ФЕДЕРАЛЬНОЕ АГЕНТСТВО

ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

ГОСТ Р МЭК 62443-3-3— 2016

СЕТИ ПРОМЫШЛЕННОЙ КОММУНИКАЦИИ

Безопасность сетей и систем

Часть 3-3

Требования к системной безопасности и уровни безопасности

(IEC 62443-3-3:2013, IDT)

Издание официальное

Москва
Стандартинформ
2016

gost.e-ecolog.ru

Предисловие

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

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

3 УТВЕРЖДЕН И ВВЕДЕН В ДЕЙСТВИЕ Приказом Федерального агентства по техническому регулированию и метрологии от 1 июня 2016 г. № 469-ст

4 Настоящий стандарт идентичен международному стандарту МЭК 62443-3-3: 2013 «Сети промышленной коммуникации. Безопасность сетей и систем. Часть 3-3. Требования к системной безопасности и уровни безопасности» (IEC 62443-3-3-1:2013 «Industrial communication networks — Network and system security — Part 3-3: System security requirements and security levels», IDT).

Международный стандарт разработан Техническим комитетом МЭК ТК 65 «Измерения и управление в промышленных процессах».

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

5 Некоторые элементы настоящего стандарта могут быть предметом патентных прав

6 ВВЕДЕН ВПЕРВЫЕ

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

© Стандартинформ, 2016

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 . . . 1
3 Термины, определения, сокращения, допущения . . . 2
3.1 Термины и определения . . . 2
3.2 Сокращения . . . 6
3.3 Допущения . . . 8
4 Общие ограничения безопасности систем управления . . . 8
4.1 Обзор . . . 8
4.2 Поддержка жизненно важных функций . . . 8
4.3 Компенсационные контрмеры . . . 9
4.4 Минимальная привилегия . . . 10
5 FR 1 — Управление идентификацией и аутентификацией . . . 10
5.1 Назначение и описания SL-C(IAC) . . . 10
5.2 Целесообразность . . . 10
5.3 SR 1.1 — Идентификация и аутентификация пользователя — физического лица . . . 10
5.4 SR 1.2 — Идентификация и аутентификация программных процессов и устройств . . . 11
5.5 SR 1.3 — Управление учетными записями . . . 12
5.6 SR 1.4 — Управление идентификаторами . . . 13
5.7 SR 1.5 — Управление аутентификаторами . . . 14
5.8 SR 1.6 — Управление беспроводным доступом . . . 15
5.9 SR 1.7 — Надежность аутентификации по паролю . . . 15
5.10 SR 1.8 — Сертификаты инфраструктуры открытых ключей (PKI) . . . 16
5.11 SR 1.9 — Надежность аутентификации по открытому ключу . . . 17
5.12 SR 1.10 — Обратная связь при аутентификации . . . 18
5.13 SR 1.11 — Неудачные попытки входа в систему . . . 18
5.14 SR 1.12 — Уведомление об использовании системы . . . 19
5.15 SR 1.13 — Доступ через недоверенные сети . . . 20
6 FR 2 — Контроль использования . . . 20
6.1 Назначение и описания SL-C(UC) . . . 20
6.2 Целесообразность . . . 20
6.3 SR 2.1 — Контроль выполнения авторизаций . . . 21
6.4 SR 2.2 — Контроль беспроводного использования . . . 22
6.5 SR 2.3 — Контроль использования портативных и подвижных устройств . . . 23
6.6 SR 2.4 — Мобильный код . . . 23
6.7 SR 2.5 — Блокировка сеанса . . . 24
6.8 SR 2.6 — Прерывание удаленных сеансов . . . 24
6.9 SR 2.7 — Контроль параллельных сеансов . . . 25
6.10 SR 2.8 — События, подлежащие аудиту . . . 25
6.11 SR 2.9 — Емкость систем хранения данных аудита . . . 26
6.12 Ответные действия в случае сбоев обработки данных аудита . . . 26
6.13 SR 2.11 — Временные метки . . . 27
6.14 SR 2.12 — Защита от непризнания участия . . . 27
7 FR 3 — Целостность системы . . . 28

7.1 Назначение и описания SL-C(SI) . . . 28
7.2 Целесообразность . . . 28
7.3 SR 3.1 — Целостность коммуникации . . . 28
7.4 SR 3.2 — Защита от вредоносного кода . . . 30
7.5 SR 3.3 — Верификация функциональности безопасности . . . 30
7.6 SR 3.4 — Целостность программного обеспечения и информации . . . 31
7.7 SR 3.5 — Валидация входных данных . . . 32
7.8 SR 3.6 — Детерминированный поток выходных сигналов . . . 32
7.9 SR 3.7 — Обработка ошибок . . . 33
7.10 SR 3.8 — Целостность сеанса . . . 33
7.11 SR 3.9 — Защита информации аудита . . . 34
8 FR 4 — Конфиденциальность данных . . . 35
8.1 Назначение и описания SL-C(DC) . . . 35
8.2 Целесообразность . . . 35
8.3 SR 4.1 — Конфиденциальность информации . . . 35
8.4 SR 4.2 — Сохранность информации . . . 36
8.5 SR 4.3 — Использование криптографии . . . 37
9 FR 5 — Ограничение потока данных . . . 37
9.1 Назначение и описания SL-C(RDF) . . . 37
9.2 Целесообразность . . . 38
9.3 SR 5.1 — Сегментация сети . . . 38
9.4 SR 5.2 — Защита границ зоны . . . 39
9.5 SR 5.3 — Ограничения на передачу общецелевой информации «абонент — абонент» . . . 40
9.6 SR 5.4 — Разбиение приложений . . . 40
10 FR 6 — Своевременный отклик на события . . . 41
10.1 Назначение и описания SL-C(TRE) . . . 41
10.2 Целесообразность . . . 41
10.3 SR 6.1 — Доступность файлов регистрации аудита . . . 41
10.4 SR 6.2 — Непрерывный мониторинг . . . 42
11 FR 7 — Работоспособность и доступность ресурсов . . . 42
11.1 Назначение и описания SL-C(RA) . . . 42
11.2 Целесообразность . . . 43
11.3 SR 7.1 — Защита от отказа в обслуживании . . . 43
11.4 SR 7.2 — Управление ресурсами . . . 43
11.5 SR 7.3 — Резервирование в системе управления . . . 44
11.6 SR 7.4 — Восстановление и воссоздание системы управления . . . 44
11.7 SR 7.5 — Аварийное питание . . . 45
11.8 SR 7.6 — Параметры конфигурации сети и безопасности . . . 45
11.9 SR 7.7 — Минимальная функциональность . . . 46
11.10 SR 7.8 — Инвентаризация компонентов системы управления . . . 46
Приложение А (справочное) Описание вектора SL . . . 47
Приложение В (справочное) Соотнесение SR и RE с уровнями SL 1 — 4 FR . . . 54
Приложение ДА (справочное) Сведения о соответствии ссылочных международных стандартов ссылочным национальным стандартам Российской Федерации . . . 58
Библиография . . . 59

0 Введение

0.1 Обзор

Примечание 1 — Настоящий стандарт представляет собой часть серии стандартов, посвященной вопросам безопасности систем промышленной автоматизации и контроля (IACS). Он разработан рабочей группой 4 исследовательской группы 2 комитета МЭК 99 в сотрудничестве с МЭК ТК65/РГ10. Настоящий документ регламентирует требования безопасности для систем управления, соотносящиеся с семью фундаментальными требованиями, определенными в МЭК 62443-1-1, и устанавливает уровни безопасности (SL) для рассматриваемой системы (РС).

