, описывающие политику, представляют собой общие положения, применимые ко всем мерам безопасности, принимаемым в расчет для ICS и ее ICN, в том числе к предварительным условиям безопасности и заданным исключениям из политики, например к требованиям безопасности, связанным с безопасностью эксплуатации;

- управление доступностью как специфическая проблема сетей реального времени, нечасто встречающаяся в общем IT (см. 8.1);

- управление целостностью, включая требования для:

  - защиты от вирусов и другого вредоносного программного обеспечения;

  - обновления и исправления ошибок программного обеспечения и фирменного программного обеспечения;

  - резервного копирования;

  - целостности файлов и файловой системы;

  - усиления защиты аппаратных средств, операционной системы и приложений;

- управление логическим доступом, связанное с доступом к хостам, устройствам, носителям и информации, включающее требования для:
  - идентификации пользователя;
  - обеспечения привилегий пользователя, например учетных записей и прав доступа;
  - шифрования;
  - управления всем вышеперечисленным.

Примечание — Эта категория мер неразрывно связана с правилами, управляющими работой шлюзов безопасности;

- управление физическим доступом представляет собой правила для безопасного физического доступа в комнаты, кабинеты и к шкафам для обеспечения безопасности хостов, устройств и носителей посредством установления требований для:
  - идентификации пользователя;
  - привилегий пользователя, например для ключей и других прав доступа;
  - управления всем вышеперечисленным;
- управление сегментом как основная мера защиты для сетей с высокой безопасностью. По этой причине проблемы с сегментацией вынесены в отдельный подпункт;
- управление внешним доступом с учетом конкретных угроз, исходящих от общедоступных сетей;
- администрирование, мониторинг, управление в опасных условиях, координация общих проблем для всего вышеперечисленного с целью обеспечения:
  - управления исключениями;
  - протоколирования и мониторинга;
  - реагирования на опасные условия.

7 Политика безопасности промышленной системы управления — принципы и допущения

Цель указанной политики — обеспечение администрации ICS директивной информацией, в которой указано, на что распространяется политика безопасности ICS, ее позиционирование внутри политик организации, соответствие другим требованиям организации или техническим требованиям, бизнес-требованиям, требованиям соответствующих законов и регламентов.

7.1 Политика безопасности промышленной системы управления — принципы

7.1.1 Политика безопасности ICS превалирует над подчиненными политиками, за исключением случаев, когда явно выражено иное.

Это обосновано тем, что при возникновении конфликта утверждений политик для различных политик, действующих на заводе и на площадках его контрагентов, должно быть установлено старшинство политик.

Правила реализации политики приведены в 7.1.1.1 и 7.1.1.2.

7.1.1.1 Должно быть заключено соглашение об уровне безопасности предоставляемых услуг между сервисной организацией и организацией ICS, устанавливающее требуемый уровень доверия.

7.1.1.2 Соглашение об уровне безопасности предоставляемых услуг должно быть согласовано с политикой ICS.

Пример — Если оператор ICS и оператор удаленного центра управления принадлежат различным организациям или находятся на разных объектах, они могут использовать отличающиеся политики информационной безопасности. Соглашение о безопасности предоставления услуг может потребоваться, например, для указания мер по аутентификации, по сдерживанию распространения информации, по пресечению угроз, исходящих от вирусов и вредоносного программного обеспечения.

Дополнительная информация относительно безопасности приведена в соглашениях со сторонними организациями в соответствии с ИСО/МЭК 27002.

7.1.2 Политика безопасности ICS подчиняется политике безопасности организации и дополняет ее. При возникновении конфликта политика безопасности организации является приоритетной.

Это обосновано тем, что существующие корпоративные политики должны соблюдаться политикой безопасности ICS.

Правила реализации политики приведены в 7.1.2.1.

7.1.2.1 Политика безопасности ICS может быть исключена из этих положений. В этом случае может потребоваться существенное дополнение положений настоящего стандарта.

Дополнительная информация — по ИСО/МЭК 27002.

7.1.3 Политика безопасности ICS подчинена функциональной политике безопасности, связанной с безопасностью эксплуатации.

Это обосновано тем, что политика безопасности ICS не распространяется на безопасность функционирования, а также на требования безопасного функционирования и эксплуатации в опасных условиях, которые во многих законодательствах считаются имеющими высокую или наивысшую важность.

Правила реализации политики приведены в 7.1.3.1.

7.1.3.1 Изменения в политике безопасности ICS должны быть утверждены администрацией, отвечающей за безопасность эксплуатации.

7.1.4 Политика безопасности ICS дополняет требования местного или национального законодательства. При возникновении противоречий приоритет имеют требования местного или национального законодательства.

Это обосновано тем, что требования законодательства, официальные распоряжения (на федеральном уровне, на уровне страны, города) имеют приоритет над техническими требованиями и требованиями организации.

7.1.5 Политика безопасности ICS может быть дополнена либо принудительно обойдена требованиями регулирующих документов.

Это обосновано тем, что регулирующие документы (например, федеральные, национальные, города, промышленности) могут дополнять или принудительно обходить организационные и технические меры этой политики.

Правила реализации политики приведены в 7.1.5.1.

7.1.5.1 Политика безопасности ICS должна быть рассмотрена и, по возможности, утверждена представителями органов государственной власти, осуществляющих надзор за соблюдением требований регулирующих документов в организации и/или в регулятивном органе.

Примечание — В соответствии с требованиями эксплуатационной безопасности, установленными в МЭК 61508 и МЭК 61511, приложения, осуществляющие мониторинг излучений, должны соответствовать требованиям действующего местного законодательства и требованиям к приложениям контроля качества, изложенным в GAMP [16]. Они могут подпадать под действие этого положения.

7.2 Политика безопасности промышленной системы управления — допущения и исключения

7.2.1 Политика безопасности ICS не обеспечивает доступности данных функционирования и целостности этих данных.

Это обосновано тем, что свойства передачи данных в реальном времени и коррекция ошибок являются частью функционала ICS, они соответствуют требованиям эксплуатационной безопасности и разработаны для коррекции отказов и ошибок функционирования системы.

Правила реализации политики приведены в 7.2.1.1.

7.2.1.1 Для передачи соответствующих данных безопасности следует использовать каналы, которые имеют требуемые свойства с точки зрения обеспечения целостности данных, если не определен транзит этих данных с использованием связных протоколов промышленного качества.

Примечание — Целостность передаваемых данных традиционно является главной целью обеспечения безопасности при эксплуатации информационных систем. Предполагается, что уверенность в том, что данные ICS переданы и приняты неизмененными между конечными точками сессии, обеспечивается промышленными связными протоколами.

7.2.2 Политика безопасности ICS не является всеобъемлющей политикой безопасности.

Это обосновано тем, что настоящий стандарт учитывает только логическую безопасность ICS. Он не содержит всех положений, обычно входящих в политику безопасности организации.

Примечание — В настоящем стандарте устанавливают меры физической безопасности только в случае, если они тесно связаны с мерами логической безопасности. Другие меры, такие как безопасность персонала, в настоящем стандарте не рассматриваются.

Правила реализации политики приведены в 7.2.2.1 и 7.2.2.2.

7.2.2.1 Всеобъемлющая политика безопасности должна быть политикой безопасности организации и включать, например, положения, касающиеся безопасности персонала, общей физической и информационной безопасности.

7.2.2.2 Для дополнения политики безопасности ICS и придания ей законченности необходимо использовать общеотраслевые или специализированные стандарты, если политика безопасности организации утрачена или недостаточна.

Дополнительная информация — по ИСО/МЭК 27002.

7.2.3 Политика безопасности ICS не распространяется на закупки.

Это обосновано тем, что закупки и, в зависимости от рисков, связанные с ними обеспечение безопасности и относящееся к ним тестирование должны рассматриваться как штатные требования, однако они не рассматриваются в настоящем стандарте.

В данной политике предусмотрены предварительные условия и ограничения, заключающиеся в том, что ICS предполагает существование соответствующей политики для закупок, тестирования оборудования и связанных с этим функций безопасности, только в той части, в какой это требуется для реализации политики ICS.

Правила реализации политики приведены в 7.2.3.1.

7.2.3.1 Требования к закупкам должны быть адаптированы, исходя из положений и мер, предусмотренных настоящим стандартом.

Дополнительная информация — по [16].

Примечание — В настоящее время нет единой точки зрения или установившейся практики по дальнейшим рекомендациям обеспечения безопасности и тестирования безопасности соответствующего оборудования и устройств ICS.

7.2.4 Политика безопасности ICS не обеспечивает всестороннего оперативного управления безопасностью.

Это обосновано тем, что для гарантии того, что политика ICS и меры имеют ожидаемый эффект на протяжении всего эксплуатационного цикла завода, необходима интеграция политики ICS в общую систему управления информационной безопасностью ISMS-системы.

В данной политике предусмотрены предварительные условия и ограничения, заключающиеся в том, что должна быть реализована всеобъемлющая система ISMS. Она должна включать управление безопасностью персонала, общей безопасностью завода, процессами и процедурами администрирования и обеспечения работоспособности, управление работой при авариях и в условиях восстановления после стихийных бедствий. Должно быть обеспечено соответствующее обучение (теоретические и практические занятия). Система ISMS должна включать организационную структуру, политики, операции планирования, разграничение ответственности, практические методы, процедуры, процессы и ресурсы.

Дополнительная информация — по ИСО/МЭК 27002.

7.2.5 Политика безопасности ICS не распространяется на эксплуатационную безопасность связи, которую должна гарантировать штатная политика, обеспечивающая, например, безопасность функционирования.

Это обосновано тем, что в случае, когда штатная политика определяет эксплуатационную безопасность, и/или в случае, когда используются общепринятые практические способы, например GAMP [16], такая политика, практические способы и меры имеют приоритет над политикой безопасности, рассматриваемой в настоящем стандарте.

В данной политике предусмотрены предварительные условия и ограничения, заключающиеся в том, что штатная политика управления, например управления эксплуатационной безопасностью, должна учитывать риски управления функционированием и безопасностью, связанные с использованием любых каналов связи ICS, в том числе каналов ICN.

Правила реализации политики приведены в 7.2.5.1—7.2.5.3.

7.2.5.1 Доступность и целостность любого канала, используемого для безопасной связи внутри завода, а также между ICS и любым удаленным центром управления, должна контролироваться администрацией, осуществляющей управление рисками безопасности.

Примечание — Недостаточно надежная доступность любого или всех центров управления означает, что каналы ICN не являются надежными для безопасной связи при функционировании в критических условиях.

7.2.5.2 Отказ в обслуживании, обусловленный, например, внешним каналом связи, является видом инцидента, который не может быть учтен непосредственно. Эффект от его влияния снижается при использовании резервирования или резервного копирования ресурсов.

Примечание — Меры по резервированию для достижения доступности в типичном случае приводят к увеличению незащищенности данных и к повышению связанных с этим рисков.

7.2.5.3 С точки зрения эксплуатационной безопасности и других штатных политик обеспечения надежности эксплуатации, ICN и ее подсети можно рассматривать как «черные каналы», позволяющие избежать затрат времени и денежных средств на сертификацию основных каналов ICS в соответствии с требованиями их политики и обеспечения надежного управления их безопасностью.

7.2.6 Политика безопасности ICS не распространяется на доступность сети ICN и ее подсетей, а также на реагирование в реальном времени для любых каналов EN.

Это обосновано тем, что реагирование в реальном времени является проблемой, связанной с функционированием. В связи с тем, что механизмы безопасности политики ICS могут обуславливать дополнительные задержки, связь в реальном времени не гарантируется.

Примечание — Это означает, что эксплуатация ICS в реальном времени не может базироваться на EN, ICN или подсетях ICN. В частности, центры удаленного управления могут реагировать неудовлетворительно.

Правила реализации политики приведены в 7.2.6.1.

7.2.6.1 Критичная связь реального времени должна быть ограничена сегментами ICN самого низкого уровня, которые должны иметь хорошо защищенную границу. В этих сегментах не должны виртуально присутствовать механизмы логической безопасности (требуемые внутри сети).

Пример — Ячейка автоматизации AC (automation cell) в типичном случае будет защищена на своей границе шлюзом SGW с требуемой защитой. Физический доступ будет разрешен только уполномоченному персоналу. Вся связь внутри ячейки считается надежной.

7.2.7 Политика безопасности ICS не распространяется на эксплуатацию завода в опасных условиях.

Это обосновано тем, что эксплуатация в опасных условиях является проблемой эксплуатации. Механизмы безопасности могут оказаться недоступны, поэтому они не могут гарантировать надежную связь.

Примечание — Это означает, что эксплуатация ICS в опасных условиях не может базироваться на EN, ICN или подсетях ICN. В частности, может оказаться невозможным использовать центры удаленного управления.

Пример — С точки зрения безопасности может быть неприемлема автономная работа ячейки автоматизации AC в опасных условиях, так как в типичном случае она не имеет внутренних механизмов безопасности.

7.3 Политика безопасности промышленной системы управления — организация и управление

Процедуры и методы управления, необходимые для эксплуатации и аудита политики безопасности.

7.3.1 Ответственность за разработку, реализацию, соблюдение, проверку и изменение политики безопасности ICS несет администрация ICS.

Это обосновано тем, что изменения в угрозах, уровнях угроз, конфигурации, технологии и т. д. являются неизбежными и требуют переоценки и совершенствования политики ICS.

Правила реализации политики приведены в 7.3.1.1—7.3.1.7.

7.3.1.1 Оперативная ответственность за соблюдение политики безопасности ICS должна быть возложена на менеджера по безопасности, который должен быть оперативно независим от ICS и эксплуатации завода.

Примечание 1 — Разделение ответственности за реализацию усиления безопасности и поддержание политики безопасности иногда рекомендуется регуляторами. Это снижает риски безопасности.

Примечание 2 — В крупных организациях менеджер по безопасности может быть независимым, для этого он освобождается от ответственности и обязанностей по оперативному управлению или администрированию системы. В небольших организациях может оказаться, что отдельные сотрудники будут совмещать эти должности.

7.3.1.2 Управление администрированием сетевого оборудования, его реализация и протоколирование должны осуществляться безопасным образом.

Примечание 1 — Конфигурирование сетевого оборудования и изменения в конфигурации весьма желательны с точки зрения безопасности. Необходимо использовать действенные механизмы управления доступом.

Примечание 2 — Во избежание атак, нацеленных на настройки сети, администрация должна использовать каналы связи и привилегии доступа, которые отделены от производственного трафика и привилегий. Допускается использование отдельной безопасной сети управления.

Примечание 3 — Администрирование безопасности и сетевого оборудования должно быть выполнимо даже в случае атаки или при реагировании на атаку. Должны иметься также каналы для передачи производственного трафика.

7.3.1.3 Политика безопасности ICS должна документироваться, должны обновляться изменения и исключения, поддерживаться доступность и доведены до соответствующего персонала.

7.3.1.4 Все применяемые в организации политики должны быть доступны администрации ICS, в том числе и политика безопасности ICS, и должны регулярно выполняться обновления политик, обеспечивающие их эффективное применение за ограниченное время.

7.3.1.5 Для неукоснительного соблюдения положений политики ICS и ее изменений должны регулярно проводиться ознакомительные тренинги.

7.3.1.6 Управление должно включать документирование исключений с указанием конкретной причины, связанной с бизнесом, а также документирование времени установления исключения, его продолжительности и срока окончания.

7.3.1.7 Должны проводиться проверки политики как периодические, так и после инцидентов.

7.3.2 Управление рисками угроз

Проблемы безопасности в значительной степени обусловлены неопределенностью, связанной с технологическим прогрессом и непредсказуемостью человека, в результате чего существует постоянно меняющийся риск для имущественных объектов. Имущественные объекты владельца или оператора в целом остаются примерно постоянными. Это делает среду угрозы основным фактором.

В данной политике предусмотрены предварительные условия и ограничения, заключающиеся в том, что в настоящем стандарте не рассматривается метод TRA. Поэтому владелец/оператор должен самостоятельно разработать метод оценки рисков, используя другие ресурсы (кроме настоящего стандарта).

Правила реализации политики приведены в 7.3.2.1—7.3.2.4.

7.3.2.1 Критичные компоненты оборудования, операционные системы, приложения и службы, используемые для эксплуатации, управления и обеспечения работоспособности системы автоматизации, должны быть оценены с точки зрения функциональной доступности, целостности системы и конфиденциальности данных.

7.3.2.2 Среда угрозы должна непрерывно контролироваться и оцениваться.

7.3.2.3 Периодически или после наступления событий безопасности должна проверяться и корректироваться мощность мер безопасности, принимаемых против угроз, таким образом, чтобы она всегда находилась на должном уровне.

Примечание 1 — Методы криптографии должны периодически корректироваться в целях соответствия развитию технологий.

Примечание 2 — Изменения, например в правилах SGW и ECG, учитывающие виды и уровни угроз, должны приводить к изменению конфигураций, технологий, добавлению дополнительных мер и оборудования и т. д.

7.3.2.4 Критичное оборудование должно быть закреплено за техником и администратором и контролироваться оборудованием мониторинга.

7.3.3 Политика эксплуатационной безопасности ICS и ее изменения должны быть скоординированы с политикой безопасности ICS.

Это обосновано тем, что эксплуатационная безопасность и безопасность (подразумевающая обеспечение конфиденциальности) тесно связаны друг с другом.

Правила реализации политики приведены в 7.3.3.1—7.3.3.4.

7.3.3.1 Политика эксплуатационной безопасности ICS и ее обновления должны храниться в файле, постоянно доступном администрации службы безопасности.

7.3.3.2 Любые меры и методы, применяемые оператором в целях безопасности, влияющие на эксплуатационную безопасность, должны быть утверждены как администрацией службы безопасности, так и администрацией, отвечающей за эксплуатационную безопасность.

Примечание — Правило «двойной ответственности» гарантирует, что меры, которые могут привести к катастрофическим последствиям, не будут инициированы единолично. Это предохраняет от намеренной или случайной неправильной эксплуатации. Двойная ответственность является наиболее действенным средством борьбы с атаками инсайдеров.

7.3.3.3 Если предусмотрено использование оператором меры или способа, влияющих на безопасность функционирования, то требуется утверждение введения их в эксплуатацию и прекращения применения.

7.3.3.4 Не должно быть исключений, которые удаляют исключения, утвержденные двумя ответственными.

7.3.4 Политика безопасности ICS должна требовать протоколирования и мониторинга соответствующих событий безопасности.

Это обосновано тем, что протоколы используются для установления событий, последовательностей и возложения ответственности за управление и аудит. В отношении несанкционированных действий, например атаки, протоколы могут использоваться для формальных выводов. Возложение ответственности особенно важно в случаях, когда критичные операции выполняются сторонней компанией.

Правила реализации политики приведены в 7.3.4.1—7.3.4.8.

7.3.4.1 Все действия пользователя системы автоматизации, существенные для безопасности, должны быть запротоколированы.

7.3.4.2 Все события системы, существенные для безопасности, должны быть запротоколированы.

7.3.4.3 Собранная информация должна включать в себя событие, срочность, службу связи, хост источника, назначение, идентификатор пользователя, дату/время начала и окончания.

7.3.4.4 Все протоколы и информация аудита должны непрерывно контролироваться, периодически проверяться, надежно храниться и архивироваться.

7.3.4.5 Протоколы должны храниться централизованно для их последующего объединения и анализа. Должно быть исключено исчерпание ограниченного пространства памяти, используемого для хранения протоколов. Также должно быть исключено изменение атакующим протоколов в результате его несанкционированного доступа к оборудованию протоколирования.

7.3.4.6 Действия по управлению протоколами также должны протоколироваться. Только аудитор службы безопасности должен иметь право удалять или изменять протоколы.

7.3.4.7 Протоколы и сообщения аварийной сигнализации должны непрерывно контролироваться. По результатам контроля должны составляться заключения и применяться необходимые меры.