Примечание 2 — Формат настоящего стандарта соответствует требованиям ИСО/МЭК, рассмотренным в Директивах ИСО/МЭК, часть 2 [11][1]. Эти директивы регламентируют формат стандарта, а также использование терминов типа «должен», «должен по возможности» и «может». Для требований, определенных в обязательных пунктах, использованы соглашения, рассмотренные в приложении Н Директив ИСО/МЭК.

Организации, эксплуатирующие системы промышленной автоматизации и контроля (IACS), все чаще используют коммерчески доступные (COTS) сетевые устройства, которые имеют малую стоимость, эффективны и высокоавтоматизированы. Кроме того, из веских коммерческих соображений, системы управления все чаще взаимодействуют и с сетями, не относящимися к IACS. Эти устройства, общедоступные сетевые технологии и возросшие возможности сетевого взаимодействия расширяют возможности для кибератак на аппаратное и программное обеспечение систем управления. Эта проблема может иметь последствия, затрагивающие охрану труда, технику безопасности и охрану окружающей среды (HSE), и/или наносить финансовые убытки и/или ущерб репутации всюду, где внедряются системы управления.

Организации, внедряющие бизнес-решения в сфере кибербезопасности информационных технологий (IT) для разрешения вопросов, связанных с безопасностью IACS, могут не вполне осознавать последствия такого выбора. Хотя многие коммерческие прикладные IT-объекты и решения безопасности могут быть применимы к IACS, их необходимо применять надлежащим образом для исключения непредвиденных последствий. По этой причине подход, используемый для определения системных требований, должен базироваться на комбинации функциональных требований и оценки риска и зачастую включает в себя и необходимость иметь осведомленность в вопросах эксплуатации.

Меры безопасности IACS не должны иметь возможность приводить к нарушению существенных сервисов и функций, включая процедуры при нештатных ситуациях. (Часто меры безопасности IT имеют данную тенденцию.) Обеспечение безопасности IACS нацелено на работоспособность и доступность систем управления, защищенность производственных объектов, производственных процессов (хотя бы в режиме ограниченной функциональности) и времени отклика системы, где это имеет критическое значение. В рамках целей IT-безопасности этим факторам зачастую придается меньшее значение. Бóльшее значение придается защите информации, чем защите физических объектов. Эти различные цели должны быть четко определены как цели безопасности, независимо от степени достигнутой интеграции производственного объекта. Ключевым этапом в оценке риска согласно требованиям МЭК 62443-2-1[2] должна по возможности быть идентификация тех сервисов и функций, которые действительно существенны для процессов хозяйствования. (Например, на тех или иных объектах техническая поддержка может быть определена как несущественный сервис или функция.) В некоторых случаях может быть допустимо, чтобы операция безопасности провоцировала временную утрату несущественного сервиса или функции, но по возможности не сказывалась отрицательно на существенном сервисе или функции.

Настоящий стандарт предполагает, что программа безопасности учреждена и управляется в соответствии с МЭК 62443-2-1. Кроме того, предполагается, что управление патчами осуществляется сообразно рекомендациям, подробно рассмотренным в МЭК/ТО 62443-2-3 [5], с соблюдением соответствующих требований и их доработок, описанных в настоящем стандарте, применительно к системам управления. Также в МЭК 62443-3-2 [8] описано, каким образом проект задает уровни безопасности (SL), основанные на риске, которые затем используются для выбора продуктов с подходящими техническими характеристиками безопасности, что подробно рассмотрено в настоящем стандарте. Ключевой

[1] Цифры в квадратных скобках относятся к элементу стандарта «Библиография».

[2] Многие стандарты из стандартов серии МЭК 62443 в настоящее время находятся на пересмотре или доработке.

исходный материал для настоящего стандарта включал в себя ИСО/МЭК 27002 [15] и NIST SP800-53, ред. 3 [24] (см. раздел 2 и Библиографию, которые содержат более полный перечень первоисточников).

Основная задача стандартов из стандартов серии МЭК 62443 — предоставить гибкую концепцию, которая облегчает устранение текущих и будущих уязвимостей в IACS и применение необходимых смягчающих мер в систематическом, оправданном порядке. Важно понимать, что назначение серии МЭК 62443 — сформировать расширения корпоративной безопасности, которые перенимают требования к коммерческим IT-системам и увязывают эти требования с едиными требованиями по обеспечению надежной работоспособности, необходимой в IACS.

0.2 Назначение и целевая аудитория

Целевая аудитория настоящего стандарта рассчитана на работников, имеющих отношение к системам IACS, и включает в себя собственников имущественных объектов, системных интеграторов, поставщиков продуктов, провайдеров сервисов и — в меру целесообразности — органы нормативно-правового регулирования. Органы нормативно-правового регулирования включают в себя правительственные агентства и регламентирующие органы, при этом нормативно-правовой орган должен осуществлять аудиты для проверки соответствия регулирующим законам и нормам.

Системным интеграторам, поставщикам продуктов и провайдерам сервисов настоящий стандарт послужит для оценки того, могут ли их продукты и сервисы обеспечивать потенциал функциональной безопасности, который соответствует требованиям целевого уровня безопасности (SL-T) собственника имущественного объекта. Как и в случае с присвоением уровней SL-T, применимость системных требований (SR) к отдельно взятой системе управления и расширений к этим требованиям (RE) должна базироваться на политиках безопасности собственника объекта, регламентах и оценке риска в контексте относящегося к ним участка применения. Следует отметить, что некоторые SR содержат специальные условия для допустимых исключений, например в случае, когда соответствие SR идет вразрез с фундаментальными требованиями эксплуатации системы управления (что может спровоцировать необходимость компенсационных контрмер).