Это обосновано тем, что протоколы событий безопасности необходимо непрерывно контролировать для выявления вредоносных атак инсайдеров и сохранять их для последующего формального анализа после того, как безопасность будет нарушена.

Примечание — Если безопасность нарушена, сетевое соединение между удаленным и локальным центром управления должно быть прервано до восстановления надежности соединения. Локальный центр управления должен осуществлять безопасную эксплуатацию ICS. Для подтверждения восстановления надежности соединения должен быть выполнен аудит безопасности.

7.3.4.8 Если протоколы предполагается использовать в качестве доказательств в суде, должны быть выполнены требования действующего местного законодательства.

Пример — Могут протоколироваться следующие данные:
- событие, например ошибка аутентификации, нарушение доступа;
- срочность, например авария, сигнал тревоги, предупреждение;
- используемая служба связи, например имя службы, номер порта, протокол;
- хост источника, например IP-адрес, имя хоста;
- назначение, например IP-адрес, имя хоста, URL;
- идентификатор пользователя;
- дата и время начала;
- дата и время окончания.

Примечание — Если эксплуатацию ICS осуществляет сторонняя компания, протокол является важным объективным доказательством для возложения ответственности после аварии.

7.3.5 Должен проводиться аудит соответствия политики безопасности ICS.

Это обосновано тем, что для контроля характеристик управления политикой ICS необходим аудит.

Правила реализации политики приведены в 7.3.5.1—7.3.5.5.

7.3.5.1 Аудит соответствия политики ICS должен выполняться периодически и, если необходимо, приводить к принятию обоснованных корректирующих мер.

7.3.5.2 Аудиты могут включать тестирование безопасности.

Примечание — Аудит ICS должен периодически проводиться для выявления неразрешенного и ненадежного оборудования связи, например использования POTS (телефонных сетей общего пользования) или беспроводной связи.

7.3.5.3 Ответственность за аудит безопасности предпочтительно возложить на квалифицированного менеджера по безопасности, не участвующего в эксплуатации, возможно, на стороннего специалиста.

7.3.5.4 Если возможно, следует разделить должности аудитора и администратора, отвечающих за меры безопасности.

7.3.5.5 Особое внимание должно уделяться формальным исключениям из установленных мер. Для них должен проводиться специальный аудит.

7.3.6 Должно осуществляться управление исключениями и их документирование для обеспечения необходимой отчетности по сотрудникам и устройствам с использованием управления рисками ad hoc (для данной конкретной цели — лат.).

Это обосновано тем, что без управления формальными исключениями по типу ad hoc произойдет потеря координации управления исключениями, их длительностью и пределами, а также потеря отчетности и личной ответственности за любые негативные последствия.

В данной политике предусмотрены предварительные условия и ограничения, заключающиеся в том, что при совместной ответственности, возникшей, например, из-за использования пользователями общих учетных записей, источник конкретных действий в системе не может быть идентифицирован, при этом подозреваемый пользователь может правдоподобно отрицать свою причастность к действию.

Закрепление ответственности может противоречить местному трудовому законодательству, в связи с чем может потребоваться заключение объединенных соглашений с исполнительной администрацией более высокого уровня.

Правила реализации политики приведены в 7.3.6.1—7.3.6.3.

7.3.6.1 Должно осуществляться управление формальными исключениями из политики, включающее в себя обоснование их со стороны бизнеса, анализ рисков, возложение ответственности на определенное лицо.

7.3.6.2 Исключения из политики должны быть сведены к минимуму и действовать минимально необходимое время.

7.3.6.3 Не должно быть исключений, исключающих управление.

7.3.7 События и сообщения аварийной сигнализации должны своевременно актироваться в соответствии с планами действий в непредвиденных ситуациях, и должен выполняться их критический анализ.

Это обосновано тем, что при наступлении инцидента безопасности очень важно свести ущерб к минимуму и продолжать эксплуатацию ICS, как можно быстрее полностью восстановив надежную эксплуатацию с обычной производительностью.

Правила реализации политик приведены в 7.3.7.1—7.3.7.10.

7.3.7.1 Должны быть установлены планы действий в непредвиденных ситуациях. Они должны периодически обновляться.

7.3.7.2 Сообщения аварийной сигнализации, имеющие отношение к безопасности в критических условиях, и события производственного управления должны актироваться администрацией службы безопасности и, если возможно, совместно с администрацией, отвечающей за эксплуатационную безопасность.

7.3.7.3 Для инцидентов различного рода и критичности, связанных с безопасностью, должны быть установлены планы реагирования на инцидент, включающие продолжение эксплуатации завода и восстановление поврежденного оборудования.

7.3.7.4 Для быстрого и эффективного разрешения проблемы для критичного оборудования должно документироваться его закрепление за техником, пользователем, администратором и оборудованием мониторинга.

7.3.7.5 Критичный инцидент безопасности должен быть исследован быстро и сразу после его возникновения.

Примечание 1 — В некоторых старых приложениях для доступа к устройствам ICS или удаленным клиентам используется протокол с открытым текстом сертификата (например, Telnet, FTP). В этом случае доступ должен использовать надежный протокол туннеллирования во избежание раскрытия сертификатов на любой части маршрута, раскрываемой общедоступными внешними сетями EN.

Примечание 2 — Должно осуществляться управление исключениями и их документирование.

Примечание 3 — Когда устройство безопасности выдает сообщение аварийной сигнализации, извещающее об инциденте безопасности, оно должно без задержки поступать на сервер управления безопасностью менеджеру по безопасности. Менеджер по безопасности должен задействовать план противодействия ущербу, то есть определить уровень поражения и очевидные меры безопасности, которые необходимо принять.

7.3.7.6 Планы должны быть опубликованы и доведены до сведения соответствующего персонала одновременно с распределением ответственности и связанных с нею имущественных объектов организации.

7.3.7.7 Должны проводиться ознакомительные занятия и технические тренинги, поддерживающие персонал в форме, необходимой для действий в непредвиденной ситуации.

7.3.7.8 Периодически и внезапно должны проводиться практические занятия по отработке действий при разнообразных сценариях атак, позволяющие оценить способность завода справляться с реальными атаками должным образом.

7.3.7.9 При обнаружении несанкционированного проникновения реагировать необходимо немедленно. Это предполагает существование адекватных и обновляемых планов для инцидентов безопасности, влияющих на функции и имущественные объекты, на которые распространяются эти политики.

7.3.7.10 Вызванные инцидентами безопасности катастрофы требуют планов восстановления после катастроф и аварий, а также соответствующей контактной информации и информации по восстановлению.

Примечание — Об использовании и мониторинге системы доступа см. ИСО/МЭК 27002.

8 Политика безопасности промышленной системы управления — меры

Цель указанной политики — снизить риск электронных атак на ICS путем установления мер безопасности для хостов, устройств, а также мер по ограничению способности периферийных устройств подключаться к внутренней сети ICN, к подчиненным ICN сетям любого уровня и к внешним сетям.

Примечание — Намеченное снижение риска может быть достигнуто только в том случае, если учитываются все способы связи, включая традиционные средства связи (телефон, радиосвязь), беспроводные частные и общедоступные сети.

8.1 Управление доступностью

Повреждение ресурсов PCS, обусловленное мерами безопасности, может приводить к простоям и даже подвергать опасности людей и окружающую среду, если приняты жесткие меры эксплуатационной безопасности.

Для предотвращения повреждения ресурсов, требуемых для производственного процесса, вследствие принятия мер безопасности, должно использоваться управление доступностью.

8.1.1 Доступность ICN и подсетей ICN должна быть гарантирована для требований эксплуатации ICS в критических условиях.

Это обосновано тем, что недостаточные или чрезмерные меры безопасности могут ухудшить доступность ICN и препятствовать удовлетворительной эксплуатации ICS.

В данной политике предусмотрены предварительные условия и ограничения, заключающиеся в том, что доступность в ICN внутренних сообщений реального времени не является требованием безопасности, но представляет собой проблему функционирования. В настоящем стандарте предполагается, что доступность сообщений реального времени гарантирована функциями автоматизации, использующими такие меры, как обеспечение целостности сообщений, актуальности сообщений, упорядочения сообщений, приоритетов сообщений.

Правила реализации политики приведены в 8.1.1.1 и 8.1.1.2.

8.1.1.1 Для повышения доступности и предотвращения отказов в одной точке может потребоваться резервирование каналов связи.

Примечание 1 — Несмотря на то что резервирование в целом увеличивает надежность и доступность, оно также увеличивает незащищенность данных и риски безопасности, так что безопасность при использовании резервирования снижается.

Примечание 2 — При частичной недоступности связи может потребоваться резервное копирование ресурсов, уменьшение числа рабочих режимов завода и, в наихудшем случае, прекращение работы завода.

8.1.1.2 Для предотвращения последствий потери доступности пользователям и приложениям данной сети должно быть предоставлено право запрашивать состояние оборудования защиты, например шлюзов SGW, и подавать сигналы тревоги при обнаружении условий, характерных для сбоя.

8.1.2 Ресурсы, используемые мерами безопасности, не должны ухудшать критичных ресурсов, требующихся функциям автоматизации и/или эксплуатационной безопасности.

Это обосновано тем, что меры безопасности должны функционировать таким образом, чтобы не нарушался производственный процесс.

Правила реализации политики приведены в 8.1.2.1 и 8.1.2.6.

8.1.2.1 На оборудовании, связанном с безопасностью, должны быть реализованы только такие функции безопасности, которые требуются для надежной работы этого оборудования.

Примечание — Доступность любых ресурсов, связанных с эксплуатационной безопасностью, не должна ограничиваться, в том числе за счет разрешения использования:

- специальных собственных средств связи;
- существующих собственных механизмов эксплуатационной безопасности;
- соответствующего облегчения физического и логического доступа к работе контрольных комнат, обеспечивающих эксплуатационную безопасность.

8.1.2.2 Необходимо избегать конкуренции функций безопасности и управления за ресурсы ICN и разрешать такие проблемы, например, путем выделения для соответствующих функций отдельного оборудования.