Если разрабатываемая система управления должна соответствовать набору SR, привязанных к конкретным SL-T, то не требуется, чтобы каждый компонент предлагаемой системы управления соответствовал каждому системному требованию до степени, предписываемой настоящим стандартом. Могут применяться компенсационные контрмеры для придания необходимой функциональности другим подсистемам, так чтобы общие требования SL-T выполнялись на уровне системы управления. Включение в расчет компенсационных контрмер на стадии разработки следует подкреплять исчерпывающей документацией, чтобы итоговый достигнутый SL-A системы управления полностью отражал расчетные характеристики безопасности, присущие проекту. Точно так же в ходе сертификационных испытаний и/или постинсталляционных аудитов могут применяться и документироваться компенсационные контрмеры для обеспечения соответствия общему SL системы управления.

В настоящем стандарте представлена не достаточно детальная информация для разработки и построения интегрированной архитектуры безопасности. Это потребовало бы дополнительного анализа на системном уровне и разработки производных требований, которые являются темой других стандартов серии МЭК 62443 (см. 0). Следует отметить, что задачей настоящего стандарта не является формирование спецификаций, достаточно детальных для построения архитектуры безопасности. Задачей является определение общего минимального набора требований для достижения соответствия все более строгим уровням безопасности. Сам проект архитектуры, удовлетворяющей этим требованиям, — это работа системных интеграторов и поставщиков продуктов. В рамках этой задачи они удерживают за собой право индивидуальных выборов, поддерживая тем самым конкуренцию и инновационную деятельность. Таким образом, в настоящем стандарте строго выдержан принцип определения функциональных требований и не рассматривается возможный порядок соответствия этим функциональным требованиям.

0.3 Применимость в контексте других частей серии МЭК 62443

На рисунке 1 графически представлена структура стандартов серии МЭК 62443 на момент разработки настоящего стандарта.

В МЭК 62443-3-2 SR и RE приводятся в виде стандартизированного перечня. После того как рассматриваемая система (SuC) описана в плане зон и трактов и данным зонам и трактам присвоены конкретные целевые SL, в указанном стандарте SR и RE, а также присвоение им потенциальных SL (SL-C)

использованы для составления перечня требований, которому должен соответствовать проект системы управления. Отдельно взятый проект системы управления может быть затем проверен на полноту, и определен достигнутый уровень безопасности (SL-A).

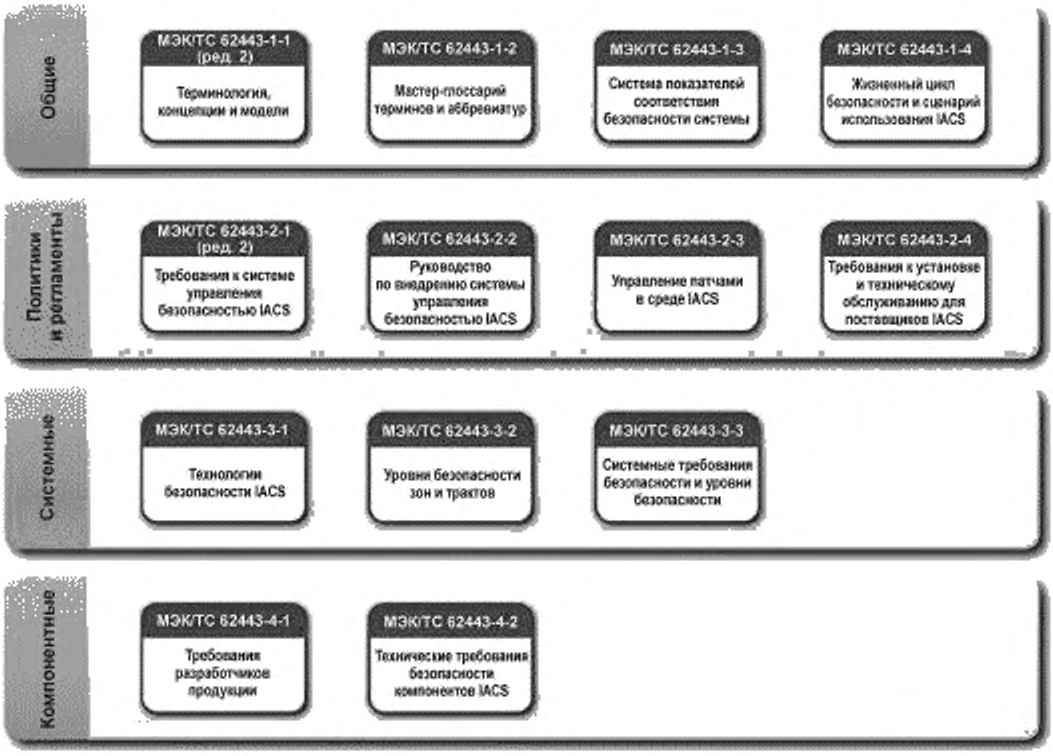

Рисунок 1 — Структура стандартов серии МЭК 62443

В МЭК/ТС 62443-1-3 [2] используются фундаментальные требования (FR), SR, RE и им присваиваются уровни SL-C в виде стандартизированного перечня для проверки полноты спецификации количественной системы показателей. Количественные системы показателей безопасности привязаны к контексту. Как и в МЭК 62443-3-3-2, присваиваемые собственником объекта SL-T преобразованы в количественную систему показателей, которая может использоваться при разработке архитектуры безопасности и служить для планирования сравнительных исследований, а также в качестве опоры для системного анализа.

В МЭК 62443-4-1 [9] рассмотрены общие требования к процессу разработки продуктов. В связи с этим МЭК 62443-4-1 ориентирован на поставщиков продуктов. Требования к безопасности продуктов являются производными перечня основополагающих требований и РТ, определенных в настоящем стандарте. Нормативы качества, определенные в МЭК 62443-4-1, будут использоваться при разработке характеристик этих продуктов.

МЭК 62443-4-2 [10] содержит наборы производных требований, которые обеспечивают детальное присвоение SR, определенных в этом стандарте, подсистемам и компонентам SuC. На момент разработки настоящего стандарта в МЭК 62443-4-2 рассматривались следующие категории компонентов: встраиваемые устройства, главные устройства, сетевые устройства и приложения. В связи с этим МЭК 62443-4-2 ориентирован на поставщика (поставщиков продуктов и провайдеров сервисов). Сначала выведены требования безопасности продуктов из перечня основополагающих требований и RE, определенных в данном стандарте. Требования безопасности и системы показателей из МЭК 62443-3-2 и МЭК/ТС 62443-1-3 использованы для уточнения этих производных нормативных требований.