Примечание — Разделение может оказаться невозможным, например, если установлен сканер вирусов и вредоносного программного обеспечения. В этих случаях необходимо удостовериться в том, что любой реализованный на промышленном оборудовании управления функционал безопасности поддерживается отделенным логически, то есть использует отдельные сертификаты, обработчики прерываний и скоординирован с персоналом, осуществляющим управление производственным процессом.

8.1.2.3 Необходимо определять меры безопасности, которые могут использовать критичные ресурсы функций управления. Также необходимо осуществлять управление такими функциями безопасности и документировать их.

8.1.2.4 Для этих мер необходимо определить, реализовать и документировать границы ресурсов и режим работы хостов в случае, когда ресурсы перегружены или переполнены. Должна быть предусмотрена подача сигнала тревоги.

8.1.2.5 В случае конфликта приоритет должен иметь функционал управления критичным промышленным оборудованием.

8.1.2.6 Должен быть реализован план реагирования при исчерпании ресурсов. С персоналом должны проводиться ознакомительные и практические занятия. Также должно осуществляться управление планами и их документирование.

Примечание 1 — План реагирования на аварии должен включать в себя анализ рисков, реализацию соответствующей эксплуатации в ухудшенных условиях и/или режимы прекращения работы, режимы уменьшенного протоколирования, подачу сигналов тревоги уполномоченным пользователем и оборудованием мониторинга.

Примечание 2 — Различное влияние действий в аварийных условиях и их последствий на безопасность, на критичные средства автоматизации и функционал эксплуатационной безопасности может быть выявлено путем активации/деактивации сегментов.

8.1.3 Для гарантирования функциональной доступности ICN должны быть реализованы меры безопасности с прозрачным управлением.

Это обосновано тем, что реализация, обновление и удаление услуг безопасности не должны оказывать влияния на функциональные свойства ICS.

Примечание — Это означает, что может использоваться конфигурация ICS, любых EN и удаленных клиентов и после встраивания функций безопасности конфигурация не изменяется.

Правила реализации политики приведены в 8.1.3.1.

8.1.3.1 Если установка, изменение или удаление привели к ожидаемым изменениям в эксплуатации, это должно быть скоординировано с администрацией ICS и/или администрацией, отвечающей за безопасность.

8.1.4 Часы всех устройств ICS должны быть синхронизированы.

Это обосновано тем, что требуется доступность точной временной синхронизации устройств от достаточно надежного источника времени, например, для гарантирования последовательной регистрации событий в протоколах для их последующего объединения и анализа.

Правила реализации политики приведены в 8.1.4.1—8.1.4.2.

8.1.4.1 Установка стандартного времени и требуемой точности.

8.1.4.2 Использование данных времени из одного источника. Если нет подходящей карты часовых поясов, используется источник времени, по которому выполняются функции безопасности и управления.

Примечание — Подразумевается синхронизация часов удаленного клиента и устройства.

8.2 Управление целостностью

Базис системы должен быть уменьшен до минимального кода, данных конфигурации, эксплуатационных данных. Они должны быть минимально необходимыми для функционала ICS и безопасности с тем, чтобы поверхность, защищаемая от атаки по раскрытию данных, была минимальной.

Примечание — Предполагается, что целостность переданных данных (то есть что данные ICS переданы и приняты неизмененными между конечными точками сессии) обеспечивается промышленными связными протоколами.

8.2.1 Конфигурации аппаратных устройств и интерфейсов должны быть уменьшены до минимально необходимых (усиление защищенности).

Это обосновано тем, что обычные или незащищенные конфигурации аппаратных средств содержат неиспользуемые интерфейсы и периферийные устройства, которые увеличивают поверхность атаки, в частности, для инсайдеров.

Правила реализации политики приведены в 8.2.1.1 и 8.2.1.2.

8.2.1.1 Неиспользуемые оператором интерфейсы ввода-вывода, периферийные устройства, устройства связи и хранения данных должны быть удалены или иным способом сделаны постоянно неработоспособными.

8.2.1.2 Шкафы и слоты, доступные снаружи, которые не могут быть удалены, должны быть защищены, то есть заперты.

8.2.2 Необходимо уменьшить до минимально необходимого уровня число приложений, а также служб и утилит O/S (усиление защиты).

Это обосновано тем, что риск того, что атакующий окажется способным раскрыть систему, возрастает с увеличением числа доступных приложений и служб на хостах и устройствах.

Правила реализации политики приведены в 8.2.2.1—8.2.2.4

8.2.2.1 Должны документироваться список и конфигурация приложений, служб и утилит O/S, требуемых для эксплуатации ICS.

Примечание — Наборы разрешенных средств связи могут зависеть от формального оперативного состояния завода или участка, например «нормальная эксплуатация», объявленная «эксплуатация в аварийных условиях» либо операции по вводу в эксплуатацию или выводу из эксплуатации.

8.2.2.2 Должны документироваться все параметры сетевых служб, требуемых на хостах, для входящих и исходящих потоков данных при обмене ими с другими хостами и устройствами ICN.

8.2.2.3 Приложения, службы и утилиты O/S, не требуемые для эксплуатации ICS, должны быть удалены из конфигураций и их резервных копий.

Примечание 1 — Службы приема непосредственного вещания должны быть удалены.

Примечание 2 — Если службы и утилиты O/S, не требуемые для эксплуатации ICS, не могут быть удалены, они должны быть выполнены постоянно недоступными любым пользователям.

Примечание 3 — Шлюз SGW на базе хоста (также называемый персональный SGW) делает неработоспособной или блокирует связь, предназначенную для некоторых служб, но не удаляет код.

8.2.2.4 Требуемые приложения, службы и утилиты ОС, службы безопасности должны быть на поверхности с усиленной защитой от атак до того, как они будут подключены к ICN.

Примечание — Имеются наилучшие практические способы усиления защиты для различных операционных систем (см., например, представленные в NIST, NSA, SANS, CISecurity).

8.2.3 Должны корректно поддерживаться уникальность и подлинность созданных конфигураций.

Это обосновано тем, что полностью идентичные конфигурации хостов будут увеличивать поверхность атаки и возможности раскрытия, например при автоматизированных атаках, приводящих к раскрытию всех идентичных систем.

В данной политике предусмотрены предварительные условия и ограничения, заключающиеся в том, что различие в конфигурациях усилит защиту за счет неизвестности. Это усиление может быть достигнуто, например, за счет:

- дополнительных затрат, например на администрирование и управление пакетами коррекции, делающими оборудование различающимся;

- уменьшения потерь в безопасности, обусловленных ошибками операторов и администраторов из-за сложности конфигурирования.

Может оказаться невозможным изменить настройки, введенные, например, изготовителями на старом оборудовании.

Правила реализации политики приведены в 8.2.3.1—8.2.3.3.

8.2.3.1 Системы, сконфигурированные изготовителем либо клонированные владельцем/оператором или системным интегратором, должны быть изменены. При этом необходимо изменить настройки, заданные по умолчанию или обычно используемые, и сделать их уникальными.

8.2.3.2 Изменение настроек должно быть документировано. Настройки должны быть прозрачны для пользователя и защищены от изменения.

8.2.3.3 Уникальные настройки, созданные владельцем/оператором, могут быть восстановлены после установки пакетов исправления.

Примечание — Пакеты исправлений могут восстановить заданные до этого настройки, выбираемые по умолчанию.

8.2.4 Должно осуществляться управление установкой системы и устройств, например установкой конфигураций, процессов запуска, поддержания работоспособности и оперативной целостности.

Это обосновано тем, что компоненты системы и их связи должны соответствовать желаемому состоянию надежности. С этой целью настройки системы должны управляться и обновляться так часто, насколько это необходимо с точки зрения безопасности.

В данной политике предусмотрены предварительные условия и ограничения, заключающиеся в том, что в целом пакеты исправлений и обновления не должны устанавливаться сразу после их появления. Однако обновление или пакет исправлений безопасности может конфликтовать с функционалом системы управления, приводя в результате к ухудшению или недоступности функционала, либо может ухудшиться режим работы по времени.

Может быть верным и обратное: пакет исправления системы управления может конфликтовать с мерами безопасности, что приводит к ухудшению или недоступности функционала безопасности.

Очевидно, что изготовитель системы автоматизации не способен протестировать обновление или пакет исправлений на каждом возможном варианте системы, в частности на конкретной реализации ICS.

Правила реализации политики приведены в 8.2.4.1—8.2.4.6.

8.2.4.1 Должны быть разработаны, документированы и поддерживаться в работоспособном состоянии текущие базовые конфигурации.

8.2.4.2 Реестр компонентов системы и оперативное состояние должны сохраняться, а также должны создаваться их резервные копии и архивы, и их целостность должна быть защищена.

8.2.4.3 Обновления и пакеты исправлений безопасности должны рассматриваться только после утверждения их изготовителем соответствующего устройства или системы.

8.2.4.4 Утвержденные изготовителем обновления и пакеты исправлений безопасности должны устанавливаться только после дополнительного тестирования на ICS.

Примечание — Если возможно, при тестировании на заводе должны выполняться: разработка систем, резервное копирование и тренинги.

8.2.4.5 Перед установкой на ICS новые приложения, службы и пакеты исправлений должны быть подписаны.

8.2.4.6 Риски частичного отказа системы или отклонений от нормального функционирования, действующие во время установки системы и после ее установки, должны быть оценены и уменьшены, например, за счет развертывания обновлений.

Примечание 1 — Должен существовать процесс разрешения возникающих проблем, включающий откат к последнему надежному и функционально корректному состоянию.

Примечание 2 — Чтобы сохранить некоторые функции управления при возникновении проблем с модификацией программного обеспечения, допускается рассмотреть вариант поэтапного развертывания.

8.2.5 Должно осуществляться управление исполняемыми образами, основной и резервной копией O/S, информацией о состоянии и производственной информацией.

Это обосновано тем, что соответствующая целостность исполняемого образа и резервной копии гарантирует, что вся важная информация и программное обеспечение могут быть восстановлены после инцидента или отказа для быстрого возобновления работы, обеспечения целостности и доступности систем и данных.

Правила реализации политики приведены в 8.2.5.1—8.2.5.4.

8.2.5.1 Должны регулярно выполняться резервное копирование и надежная архивация, резервные копии должны тестироваться и выполняться подтверждение их подлинности.

8.2.5.2 Резервная копия должна содержать в себе все параметры функционала безопасности, производственного функционала и оперативно требуемые параметры функционала для быстрого восстановления.

8.2.5.3 Должны быть установлены и доступны утилиты, проверяющие целостность файловой системы O/S, позволяющие обнаружить изменения. Должны быть доступны процедуры и инструменты для точного восстановления в требуемое состояние.

8.2.5.4 Должны предотвращаться неразрешенные изменения конфигурации, например, с помощью вредоносного программного обеспечения или заражения вирусами. Если это все же произошло, должен быть выдан сигнал тревоги, и после соответствующего реагирования должны быть приняты меры по исправлению ситуации.

Примечание 1 — Ресурсы ICS могут сильно перегружаться при сканировании. См. управление доступностью ресурсов в настоящем стандарте.

Примечание 2 — Сканеры вредоносного программного обеспечения и вирусов, использующие подписи, эффективны только для текущих подписей.

Примечание 3 — Сканеры должны быть развернуты и сконфигурированы только таким образом, как указано изготовителем системы автоматизации, и сканировать только обозначенное оборудование.

Примечание 4 — Сканеры и подписи для хостов и устройств COTS, не являющихся критичными, могут быть установлены владельцем/оператором на свой риск, при этом следует обеспечить, чтобы сканирование не нарушало критичных границ, например, сетевых устройств.

Примечание 5 — Подписи COTS могут ложно идентифицировать некоторые легальные файлы специальных приложений как вредоносное программное обеспечение. Поэтому подписи должны быть тестированы до применения к конкретной системе автоматизации или должно быть получено одобрение у изготовителя соответствующей системы автоматизации.

8.2.6 Управление целостностью должно включать мониторинг, протоколирование, процедуры эскалации аварий.

Это обосновано тем, что без мониторинга целостности и аварий владелец/оператор не сможет доказать, что целостность была обеспечена. Протоколирование также необходимо для обнаружения отклонений от нормы и судебного разбирательства.

8.2.6.1 Должен осуществляться централизованный мониторинг всех шлюзов SGW.

Примечание — См. протоколирование в 7.3.4.2.

8.3 Управление логическим доступом

Гарантируется только санкционированный логический доступ к ресурсам ICS в соответствии с присвоенными привилегиями.

8.3.1 Должны быть присвоены особенности, устанавливающие подлинность, адреса, ключи, соответствующие сертификаты пользователей и устройств, а также права/привилегии. Также должно осуществляться управление всем перечисленным.

Это обосновано тем, что проверка подлинности пользователей и устройств в точках окончания сессии связи сделает невозможным несанкционированный доступ и отказ от факта получения или отправления сообщения. Для безопасности ICS важно ограничить привилегии каждого пользователя до минимально необходимых для эксплуатации и поддержания работоспособности ICS.

В данной политике предусмотрены предварительные условия и ограничения, заключающиеся в том, что открытый логический доступ может быть необходим, например, для эксплуатации, выполняемой из контрольной комнаты, из которой осуществляется управление безопасностью функционирования. Это исключение должно контролироваться за счет физического ограничения доступа в контрольную комнату.

Правила реализации политики приведены в 8.3.1.1—8.3.1.9.

8.3.1.1 Должны быть удалены сертификаты, заданные по умолчанию на заводе-изготовителе.

8.3.1.2 Пользователям и устройствам должны быть присвоены минимально необходимые привилегии и только такие, которые требуются для эксплуатации в соответствии с их ролями при эксплуатации.

Примечание 1 — Учетные записи, назначенные по умолчанию, и устаревшие сертификаты исторически были одними из самых больших угроз безопасности. В настоящем стандарте принято предположение, что они были изменены при установке системы операцией контроля целостности системы, см. раздел 8.2.3.1.

Примечание 2 — Принцип наименьших привилегий — это принцип обеспечения безопасности, гарантирующий, что каждая система использует минимальные ресурсы и только те авторизации, которые требуются для ее работы.

Примечание 3 — Управление доступом на основе ролей — это хорошо отработанная схема управления и рационализации прав доступа для больших групп пользователей или устройств с изменяющимися требованиями доступа и может включать их присутствие на физической площадке в соответствующий период времени.

Примечание 4 — Разделение пользователей по различным, совместно управляемым ролям уменьшает вероятность атак инсайдеров.

8.3.1.3 Когда персонал оставляет свои роли или они меняются, должны обновляться учетные записи и привилегии управления доступом.

Примечание — Изменения должны вноситься быстро, сразу после того как произошли соответствующие события, то есть после прекращения обязанностей, изменений в закреплениях и настройках устройств.

8.3.1.4 Для аутентификации должны использоваться сложные сертификаты.

Примечание — Должны контролироваться длина и характеристики паролей, они должны быть достаточно сложными, чтобы предотвратить их обход, например, с помощью догадок и рассуждений или взлома. Если они признаны простыми, необходимо добавить дополнительные факторы, например использование аппаратных ключей, биометрии, ограничение физического доступа к пульту аутентификации.

8.3.1.5 Для файлов, приложений, инструментов O/S, служб, устройств и сегментов должны быть установлены привилегии наиболее подходящего уровня.

Примечание 1 — Некоторые утилиты O/S позволяют значительно изменить состояние, настройку хоста и всей системы автоматизации. Большинству пользователей системы ICS, например операторам, может не требоваться доступ ко всем этим утилитам (или к их части).

Примечание 2 — Большинство каналов связи, идущих снаружи в сегмент и из сегмента наружу, и каналов связи между сегментами должны быть ассоциированы с правами доступа пользователей и устройств к этим сегментам.

Примечание 3 — Привилегии установки исполняемых файлов, например приложений, должны строго контролироваться.

8.3.1.6 Привилегии связи должны устанавливаться отдельно для источника и назначения — по устройствам, хостам и носителям.

Примечание 1 — Особое внимание следует уделять присвоению IP-адресов и управлению ими, например трансляции адресов, зависимостям сегментов от масок подсетей, службе каталогов, размещению соответствующих серверов, службе доменных имен (DNS), предотвращению использования трансляции сетевых адресов (NAT), используемых ICN.

Примечание 2 — Не допускается открытое закрепление, например закрепление и монтирование дисков, либо вещание во внешние сети или из них.

8.3.1.7 Привилегии на изменение настроек конфигурации операционных систем и аппаратных средств должны строго контролироваться.

8.3.1.8 Для привилегий на изменение настроек конфигурации, влияющих на безопасность и существенно влияющих на правильность функционирования ICS — для коммутаторов, маршрутизаторов, систем обнаружения вторжений IDS, шлюзов SGW и т. д., должна быть применена сильная защита управления доступом.

8.3.1.9 Должны быть установлены конкретные процедуры проверки привилегий управления доступом, гарантирующие, что привилегии и уровни, присвоенные каждому пользователю или устройству, употребляются и используются по назначению, обоснованно и соответствуют текущим требованиям.

8.3.2 В случае слабости мер управления доступом должны быть реализованы дополнительные меры защиты конфиденциальности и/или повышены требования к конфиденциальности.

Это обосновано тем, что защита доступа к устройствам и носителям, содержащим конфиденциальные данные, может оказаться недостаточной из-за требований повышения конфиденциальности данных, например при наличии ненадежных кабелей или для сертификатов пользователей. В этом случае может потребоваться шифрование.

Правила реализации политики приведены в 8.3.2.1 и 8.3.2.2.

8.3.2.1 В автономных внешних устройствах SED чувствительные производственные данные должны быть защищены отдельно от данных программ.

8.3.2.2 Необходимо изменять методы шифрования и проверять их, чтобы гарантировать разумно достаточную сопротивляемость к прямым атакам в течение ожидаемых периодов времени.

Примечание 1 — Сложное шифрование подразумевает периодическую смену ключей, управление ключами, а также периодическое физическое уничтожение ключей, носителей и данных.

Примечание 2 — Время между этими событиями должно быть сбалансированным, требования безопасности должны быть выполнимыми при нарушениях канала связи между сторонами.

8.3.3 При повышении требований по невозможности отказа от авторства сообщения дополнительно должны быть реализованы меры, делающие отказ от авторства сообщения невозможным.

Это обосновано тем, что гарантирование ответственности путем невозможности отказа от авторства сообщения является одной из наиболее важных мер против атак инсайдеров.

Примечание — Могут оказаться пригодными меры криптографии.

8.3.4 На выделенном оборудовании, в соответствии с закрепленными привилегиями, должны быть установлены и инициализированы привилегии аутентификации, обмен ключами, механизмы управления доступом. Должно осуществляться управление привилегиями аутентификации, обменом ключами и механизмами управления доступом.

Это обосновано тем, что для управления доступом требуется аутентификация.

В данной политике предусмотрены предварительные условия и ограничения, заключающиеся в том, что при аварии должны быть предусмотрены возможности для принудительного обхода отказавшей аутентификации, например, из-за возможного технического отказа подсистемы управления аутентификацией и доступом или из-за отсутствия оператора.

Правила реализации политики приведены в 8.3.4.1 и 8.3.4.2.

8.3.4.1 Должно быть обеспечено эффективное администрирование привилегий с использованием инструментов и, по возможности, средств автоматизации, таких как серверы аутентификации и центры ключей.

Примечание — Серверы аутентификации и центры ключей содержат высокочувствительные данные и должны быть размещены внутри завода, контролируемого администрацией ICN. Они должны быть защищены логически и физически.

8.3.4.2 Должно быть определено действие системы при событии отказа аутентификации.

Примечание 1 — Могут быть заданы стандартные действия, например неограниченное число попыток, неограниченное число попыток с возрастающей задержкой, блокировка после заданного числа попыток, возможная генерация и эскалация сообщений аварийной сигнализации.

Примечание 2 — Может быть использована процедура передачи на хранение третьему лицу, гарантирующая невозможность ситуаций неконтролируемого пользовательского доступа или отказа от авторства.