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

СЕТИ ПРОМЫШЛЕННОЙ КОММУНИКАЦИИ

Безопасность сетей и систем

Часть 3-3

Требования к системной безопасности и уровни безопасности

Industrial communication networks. Network and system security.
Part 3-3. System security requirements and security levels

Дата введения — 2017—04—01

1 Область применения

В настоящем стандарте сформулированы детальные системные требования (SR) к техническим системам управления, привязанные к семи фундаментальным требованиям (FR), описанным в МЭК 62443-1-1, который включает в себя определение требований к потенциальным уровням безопасности (SL-C) (система управления). Работники, имеющие отношение к системам промышленной автоматики и контроля (IACS), смогут использовать данные требования вместе с информацией о зонах и трактах, определенных для рассматриваемой системы (SuC), в ходе разработки целевого уровня, SL-T (система управления) соответствующей системы управления, применительно к конкретному объекту.

Как определено в МЭК 62443-1-1, существует семь FR.

a) управление идентификацией и аутентификацией (IAC);

b) контроль использования (UC);

c) целостность системы (SI);

d) конфиденциальность данных (DC);

e) ограничение потока данных (RDF);

f) своевременный отклик на события (TRE);

g) работоспособность и доступность ресурсов (RA).

Данные требования лежат в основе потенциальных SL, SL-C (система управления) систем управления. Цель и задача настоящего стандарта — определение потенциальной безопасности на уровне системы управления в противоположность целевым SL, SL-T или достигнутым SL, SL-A, которые выходят за рамки настоящего стандарта.

См. МЭК 62443-2-1, в котором представлен эквивалентный набор нетехнических, относящихся к программам потенциальных SL, необходимых для полного достижения целевого SL системы управления.

2 Нормативные ссылки

В настоящем стандарте использованы нормативные ссылки на следующие стандарты. Для датированных ссылок применяют только указанное издание ссылочного документа. Для недатированных ссылок применяют последнее издание ссылочного документа (включая все его изменения).

Издание официальное

МЭК 62443-1-1:2009 Сети промышленной коммуникации. Безопасность сетей и систем. Часть 1-1. Терминология, концепции и модели (IEC 62443-1-1:2009, «Industrial communication networks — Network and system security — Part 1-1: Terminology, concepts and models», IDT)

МЭК 62443-2-1 Сети промышленной коммуникации. Безопасность сетей и систем. Часть 2-1. Учреждение программы безопасности систем промышленной автоматизации и контроля (IEC 62443-2-1, «Industrial communication networks — Network and system security — Part 2-1: Establishing an industrial automation and control system security program», IDT)

3 Термины, определения, сокращения, допущения

3.1 Термины и определения

В настоящем стандарте применены термины и определения по МЭК 62443-1-1 и МЭК 62443-2-1, а также следующие термины с соответствующими определениями:

Примечание — Многие из нижеследующих терминов и определений изначально базируются на соответствующих источниках Международной организации по стандартизации (ИСО), Международной электротехнической комиссии (МЭК) или Национального института стандартов и технологий (NIST) (США), при этом изредка делаются незначительные поправки для лучшей применимости терминов и определений при определении требований к безопасности систем управления.

3.1.1 **имущественный объект (объект, актив)** (asset): Физический или логический объект, который представляет для IACS ощущаемую или реальную ценность.

Примечание — В настоящем стандарте имущественный объект — это любая единица, которую следует защищать в рамках системы управления безопасностью IACS.

3.1.2 **собственник объекта** (asset owner): Лицо или организация, отвечающие за один или более IACS.

Примечание 1 — Термин «собственник объекта» используется взамен родового термина «конечный пользователь» в целях их дифференциации.

Примечание 2 — Это определение распространяется на компоненты, являющиеся частью IACS.

Примечание 3 — В контексте настоящего стандарта собственник объекта включает в себя также оператора IACS.

3.1.3 **атака** (attack): Посягательство на систему, являющееся следствием рациональной угрозы.

Примечание 1 — Например, осмысленное действие, представляющее собой продуманную попытку (особенно в плане метода или стратегии) обойти сервисы безопасности и нарушить политику безопасности системы.

Примечание 2 — Существуют различные общепризнанные типы атак:

- «активная атака» имеет целью преобразовать ресурсы системы или воздействовать на их работу;

- «пассивная атака» имеет целью заполучить или использовать информацию системы без воздействия на ресурсы системы;

- «внутренняя атака» — атака, инициированная субъектом в пределах периметра безопасности («инсайдером») — т. е. субъектом, который наделен правами на получение доступа к ресурсам системы, но использует их в целях, не одобренных теми, кто предоставил эти права;

- «внешняя атака» — атака, инициированная за пределами периметра безопасности неавторизованным или неуполномоченным пользователем системы (им может быть и инсайдер, атакующий за пределами периметра безопасности). Потенциальными злоумышленниками, осуществляющими внешнюю атаку, могут быть как простые любители пошутить, так и организованные преступные группы, международные террористы и враждебные правительства.

3.1.4 **аутентификация** (authentication): Обеспечение уверенности в том, что заявляемая характеристика идентичности корректна.

Примечание — Аутентификация обычно — необходимое предварительное условие предоставления доступа к ресурсам в системе управления.

3.1.5 **аутентификатор** (authenticator): Средство, используемое для подтверждения идентичности пользователя (человека, программного процесса или устройства).

Примечание — Например, в качестве аутентификатора могут использоваться пароль или токен.

3.1.6 **аутентичность** (authenticity): Свойство соответствия субъекта тому, за кого или за что он себя выдает.

Примечание — Аутентичность обычно употребляется в контексте достоверности идентичности субъекта или правомерности передачи сообщения, самого сообщения или его источника.

3.1.7 **автоматический** (automatic): Процесс или оборудование, которые при определенных условиях функционируют без вмешательства человека.

3.1.8 **доступность** (availability): Свойство, гарантирующее своевременный и надежный доступ к информации и функциям, относящимся к системе управления, и их использование.

3.1.9 **канал связи** (communication channel): Особая линия логической или физической связи между субъектами.

Примечание — Канал облегчает установление соединения.

3.1.10 **компенсационная контрмера** (compensating countermeasure): Контрмера, применяемая взамен или в дополнение к встроенным или рекомендованным мерам безопасности для обеспечения более полного соответствия требованиям безопасности.