8.3.5 Должны осуществляться мониторинг и протоколирование привилегий аутентификации, обмена ключами и механизмов управления доступом.

Это обосновано тем, что протоколы привязывают пользователей к устройствам и позволяют установить авторов произошедшего и их ответственность.

В данной политике предусмотрены предварительные условия и ограничения, заключающиеся в том, что некоторые законы, касающиеся конфиденциальности, могут потребовать уменьшения данных отчета или их анонимности.

Правила реализации политики приведены в 8.3.5.1.

8.3.5.1 Для пользователя (по крайней мере для пользователя, установившего сессию) должны быть запротоколированы время и все действия, касающиеся безопасности, которые были выполнены с данного пульта управления.

Примечание — Об использовании и мониторинге доступа в систему см. ИСО/МЭК 27002.

8.4 Управление физическим доступом

Управление физическим доступом гарантирует только санкционированный физический доступ к ресурсам ICS на площадке в соответствии с присвоенными привилегиями, в том числе санкционированный доступ к оборудованию и инструментам, носителям или к информации в целом.

8.4.1 Хосты, устройства, носители должны быть защищены от несанкционированного доступа, перемещения, разрушения и воровства. Защита должна удовлетворять соответствующим требованиям.

Это обосновано тем, что в дополнение к логической защите ICS должна обеспечивать физическую защиту путем механической блокировки, размещения хостов, устройств и носителей в запертых на замок шкафах для исключения их воровства, порчи, перемещения и несанкционированного доступа к ним.

Примечание — Оборудование, надежное в физическом смысле, включает в себя:
- комнаты, шкафы, кожухи коммутаторов, SGW, корпуса для персональных компьютеров (ПК);
- мобильное оборудование и носители, например ПК, портативные компьютеры;
- USB-порты, приводы дискет;
- автономные промышленные устройства управления;
- кабели.

8.4.2 Должно осуществляться управление особенностями (устанавливающими подлинность), адресами, ключами, соответствующими сертификатами пользователей и устройств, а также правами и привилегиями.

Это обосновано тем, что для безопасности ICS важно обеспечить закрепление за пользователем привилегий доступа к оборудованию эксплуатации и поддержания работоспособности ICS.

В данной политике предусмотрены предварительные условия и ограничения, заключающиеся в том, что менеджментом по персоналу должны контролироваться надежность и платежеспособность подчиненного ему персонала.

Правила реализации политики приведены в 8.4.2.1.

8.4.2.1 Привилегии доступа должны быть ассоциированы с доступом через ворота (на вход и выход) сегмента и, при необходимости, с другими сегментами.

8.4.3 Должны осуществляться мониторинг и протоколирование физического доступа в аппаратные комнаты, к шкафам и корпусам, также должны подаваться соответствующие сигналы тревоги.

Это обосновано тем, что верификация подлинности пользователей, допущенных в закрытые физические сегменты, будет снижать возможности несанкционированного доступа и отказа от содеянного. Протоколы связывают пользователя (или по крайней мере пользователя, который работал с механизмом управления доступом) с временем и обеспечивают установление авторства и ответственности.

В данной политике предусмотрены предварительные условия и ограничения, заключающиеся в том, что телевизионный мониторинг может быть запрещен соглашениями между работодателем и сотрудниками либо местным законодательством.

Правила реализации политики приведены в 8.4.3.1—8.4.3.4.

8.4.3.1 В критичных воротах физического доступа PAG и/или сегментах должен находиться персонал охраны или должен осуществляться их телевизионный мониторинг, позволяющий обнаруживать нарушения и нарушителей.

8.4.3.2 Частью эффективного управления физическим доступом должны быть ознакомительные занятия с персоналом, имеющим одинаковые должностные обязанности.

8.4.3.3 В критичных воротах физического доступа PAG и/или сегментах должен находиться персонал охраны или должен осуществляться их телевизионный мониторинг, обеспечивающий ознакомление.

8.4.3.4 Реагирование на нарушение физического доступа должно управляться и координироваться человеческими ресурсами.

8.5 Управление сегментом

Структурирование ICS на отдельные логические или физические сегменты, защищенные SGW и/или PAG, эффективно уменьшает поверхность атаки за счет добавления еще одного параметра к параметрам присвоенной привилегии.

Примечание 1 — Различные логические сегменты могут пересекаться, например, магистралью (на том же уровне или в иерархической структуре).

Примечание 2 — О пересечениях между ICN и любой EN см. раздел 8.6.

8.5.1 Для защищенных границ логических и физических сегментов должны быть реализованы ворота PAG и шлюзы SGW с соответствующими правилами управления доступом, требованиями к защите и топологии.

Это обосновано тем, что обычно более экономично защищать оборудование, HMI и кабели, сгруппировав их, например, по отдельным зонам, комнатам, шкафам или арматурам и определив единственную точку входа, а не множество отдельных точек доступа.

Правила реализации политики приведены в 8.5.1.1—8.5.1.4

8.5.1.1 Каждый сегмент должен быть защищен SGW в единственной точке входа/выхода в общую магистраль или в подчиненный сегмент.

Примечание — Функция SGW и любые связанные с ним вспомогательные функции должны быть реализованы на выделенных хостах или приборах.

8.5.1.2 Шлюзы SGW должны разрешать связь со своей защищенной зоной только для станций из надежных зон или надежных устройств магистрали.

Примечание — Вся связь, не являющаяся необходимой, должна быть заблокирована, например связь, не являющаяся необходимой для бизнеса, либо связь, за которую явно никто не несет ответственности.

8.5.1.3 Управление доступом через шлюз SGW к сегменту может дополнительно контролироваться криптозащищенными протоколами или PAG.

Примечание — Оборудование (основное и вспомогательное), функции, служебные обязанности должны быть сгруппированы электрически, логически и физически в соответствии с функционалом и требованиями защиты.

8.5.1.4 Каждый шлюз SGW должен протоколировать соответствующие действия безопасности, например попытку доступа к защищаемому им сегменту.

8.5.2 Должен осуществляться постоянный мониторинг логической и/или физической активности внутри сегментов для обнаружения или пресечения неправильных или сомнительных действий (например, вторжения), создания соответствующих протоколов и выдачи сигналов тревоги.

Это обосновано тем, что ворота PAG и шлюзы SGW являются единственными точками потенциально возможного вторжения через границу сегмента, поэтому они предпочтительны для индикации несанкционированной деятельности. Это управление границей должно дополняться внутренними мерами, такими как система обнаружения вторжений IDS, в частности, при угрозе атак инсайдеров.

Правила реализации политики приведены в 8.5.2.1—8.5.2.4.

8.5.2.1 Должна быть реализована система IDS для обнаружения успешных вторжений и несанкционированных действий инсайдеров.

Примечание 1 — Датчик IDS должен быть неадресуемым, он должен только прослушиваться, для исключения вероятности атаки на него.

Примечание 2 — Системы IDS на базе хоста, IDS на базе сети и средств проверки целостности файловой системы должны иметь возможность дополнять друг друга.

Примечание 3 — Система обнаружения вторжений должна подразумевать подачу сигнала тревоги пользователями на хост.

8.5.2.2 Индикаторы, например, системы управления, HMI и/или подсистемы управления сигналами тревоги должны оповещать операторов о проблемах с изменениями потока данных, обусловленных реагированием на обнаруженную атаку.

8.5.2.3 Меры по уклонению от атак, например провокации, приманки, обеспечивают дополнительные возможности обнаружения после вторжения.

8.5.2.4 Персонал мониторинга и поддержки должен своевременно уведомляться о любых изменениях правил, которые могут привести к срабатыванию триггера, включающего подачу сигнала тревоги SGW.

8.5.3 Должно осуществляться надежное администрирование ворот PAG и шлюзов SGW.

Это обосновано тем, что шлюзы SGW должны надежно администрироваться, чтобы гарантировать, что сами правила доступа и строгость их соблюдения соответствуют развивающимся угрозам.

Правила реализации политики приведены в 8.5.3.1—8.5.3.3.

8.5.3.1 Управление должно распространяться на хосты, комнаты с сетевым оборудованием, шкафы, корпуса, кабельное хозяйство.

8.5.3.2 Необходимо уделять особое внимание трафику управления безопасностью.

Примечание — Каналы связи, используемые для управления безопасностью, должны быть отделены от каналов передачи производственного трафика.

8.5.3.3 Особое внимание должно быть уделено защите трафика управления безопасностью, поступающего из внешних сетей и уходящего во внешние сети, например внешнего поставщика услуг безопасности или удаленных сегментов.

8.6 Управление внешним доступом

Вся связь между ICN, сетями и устройствами, внешними по отношению к ICN, считается ненадежной, кроме безопасной, такой как связь во внешней сети EN организации. Общедоступная EN имеет гораздо большее число более разнообразных и менее надежных пользователей, чем сеть ICN.

8.6.1 Внешние соединения должны быть разрешены и реализованы, только если они необходимы для эксплуатации, управления и поддержания работоспособности ICS.

Это обосновано тем, что намеренный или случайный импорт в систему файлов с вредоносным программным обеспечением является существенной угрозой.

Правила реализации политики приведены в 8.6.1.1—8.6.1.7.

8.6.1.1 Должны быть установлены и соблюдаться процедуры защиты от импорта несанкционированных или зараженных файлов из ненадежных источников, таких как сети и портативные носители для хранения данных.

Примечание — Соответствующие директивы политики безопасности могут быть усилены техническими средствами.

8.6.1.2 Администрация ICS должна полностью контролировать все данные, импортированные в ICN, а также время их поступления.

8.6.1.3 Портативные устройства, пронесенные на завод, например портативные компьютеры, носители данных, должны считаться внешними устройствами.

8.6.1.4 Для критичных файлов, например исполняемых, импортированных физически или электронно, администрация ICS должна установить и соблюдать процедуры верификации, подтверждающие следующее: эти файлы являются именно теми файлами, которые требуются, они пригодны для использования, не содержат вредоносного кода, не были подделаны при передаче, были импортированы по требуемому назначению.