Примечание — Примеры включают в себя следующие компенсационные меры:

- (уровня компонентов): запертый шкафчик контроллера, не имеющий достаточно контрмер управления кибербезопасностью;

- (уровня системы управления/зоны): средства управления физическим доступом (охрана, ворота и ружья) для защиты пульта управления с целью ограничения доступа к группе известного персонала, что позволяет компенсировать техническое требование, согласно которому персонал должен уникально идентифицироваться IACS; и

- (уровня компонентов): программируемый логический контроллер (PLC) поставщика не может соответствовать характеристикам управления доступом, определенным конечным пользователем, в результате чего поставщик устанавливает межсетевой экран перед PLC и продает их как одну систему.

3.1.11 **орган нормативно-правового регулирования** (compliance authority): Субъект с правовой юрисдикцией определять корректности оценки безопасности, ее реализации или эффективности, регламентированных в руководящем документе.

3.1.12 **тракт** (conduit): Логическое объединение каналов связи, связывающее между собой две или более зоны, для которых действуют общие требования безопасности.

Примечание — Допустимо пересечение трактом зоны при условии, что эта зона не влияет на безопасность каналов, содержащихся в тракте.

3.1.13 **конфиденциальность** (confidentiality): Сохранение авторизованных ограничений на доступ и раскрытие информации, включая средства защиты неприкосновенности частной жизни и проприетарной информации.

Примечание — При употреблении в контексте IACS термин относится к защите данных и информации, относящихся к IACS, от неавторизованного доступа.

3.1.14 **соединение** (connection): Связь, установленная между двумя или более оконечными точками, которая поддерживает установление сессии.

3.1.15 **последствие** (consequence): Состояние или условие, которое является логическим или естественным следствием события.

3.1.16 **система управления** (control system): Компоненты аппаратного и программного обеспечения IACS.

3.1.17 **контрмера** (countermeasure): Действие, устройство, процедура или методика, смягчающие угрозу, уязвимость или атаку посредством их устранения или предотвращения, посредством минимизации ущерба, который они способны нанести, или посредством их обнаружения и информирования о них, чтобы могло быть предпринято корректирующее воздействие.

Примечание — В некоторых контекстах для описания этого понятия используется также термин «управление». Применительно к настоящему стандарту выбран термин «контрмера» во избежание путаницы с термином «управление» в контексте «управление процессами».

3.1.18 **режим ограниченной функциональности** (degraded mode): Режим функционирования при наличии неполадок, которые были приняты в расчет в проекте системы управления.

Примечание — Режимы ограниченной функциональности допускают дальнейшее выполнение системой управления жизненно важных функций, несмотря на снижение эффективности одного или нескольких элементов системы, например неполадки или отказ управляющего оборудования, перебои в связи из-за отказа или целенаправленного отключения системы как ответной меры против выявленной или ожидаемой угрозы безопасности подсистем.

3.1.19 **демилитаризованная зона** (demilitarized zone): Простая ограниченная сеть серверов, связывающая между собой две или более зоны в целях управления потоком данных между зонами.

Примечание — Демилитаризованные зоны (DMZ) обычно используются для исключения прямых соединений между разными зонами.

3.1.20 **устройство** (device):Объект, включающий в себя один или более процессоров, способных посылать или принимать данные/управляющие команды к другому объекту или от него.

Примечание — Примеры включают в себя контроллеры, человеко-машинные интерфейсы (HMI), PLC, пульты дистанционного управления (RTU), передатчики, исполнительные механизмы, клапаны, сетевые коммутаторы и т. д.

3.1.21 **среда** (environment): Окружение объектов, область или обстоятельства, которые могут воздействовать на функционирование IACS и/или подвергаться воздействию со стороны IACS.

3.1.22 **жизненно важная функция** (essential function): Функция или характеристика, которая требуется для поддержания охраны труда, техники безопасности, охраны окружающей среды, а также работоспособности и доступности управляемого оборудования.

Примечание — Жизненно важные функции включают в себя, но не ограничиваются этим, функцию отказа в случае возникновения опасной ситуации (SIF), функцию управления и возможность оператора отслеживать и манипулировать управляемым оборудованием. Утрата существенных функций обычно носит название утраты защиты, утраты управления и утраты отслеживаемости соответственно. В некоторых отраслях промышленности могут считаться существенными дополнительные функции, такие как архивирование.

3.1.23 **событие** (event): Появление или изменение определенного набора обстоятельств.

Примечание — В контексте системы IACS событием может быть действие, предпринятое тем или иным лицом (авторизованным или неавторизованным), изменение, обнаруженное в пределах системы управления (штатное или нештатное), или автоматический отклик со стороны самой системы управления (штатный или нештатный).

3.1.24 **пожарный вызов** (firecall): Метод, учрежденный для обеспечения аварийного доступа к защищенной системе управления.

Примечание — В аварийной ситуации непривилегированные пользователи могут получать доступ к ключевым системам для урегулирования проблемы. Если применен пожарный вызов, то обычно проводится процедура проверки того, что доступ был использован корректно для урегулирования проблемы. Эти методы в общем случае предусматривают одноразовый идентификатор (ID) пользователя или одноразовый пароль.

3.1.25 **идентификатор** (identifier): Символ, уникальный в пределах своего домена безопасности, обозначающий или используемый для заявления притязания субъекта на название или другую идентичность.

3.1.26 **идентифицировать** (identify): Операция контроля идентичности.

3.1.27 **воздействие** (impact): Оцененное последствие отдельно взятого события.

3.1.28 **инцидент** (incident):Событие, которое не является частью ожидаемого функционирования системы или сервиса и которое вызывает или может вызвать сбой или ухудшение качества сервиса, предоставляемого системой управления.

3.1.29 **система промышленной автоматики и контроля; IACS** (industrial automation and control system; IACS): Совокупность персонала, аппаратного и программного обеспечений и политик, задействованных в функционировании промышленного процесса и способных влиять или воздействовать иным образом на его защищенное, безопасное и надежное функционирование.

3.1.30 **целостность** (integrity): Свойство защиты корректности и полноты имущественных объектов.

3.1.31 **минимальная привилегия** (least privilege): Основополагающий принцип, который гласит, что пользователи (люди, программные процессы или устройства) должны по возможности наделяться минимальными привилегиями в соответствии с вмененными им обязанностями и функциями.

Примечание — Минимальная привилегия в контексте IACS обычно реализуется в виде набора ролей.

3.1.32 **мобильный код** (mobile code): Программа, передаваемая в пределах удаленной, возможно — «недоверенной», системы через сеть или съемные носители, которая может запускаться в неизменном виде на локальной системе без явной инсталляции или запуска этой программы получателем.

Примечание — Примеры мобильного кода включают в себя JavaScript, VBScript, Java-апплеты, управляющие элементы ActiveX, Flash-анимации, видеофрагменты Shockwave и макросы Microsoft Office.

3.1.33 **защита от непризнания участия** (non-repudiation): Возможность подтверждения факта заявленного события или действия и породивших его субъектов.