Примечание 1 — Физический импорт означает импорт портативных носителей хранения данных и других портативных электронных устройств.

Примечание 2 — Правила физического импорта должны быть увязаны с процедурами усиления защиты в части ограничения возможных назначений физического импорта, например интерфейсов и портов доступа.

8.6.1.5 Для обновлений и операций обслуживания, выполняемых техническими специалистами изготовителя, должны быть утверждены процедуры установления временных или специально выделенных для этой цели соединений.

8.6.1.6 Для непрерывных онлайн-сессий должны часто меняться ключи, например при каждой новой регистрации.

Примечание — Требования к безопасности должны учитывать сбои канала связи.

8.6.1.7 Должен осуществляться мониторинг несанкционированного доступа ко всем средствам связи, предназначенным как для внутризаводской связи, так и для связи с объектами, находящимися за пределами завода.

Примечание — Должен осуществляться мониторинг возможных средств связи, в том числе телефонных сетей общего пользования POTS, средств радиосвязи, сотовой связи, беспроводного доступа и т. д.

8.6.2 Соединения с внешними сетями связи должны быть защищены ECG в соответствии с требованиями защиты.

Это обосновано тем, что вся связь между хостами, устройствами ICS и внешними сетями или устройствами должна быть защищена от угроз, исходящих от внешних сетей организации, и виртуально неограниченных угроз, исходящих от общедоступных внешних сетей.

В данной политике предусмотрены предварительные условия и ограничения, заключающиеся в том, что в политике управления доступом должен быть запрещен массовый/полный доступ через ECG, например вещание, монтирование файлов и т. д.

Правила реализации политики приведены в 8.6.2.1 и 8.6.2.2.

8.6.2.1 Соответствующие механизмы должны использоваться только для того, например, чтобы гарантировать целостность источника, целостность данных и, если требуется, конфиденциальность.

Примечание — Собственные механизмы безопасности могут при работе через ECG функционировать неправильно, при этом может потребоваться специальная обработка.

8.6.2.2 Если для адекватной защиты, в том числе аутентификации, требуются прокси-серверы, они должны быть реализованы.

Это предотвращает угрозы, исходящие от EN, например прямое наблюдение ICN, трафика и характеристик протоколов хостов ICN. Кроме того, можно экранировать входящий и исходящий контент на уровне приложений.

8.6.3 Должны управляться и протоколироваться доступ к внешним пользователям и устройствам и доступ от них.

Это обосновано тем, что это требование обеспечивает надежную связь по линиям удаленного доступа, отражение атак инсайдеров, использующих удаленного клиента, и позволяет отслеживать очевидные атаки и вторжения.

Правила реализации политики приведены в 8.6.3.1 и 8.6.3.2.

8.6.3.1 Когда сессии удаленного доступа не требуются, в соответствующие этому периоды времени связь с внешними пользователями и устройствами должна быть неработоспособна.

Примечание — Представляется более надежным электрическое отсоединение пользователей и устройств, чем логическое блокирование учетных записей пользователей удаленного доступа на ESG или прокси-сервере.

8.6.3.2 Для критичных видов связи протоколирование действий внешнего доступа должно позволять воспроизвести сессию повторно во всех подробностях.

8.6.4 Должны осуществляться управление безопасностью удаленных клиентов, их сертификация и авторизация.

Это обосновано тем, что для установления и поддержания доверия удаленные клиенты требуют соответствующих технических механизмов и настроек, на них распространяется политика безопасности ICS.

Примечание — Сюда входят удаленные: центр управления, клиент, хосты, рабочие станции, устройства.

В данной политике предусмотрены предварительные условия и ограничения, заключающиеся в том, что если управление осуществляется другой организацией (не ICS), то эта организация может иметь отличающиеся IT-политики безопасности. В этом случае должны быть заключены подробные контрактные соглашения между организацией ICS и организацией удаленного клиента.

Правила реализации политики приведены в 8.6.4.1—8.6.4.3.

8.6.4.1 Политика ICS должна применяться к удаленному клиенту в полном объеме. Должны быть соблюдены периоды времени использования и соединения с ICN.

8.6.4.2 Закрепленные службы и порты должны быть сконфигурированы заранее, например использование идентификации вызывающего абонента или обратный набор фиксированного номера в телефонных сетях. Безопасные каналы также должны быть сконфигурированы заранее.

8.6.4.3 Администрация ICS должна периодически проводить аудит соответствия работы удаленного клиента политике безопасности ICS или контрактным соглашениям.

8.6.5 Шлюзы SGW должны осуществлять мониторинг правил доступа к связи и контролировать их соблюдение.

Это обосновано тем, что для гарантии того, что персонал ICS осведомлен о всех входящих сессиях удаленного доступа и может контролировать время сессий удаленного доступа, должны использоваться технические средства.

Правила реализации политики приведены в 8.6.5.1—8.6.5.3.

8.6.5.1 Должен осуществляться централизованный мониторинг шлюзов SGW.

8.6.5.2 Должно быть определено реагирование на нарушения управления доступом. Это реагирование должно быть задокументировано и выполняться немедленно после нарушения, в соответствии с планом действий в непредвиденных обстоятельствах.

8.6.5.3 Должно быть определено реагирование на проблемы с доступностью. Это реагирование должно быть документировано и выполняться немедленно, в соответствии с планом действий в непредвиденных обстоятельствах.

См. об отчетах о событиях информационной безопасности и ее слабостях в ИСО/МЭК 27002.

8.6.6 Риски доступности критичных внешних каналов связи могут быть уменьшены.

Это обосновано тем, что доступность может быть важным аспектом при эксплуатации и поддержании работоспособности ICS.

В данной политике предусмотрены предварительные условия и ограничения, заключающиеся в том, что сбой канала связи во время атаки отказа в обслуживании невозможно предотвратить, так как механизмы безопасности, применимые к хостам ICN и/или коммуникационным устройствам, не влияют на доступность внешней связи.

Доступность любого индивидуального канала связи внешней сети не управляется администрацией ICS и поэтому не может быть гарантирована с какой-либо разумной степенью достоверности.

Правила реализации политики приведены в 8.6.6.1 и 8.6.6.2.

8.6.6.1 Скорость передачи в заданной полосе частот при связи должна быть выбрана с учетом важности для эксплуатации и поддержания работоспособности.

Примечание — Доступная полоса частот может быть выделена нескольким пользователям, с ограничениями по скорости и с установкой приоритетов.

8.6.6.2 Для повышения доступности должны использоваться методы резервирования и разветвления.

Примечание 1 — Методы разветвления включают в себя использование отдельных поставщиков услуг, дополнение общедоступных сетей телефонными сетями общего пользования или беспроводными сетями.

Примечание 2 — Разветвление или простое резервирование повышают уязвимость к атакам (см. 8.1.1.1).

Приложение А
(справочное)

Готовящееся к публикации новое издание МЭК 62443

Под общим наименованием «Безопасность при измерении производственного процесса и управлении им — безопасность системы и сети» готовящееся к публикации новое издание МЭК 62443 объединит следующие части:

- часть 1: Рабочий процесс — анализ рисков и угроз*;
- часть 2: Гарантирование безопасности: принципы, политика, практические методы**;
- часть 3: Требования безопасности при типовых сценариях безопасности.

Готовящееся издание МЭК 62443 должно приобрести статус основной публикации по безопасности, наподобие того, как основной публикацией по эксплуатационной безопасности является IEC Guide 104.

Введение

По мере роста использования общедоступных сетей, системы автоматизации, ранее бывшие изолированными от них, становятся все более уязвимыми для атак. Стандартные IT-механизмы безопасности, использующие защищаемые цели и стратегии защиты, могут оказаться непригодными для систем автоматизации, например, когда своевременное реагирование может оказаться критичным для безопасности и эксплуатационной безопасности персонала завода, окружающей среды и корпорации. Этот стандарт посвящен конкретным аспектам безопасного доступа к промышленным системам и внутри них, в частности когда наиболее широко распространенные методы обеспечения безопасности на основе IT оказываются неэффективными или неподходящими.

Особые акценты сделаны на обеспечении жизненного цикла безопасности, на использовании глобального перехода от добавления компонент безопасности системы к интеграции требуемых свойств безопасности в продукты и системы в виде неотъемлемой части их функционала и жизненного цикла.

Для приложений эксплуатационной безопасности, приложений в фармацевтической и других высокоспециализированных отраслях промышленности могут применяться дополнительные стандарты, рекомендации, определения и условия, например МЭК 61508, GAMP (ISPE), для GMP — совместимость с 21 CFR (FDA) и стандартная процедура эксплуатации, принятая Европейским медицинским агентством (SOP/INSP/2003).

Обзор

Данный стандарт будет устанавливать требования для безопасного доступа к измерениям производственного процесса, сетям управления и устройствам этих сетей в течение всего жизненного цикла ICS.

Данный стандарт будет предоставлять требования и руководящие принципы по целям безопасности для:

- разработчиков систем автоматизации;
- производителей (изготовителей) устройств, подсистем и систем;
- интеграторов подсистем и систем;
- владельцев и операторов систем автоматизации (ответственных за эксплуатацию завода).

Стандарт будет учитывать следующие аспекты:

- постепенное развитие и миграцию для существующих систем, меры, принимаемые при разработке новых систем и компонентов;
- технологии и продукты, удовлетворяющие целям безопасности, включая COTS;
- режимы работы после отказа, при которых обеспечивается эксплуатационная безопасность процесса, в том числе при отказе в обслуживании (например, автономная работа);
- надежность и доступность;
- масштабируемость (от сложных заводов до маленьких недорогих систем с малыми рисками);
- разделение требований безопасности, эксплуатационной безопасности и требований функционала, насколько это возможно;
- рассмотрение аспектов безопасности во время разработки систем автоматизации и их компонент.

Примечание — Заводы и системы могут содержать критичные для эксплуатационной безопасности компоненты и устройства, особенно устройства, разработанные в соответствии с МЭК 61508 и SILs. Критичные для эксплуатационной безопасности компоненты и устройства могут применяться в целях безопасности, определяемых с помощью отдельного анализа. Эти цели безопасности могут соответствовать рекомендациям, предложенным в данном стандарте, однако он не гарантирует, что все его спецификации будут пригодными или существенными для безопасности таких устройств обеспечения эксплуатационной безопасности. Этот стандарт не решает проблем безопасности домов, защиты граждан и защиты от военных атак или природных катастроф.