Примечание — Целью защиты от непризнания участия является разрешение диспутов относительно факта наличия или отсутствия события или действия и причастности к нему субъектов.

3.1.34 **производитель продукта** (product supplier): Производитель аппаратного и/или программного продукта.

Примечание — Данное понятие используется взамен обобщенного термина «поставщик» в целях их дифференциации.

3.1.35 **удаленный доступ** (remote access): Доступ к системе управления со стороны любого пользователя (человека, программного процесса или устройства), осуществляемый из (вне) периметра рассматриваемой зоны.

3.1.36 **роль** (role): Набор взаимосвязанных характеристик, привилегий и обязательств, привязанных ко всем пользователям (людям, программным процессам или устройствам) IACS.

Примечание — Привилегии на выполнение определенных операций ставятся в соответствие конкретным ролям.

3.1.37 **автоматизированная система безопасности** (safety instrumented system): Система, используемая для реализации одной или более функций технологической безопасности.

3.1.38 **уровень безопасности** (security level): Мера достоверности того, что IACS лишена уязвимостей и функционирует надлежащим образом.

Примечание — Уязвимости могут быть внесены на этапе проектирования IACS или в любой момент ее жизненного цикла либо быть следствием меняющихся угроз. Проектные уязвимости могут обнаруживаться спустя длительное время после начальной реализации IACS, например: может быть взломан алгоритм шифрования или применена некорректная политика управления учетными записями, когда, например, не удаляются старые учетные записи пользователей. Внесенные уязвимости могут возникать по вине патча или изменения в политике, которое вскрывает новую уязвимость.

3.1.39 **провайдер сервиса** (service provider): Организация (внутренняя или внешняя организация, производитель и т. д.), согласившаяся взять на себя обязательство на предоставление того или иного сервиса поддержки, а также добывание материально-технических средств в порядке соответствующего соглашения.

Примечание — Это понятие используется взамен родового термина «поставщик» в целях их дифференциации.

3.1.40 **сессия** (session): Устойчивый, интерактивный, с отслеживанием состояний, обмен информацией между двумя или более коммуникационными устройствами.

Примечание — В типичном случае сессия включает в себя четко определенные процессы начала и завершения.

3.1.41 **ID сессии** (session ID): Идентификатор, используемый для обозначения конкретного входа в сессию.

3.1.42 **уставка** (set point): Целевое значение, обозначенное внутри системы управления, которое позволяет контролировать одно или более действий в пределах системы управления.

3.1.43 **системный интегратор** (system integrator): Лицо или организация, которые специализируются на сведении воедино подсистем компонентов и обеспечении того, чтобы эти подсистемы функционировали в соответствии с проектными спецификациями.

3.1.44 **угроза** (threat): Обстоятельство или событие, способное отрицательно отразиться на процессах хозяйствования (включая задачи, функции, имидж или репутацию), объектах, системах управления или людях посредством получения несанкционированного доступа, уничтожения, раскрытия, видоизменения данных и/или отказа в обслуживании.

3.1.45 **доверие** (trust): Уверенность в том, что на операцию, источник данных, сетевой или программный процесс можно полагаться в отношении их ожидаемого функционирования.

Примечание 1 — В общем случае может считаться, что некий субъект «доверяет» второму субъекту, если делает допущение, что второй субъект будет функционировать в соответствии с ожиданиями первого субъекта.

Примечание 2 — Это доверие может быть применимо только в отношении какой-то конкретной функции.

3.1.46 **недоверенный** (untrusted): Не соответствующий заданным требованиям доверия.

Примечание — Субъект может быть просто объявлен недоверенным.

3.1.47 **зона** (zone): Совокупность логических или физических объектов, соответствующих общим требованиям безопасности.

Примечание — Зона имеет четкую границу. Политику безопасности зоны обычно составляют комбинации механизмов безопасности как на периферии зоны, так и внутри нее.

3.2 Сокращения

В настоящем стандарте применены следующие сокращения:

AES — улучшенный стандарт шифрования;

API — интерфейс программирования приложений;

ASLR — случайное размещение схем адресного пространства;

BPCS — основная система управления процессами;

CA — центр сертификации;

CIP — защита объектов жизнеобеспечения;

COTS — коммерчески доступные продукты;

CRL — перечень отзыва сертификатов;

DC — конфиденциальность данных;

DEP — предотвращение выполнения данных;

DHCP — протокол динамического конфигурирования хостов;

DMZ — демилитаризованная зона;

DNS — служба доменных имен;

DoS — отказ в обслуживании;

EICAR — Европейский институт компьютерных антивирусных исследований;

EMI — электромагнитные помехи;

FAT — заводские приемочные испытания;

FIPS — Федеральный стандарт обработки информации (NIST, США);

FR — фундаментальное требование;

FS-PLC — PLC функциональной безопасности;

FTP — протокол передачи файлов;

GLONASS — Глобальная навигационная спутниковая система (ГЛОНАСС);

GPS — система глобального позиционирования;

HMI — человеко-машинный интерфейс;

HSE — охрана труда, техника безопасности и охрана окружающей среды;

HTTP — протокол передачи гипертекста;

HTTPS — HTTP защищенный;

IAC — управление идентификацией и аутентификацией;

IACS — система(ы) промышленной автоматики и контроля;

IAMS — система управления контрольно-измерительными объектами;

ID — идентификатор;

IDS — система обнаружения несанкционированных проникновений,

IEC — Международная электротехническая комиссия (МЭК);
IEEE — Институт инженеров по электротехнике и электронике;
IETF — инженерный совет Интернета;
IM — система мгновенного обмена сообщениями;
IP — интернет-протокол;
IPS — система предотвращения несанкционированных проникновений;
ISA — Международная ассоциация автоматизации;
ISO — Международная организация по стандартизации (ИСО);
IT — информационная технология;
MES — система управления производственными процессами;
NERC — Североамериканская корпорация по обеспечению надежности электросистем;
NIST — Национальный институт стандартов и технологий (США);
NX — запрет исполнения;
OCSP — онлайновый протокол статуса сертификата;
OWASP — открытый проект обеспечения безопасности веб-приложений;
PDF — формат переносимых документов;
PKI — инфраструктура открытых ключей;
PLC — программируемый логический контроллер;
RA — работоспособность и доступность ресурсов;
RAM — оперативное запоминающее устройство;
RDF — ограничение потока данных;
RE — расширение требований;
RFC — запрос на комментарии;
RJ — стандартный телекоммуникационный интерфейс;
RTU — пульт дистанционного управления;
SAT — приемо-сдаточные испытания;
SHA — алгоритм безопасного хеширования;
SI — целостность системы;
SIEM — управление информацией о безопасности и событиями безопасности;
SIF — функция отказа в случае возникновения опасной ситуации,
SIL — уровень целостности безопасности;
SIS — автоматизированная система безопасности;
SL — уровень безопасности;
SL-A — достигнутый уровень безопасности;
SL-C — потенциальный уровень безопасности;
SL-T — целевой уровень безопасности;
SP — специальная публикация;
SR — системное требование;
SSH — безопасная оболочка;
SuC — рассматриваемая система;
TCP — протокол управления передачей;
TPM — модуль доверительной платформы;
TRE — своевременный отклик на события;
UC — контроль использования;
USB — универсальная последовательная шина;

VoIP I — P-телефония;

WEP — конфиденциальность на уровне проводных сетей;

WLAN — беспроводная локальная сеть.

3.3 Допущения

Настоящий стандарт расширяет семь FR, установленных в МЭК 62443-1-1, до серии SR. Каждое SR содержит основополагающее требование, а также может содержать одно или несколько расширений требования (RE) для ужесточения безопасности. По мере необходимости для читателя дополнительно приводятся наглядная и аргументированная методологическая основа к каждому основополагающему требованию и комментарии к любым привязанным к ним RE. Основополагающее требование и расширения RE, при их наличии, затем ставятся в соответствие одному из четырех потенциальных уровней безопасности SL-C (FR, система управления).

Все семь FR имеют определенный набор из четырех SL. Применительно к системе управления соответствие уровню 0 для отдельно взятого FR определено неявным образом как отсутствие требований. Например, постановка задачи для раздела 8, FR 4 — Конфиденциальность данных, звучит следующим образом:

Обеспечивать конфиденциальность информации на коммуникационных каналах и в хранилищах данных для предотвращения их неавторизованного раскрытия.

Соответствующие четыре SL определены как:

- SL 1 — предотвращать неавторизованное раскрытие информации посредством ее несанкционированного извлечения или случайного обнародования;
- SL 2 — предотвращать неавторизованное раскрытие информации субъекту, активно ее ищущему с использованием простых средств, при незначительных ресурсах, посредственных навыках и низкой мотиваци;
- SL 3 — предотвращать неавторизованное раскрытие информации субъекту, активно ее ищущему с использованием изощренных средств при умеренных ресурсах, наличии специальных познаний в IACS и умеренной мотивации;
- SL 4 — предотвращать неавторизованное раскрытие информации субъекту, активно ее ищущему с использованием изощренных средств при обширных ресурсах, наличии специальных познаний в IACS и высокой мотивации.

Таким образом, выдвижение отдельных SR и RE основано на ступенчатом повышении общей безопасности системы управления для данного конкретного FR.

SL-C (система управления), используемый на протяжении всего настоящего стандарта, обозначает наличие ресурсов, необходимых для соответствия конкретному SL, соотносящемуся с конкретным FR. Полное описание векторной концепции SL можно найти в приложении А.

4 Общие ограничения безопасности систем управления

4.1 Обзор

В ходе ознакомления, определения и реализации SR к системам управления, подробно раскрытых в разделах 5—11 настоящего стандарта, необходимо придерживаться ряда ограничений. Во введении настоящего стандарта приведено контекстуальное информативное описание того, что призван выполнять настоящий стандарт. В данном разделе и последующих разделах, характеризующих FR, приведен нормативный материал, необходимый для формирования расширений к существующей корпоративной безопасности, в дополнение к неукоснительным требованиям целостности и работоспособности, необходимым для IACS.

Примечание — Содержание данного раздела будет включено в МЭК 62443-1-1.

4.2 Поддержка жизненно важных функций

Как определено в 3.1.22, жизненно важная функция — это функция или возможность, необходимая для обеспечения охраны труда, техники безопасности и охраны окружающей среды, а также работоспособности и доступности управляемого оборудования.

Меры безопасности не должны отрицательно сказываться на существенных функциях IACS с высокой работоспособностью, за исключением случаев, оправданных с точки зрения оценки рисков.

Примечание — См. МЭК 62443-2-1, в котором приведены требования к документированию, относящиеся к оценке рисков, необходимой для обоснования случаев, когда меры безопасности могут отрицательно сказываться на жизненно важных функциях.

В ходе ознакомления, определения и реализации SR, описанных в настоящем стандарте, и реализации мер безопасности по возможности не должны утрачиваться защищенность, управление, возможность отслеживания или другие жизненно важные функции. После анализа рисков может оказаться, что те или иные технические средства обуславливают определенные типы мер безопасности, которые могут вызвать сбои в непрерывных процессах, однако меры безопасности не должны приводить к утрате защищенности, способной отразиться на охране труда, технике безопасности и охране окружающей среды (HSE). Вот некоторые специальные ограничения:

- меры управления доступом (IAC и UC) не должны препятствовать управлению жизненно важными функциями, а именно:
- учетные записи, используемые для жизненно важных функций, не должны блокироваться, в том числе временно (см. 5.5, SR 1.3 — Управление учетными записями, 5.6, SR 1.4 — Управление идентификаторами, 5.13, SR 1.11 — Неуспешные попытки входа в систему, и 6.7, SR 2.5 — Блокировка сессий);
- верификация и фиксация действий операторов для укрепления защиты от непризнания участия не должны вносить существенных задержек в быстродействие системы (см. 6.14, SR 2.12 — Защита от непризнания участия);
- для систем управления с высокой работоспособностью отказ Центра сертификации не должен вызывать сбои жизненно важных функций [см. 5.10, SR 1.8 — сертификаты Инфраструктуры открытых ключей (PKI)];
- идентификация и аутентификация не должны препятствовать инициации SIF (см. 5.3, SR 1.1 — Идентификация и аутентификация пользователя — физического лица, и 5.4, SR 1.2 — Идентификация и аутентификация программных процессов и устройств). То же самое относится и к контролю выполнения авторизаций (см. 6.3, SR 2.1 — Контроль выполнения авторизаций);
- записи аудитов с некорректными временными метками (см. 6.10, SR 2.8 — События, подлежащие аудиту, и 6.13, SR 2.11 — Временные метки) не должны отрицательно отражаться на жизненно важных функциях;
- жизненно важные функции IACS должны сохраняться, если защита границ зон переходит в режим закрытия при отказе и/или островной режим (см. 9.4, SR 5.2 — Защита границ зон);
- событие DoS в сети системы управления или в SIS не должно препятствовать срабатыванию SIF (см. 11.3, SR 7.1 — Защита от отказов в обслуживании).