---

* Действует IEC/TS 62443-1-1:2009.

** Действует МЭК 62443-2-1:2010.

МЭК 62443 (часть 1) позволит пользователю оценить ситуацию с безопасностью, например, в терминах применимых угроз и уязвимостей и подготовиться к управлению рисками безопасности в течение всего жизненного цикла системы пользователя. Часть 1 включает:

- словарь, определения терминов, целевую аудиторию, область применения, заинтересованные стороны, роли;
- общие черты и отличия промышленных систем управления в сравнении с широко распространенными применениями IT;
- события атак и их сценарии;
- жизненный цикл;
- ожидаемые результаты анализа рисков и угроз;
- примеры для:
- цели безопасности;
- анализа уязвимостей;
- оценки рисков.

МЭК 62443 (часть 2) позволяет пользователям определить и реализовать их политики безопасности, связать результирующие требования с желаемыми практическими аспектами и уровнем детальности и со всеми фазами жизненного цикла. В части 2 рассмотрены:

- принципы обеспечения надежности, классификация, оценка;
- принципы разработки устройств, критерий проектирования, свойства устройств;
- старые устройства, COTS и устройства, находящиеся на стадии разработки;
- аспекты безопасности во время разработки компонентов (не только компонентов безопасности) промышленных систем управления (датчики/актюаторы/PLC/сеть/сервер/HMI).

В МЭК 62443 (часть 3) приведены примеры решений на основе использования практических методов для типовых сценариев. Приведенные примеры помогут пользователям выполнить конкретную реализацию:

- типовых сценариев и мер безопасности;
- типовых политик безопасности, описаний процессов и процедур.

Приложение ДА
(справочное)

Алфавитный указатель терминов

Атака (attack)	3.1.6
Аудит (audit)	3.1.8
Владелец/оператор (owner/operator)	3.1.41
Внешний (external)	3.1.19
Внешняя сеть (external network; EN)	3.1.21
Ворота физического доступа (physical access gate; PAG)	3.1.44
Вредоносные программы (malware)	3.1.36
В режиме реального времени (real-time)	3.1.49
Демилитаризованная зона (demilitarized zone, DMZ)	3.1.15
Детектирование несанкционированных проникновений (intrusion detection)	3.1.33
Доверие, доверять (trust, trusted)	3.1.61
Доступность (availability)	3.1.10
Завод (plant)	3.1.46
Защита от непризнания участия (non-repudiation)	3.1.40
Защищенный, защищенность (secure, security)	3.1.53
Значимость для безопасности/значимый для безопасности (security relevance/relevant)	3.1.58
Имущественный объект (asset)	3.1.4
Инсайдер, в пределах, внутренний (insider, inside, internal)	3.1.29
Интранет, интрасеть (intranet)	3.1.31
Инцидент (incident)	3.1.26
Источник угрозы (adversary)	3.1.2
Коммерчески доступные продукты (Commercial off the shelf, COTS)	3.1.11
Контрмера (countermeasure)	3.1.37
Конфиденциальность (confidentiality)	3.1.13
Криптографический или физический ключ [(cryptographic or physical) key]	3.1.34
Мера безопасности (security measure)	3.1.56
Надежность (assurance)	3.1.5
Нарушение безопасности (security violation)	3.1.59
Незащищенный, незащищенность (exposed, exposure)	3.1.18
Несанкционированное проникновение (intrusion)	3.1.32
Остаточный риск (residual risk)	3.1.51
Отказ в обслуживании (атака) [denial of service (attack)]	3.1.16
Открытый текст (plaintext)	3.1.45
Отслеживать (monitor)	3.1.39
Периметр (perimeter)	3.1.43
Поверхность атаки (attack surface)	3.1.7
Политика безопасности (security policy)	3.1.57
Пользователь (user)	3.1.63
Привилегия (privilege)	3.1.47
Проведение аутентификации, аутентификация (authenticate, authentication)	3.1.9
Прокси (сервер) [proxy (server)]	3.1.48
Промышленная сеть управления (industrial control network; ICN)	3.1.27
Промышленная система управления (industrial control system; ICS)	3.1.28
Протоколировать, протоколирование (log, logging)	3.1.35
Регистрационные данные (credentials)	3.1.14
Резервирование (redundancy)	3.1.50
Риск (risk)	3.1.52
Сегмент, сегментирование (partition, partitioning)	3.1.42
Сигнал тревоги (alert)	3.1.3
Система управления (информационной) безопасностью [(information) security management system (ISMS)]	3.1.55
Событие (event)	3.1.17
Сообщение (message)	3.1.38
Угроза (threat)	3.1.62
Управление доступом (access control)	3.1.1
Усилить защиту, усиление защиты (harden, hardening)	3.1.24

Утечка информации (compromise) 3.1.12
Целостность (integrity) 3.1.30
Центр безопасности (security centre) 3.1.54
Человеко-машинный интерфейс (human-machine-interface; HMI) 3.1.25
Шлюз внешних подключений (external connectivity gateway; ECG) 3.1.20
Шлюз, шлюз безопасности (gateway, security gateway; SGW) 3.1.23
Экспертиза (forensic) 3.1.22
Эффективность функции (strength of function) 3.1.60

Приложение ДБ
(справочное)

Сведения о соответствии ссылочных международных стандартов национальным стандартам

Таблица ДБ.1

Обозначение ссылочного международного стандарта	Степень соответствия	Обозначение и наименование соответствующего национального стандарта
ISO/IEC 15408 (all parts)	IDT	ГОСТ Р ИСО/МЭК 15408-14—2012 «Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 1. Введение и общая модель»
	IDT	ГОСТ Р ИСО/МЭК 15408-2—2013 «Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 2. Функциональные компоненты безопасности»
	IDT	ГОСТ Р ИСО/МЭК 15408-3—2013 «Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 3. Компоненты доверия к безопасности»
ISO/IEC 27002:2005	IDT	ГОСТ Р ИСО/МЭК 27002—2012 «Информационная технология. Методы и средства обеспечения безопасности. Свод норм и правил менеджмента информационной безопасности»
ISO/IEC Guide 73:2002	IDT	ГОСТ Р 51897—2011/Руководство ИСО 73:2009 «Менеджмент риска. Термины и определения»
Примечание — В настоящей таблице использовано следующее условное обозначение степени соответствия стандартов: - IDT — идентичные стандарты.		

Библиография

[1] ISO/IEC 13335-1:2004, Information technology — Security techniques — Management of information and communications technology security — Part 1: Concepts and models for information and communications technology security management

[2] ISO/IEC TR 13335-4:2000, Information technology — Guidelines for the management of IT Security — Part 4: Selection of safeguards

[3] ISO/IEC TR 13335-5:2001, Information technology — Guidelines for the management of IT Security — Part 5: Management guidance on network security

[4] ISO/IEC 15288:2002, Systems engineering — System life cycle processes

[5] ISO/IEC TR 15443-1:2005, Information technology — Security techniques — A framework for IT security assurance — Part 1: Overview and framework

[6] ISO/IEC 15446:2004, Information technology — Security techniques — Guide for the production of Protection Profiles and Security Targets

[7] ISO/IEC 21827:2002, Information technology — Systems Security Engineering — Capability Maturity Model (SSE-CMM)

[8] ISO/IEC 27001:2005, Information technology — Security techniques — Information security anagement systems — Requirements

[9] IEC 61508:1998 (all parts), Functional safety of electrical/electronic/programmable electronic safety-related systems

[10] NIST SP 800-82, «Guide to Supervisory Control and Data Acquisition (SCADA) and Other Industrial Control System Security», Initial Public Draft, September 2006

[11] NIST SP 800-53, «Recommended Security Controls for Federal Information Systems», Second Public Draft, July 2006

[12] Technology Assessment — Cybersecurity For Critical Infrastructure Protection», United States General Accounting Office, May 2004

[13] «Cyber Security Procurement Language for Control Systems», Draft, November 2006, Idaho National Laboratory, Idaho Falls, ID 83415, USA

[14] «Systems Assurance — Delivering Mission Success in the Face of Developing Threats», Systems Assurance Committee, NDIA, USA

[15] «A study of the applicability of ISO/IEC 17799 and the German Baseline Protection Manual to the needs of safety critical systems», EWICS (European Workshop on Industrial Computer Systems) Technical Committee No. 7: Reliability, Safety and Security; Roadmap D31.

gost.e-ecolog.ru

[16] «Good Automated Manufacturing Practice (GAMP): Guide for Validation of Automated Systems in Pharmaceutical Manufacture», ISPE, 3109 W. Dr. Martin Luther King Jr. Blvd., Suite 250, Tampa, FL 33607, USA

УДК 004.056.5:006.354

ОКС 25.040.40
35.110

Ключевые слова: промышленные коммуникационные сети, сети и системы, защищенность, кибербезопасность, промышленная система управления, модель угроз-рисков, жизненный цикл безопасности, модель защиты, политика безопасности

Редактор *Н.В. Таланова*
Технический редактор *В.Н. Прусакова*
Корректор *Е.М. Поляченко*
Компьютерная верстка *Д.В. Кардановской*

Сдано в набор 17.01.2019. Подписано в печать 25.01.2019. Формат 60 × 84 1/8. Гарнитура Ариал.
Усл. печ. л. 5,58. Уч.-изд. л. 5,10.

Подготовлено на основе электронной версии, предоставленной разработчиком стандарта

ИД «Юриспруденция», 115419, Москва, ул. Орджоникидзе, 11.
gost.e-ecolog.ru gost.e-ecolog.ru

Создано в единичном исполнении ФГУП «СТАНДАРТИНФОРМ»
для комплектования Федерального информационного фонда стандартов,
117418 Москва, Нахимовский пр-т, д. 31, к. 2.
gost.e-ecolog.ru stinfo.ru

gost.e-ecolog.ru