4.3 Компенсационные контрмеры

Компенсационные контрмеры, раскрытые в настоящем стандарте, должны быть привязаны к директивам, приведенным в МЭК 62443-3-2.

В настоящем стандарте в порядке нормативов SR говорится, что «система управления должна обеспечивать возможность…» поддержания того или иного требования безопасности. Система управления должна обеспечивать возможность, но она может реализовываться с помощью внешнего компонента. В этом случае система управления должна образовывать «интерфейс» к этому внешнему компоненту. Некоторые примеры компенсационных контрмер включают в себя идентификацию пользователей (в том числе централизованную в противоположность распределенной), повышение надежности паролей, проверку достоверности подписей, выявление корреляций событий безопасности и списание устройств (сохранность информации).

Примечание 1 — Требования безопасности систем управления, детально раскрытые в настоящем стандарте, касаются всех технических функций, имеющих отношение к системе управления, включая ее инструменты и приложения. Однако, как отмечается здесь, некоторые из этих функций могут управляться посредством внешнего ресурса.

Примечание 2 — В некоторых приложениях с высокой работоспособностью и доступностью ресурсов [высоким SL-T (RA, система управления)] потребуются компенсационные контрмеры, внешние по отношению к системе управления (например, дополнительные меры физической безопасности и/или ужесточенные проверки биографических данных персонала). В этих случаях можно встретить систему управления с SL, как правило, соответ-

ствующим высокой работоспособности и доступности ресурсов, при более низких SL IAC — 1 или 2, в зависимости от компенсационных контрмер. Для системы управления с SL, соответствующим очень высокой работоспособности и доступности, вероятность блокировки или утраты управления из-за мер безопасности возрастает, а не наоборот. Таким образом, высокие SL не всегда «лучше», даже если расходы не являются существенным фактором.

4.4 Минимальная привилегия

Должна быть предусмотрена возможность укрепления концепции минимальной привилегии, с ранжированием полномочий и гибкостью соотнесения этих полномочий с ролями, достаточной для ее поддержания.

5 FR 1 — Управление идентификацией и аутентификацией

5.1 Назначение и описания SL-C(IAC)

Идентифицировать и аутентифицировать всех пользователей (людей, программные процессы и устройства) перед предоставлением им доступа к системе управления:

- SL 1 — идентифицировать и аутентифицировать всех пользователей (людей, программные процессы и устройства) посредством механизмов, которые препятствуют осуществлению случайного или непредумышленного доступа неаутентифицированными субъектами;
- SL 2 — идентифицировать и аутентифицировать всех пользователей (людей, программные процессы и устройства) посредством механизмов, которые препятствуют осуществлению умышленного неаутентифицированного доступа субъектами с использованием простых средств, при незначительных ресурсах, посредственных навыках и низкой мотивации,
- SL 3 — идентифицировать и аутентифицировать всех пользователей (людей, программные процессы и устройства) посредством механизмов, которые препятствуют осуществлению умышленного неаутентифицированного доступа субъектами с использованием изощренных средств, при умеренных ресурсах, наличии специальных познаний в IACS и умеренной мотивации;
- SL 4 — идентифицировать и аутентифицировать всех пользователей (людей, программные процессы и устройства) посредством механизмов, которые препятствуют осуществлению умышленного неаутентифицированного доступа субъектами с использованием изощренных средств, при обширных ресурсах, наличии специальных познаний в IACS и высокой мотивации.

5.2 Целесообразность

Собственники имущественных объектов должны будут разрабатывать перечень всех пользователей (людей, программных процессов и устройств) и определять для каждого компонента систем управления требуемый уровень защиты посредством IAC. Функция IAC — защита системы управления посредством верификации идентичности любого пользователя, запрашивающего доступ к системе управления до инициации коммуникации. Рекомендации и директивы должны по возможности затрагивать механизмы, которые будут функционировать в смешанных режимах. Например, одни компоненты системы управления требуют усиленного IAC, например усиленных механизмов аутентификации, а другие — нет.

5.3 SR 1.1 — Идентификация и аутентификация пользователя — физического лица

5.3.1 Требование

Система управления должна обеспечивать возможность идентификации и аутентификации всех пользователей — физических лиц. Эта возможность должна навязывать такую идентификацию и аутентификацию на всех интерфейсах, которые обеспечивают доступ людей-пользователей к системе управления, с поддержанием ранжирования обязанностей и минимальной привилегии в соответствии с применимыми политиками и регламентами безопасности.

5.3.2 Целесообразность и дополнительная методологическая основа

Все пользователи — физические лица должны проходить идентификацию и аутентификацию для осуществления любого доступа к системе управления. Аутентификация идентичности этих пользователей должна по возможности осуществляться посредством таких методов, как пароли, токены, биометрические признаки, или, в случае многофакторной аутентификации, той или иной их комбинации.

Географическое местонахождение пользователей — физических лиц также может использоваться в рамках процесса аутентификации. Это требование должно быть по возможности применимо и к локальному, и к удаленному доступу к системе управления. Помимо идентификации и аутентификации всех пользователей — физических лиц на уровне системы управления (например, при регистрации на входе в систему), механизмы идентификации и аутентификации часто применяются на уровне приложения.

Там, где пользователи — физические лица действуют как единая группа (например, операторы пульта управления), идентификация и аутентификация пользователей может быть проведена на основе ролей или групп. Применительно к некоторым системам управления критически важна возможность беспрепятственного взаимодействия между операторами. Жизненно важно, чтобы требования идентификации или аутентификации не затрудняли локальных действий в чрезвычайных ситуациях, а также не вносили ограничений в жизненно важные функции системы управления (см. раздел 4 для получения более полных сведений). Доступ к этим системам может быть сдержан соответствующими механизмами физической безопасности (см. МЭК 62443-2-1). Примером такой ситуации служит пульт управления в критических режимах, где действуют строгий контроль и мониторинг физического доступа и, в соответствии с планами работы на рабочую смену, ответственность распределяется между той и иной группой пользователей. Эти пользователи затем могут использовать персоналии одного и того же пользователя. Кроме того, по возможности должны проходить аутентификацию клиенты выделенных рабочих станций операторов (см. 5.4, SR 1.2 — Идентификация и аутентификация программных процессов и устройств), или использование этой разделенной учетной записи должно быть по возможности ограничено средой пульта управления.

Для поддержания политик IAC, как определено в МЭК 62443-2-1, система управления в качестве первого этапа верифицирует идентичность всех пользователей — физических лиц. На втором этапе вводятся в действие полномочия, закрепленные за идентифицированным пользователем — физическим лицом (см. 6.3, SR 2.1 — Обязательная авторизация).

5.3.3 Расширения требований

5.3.3.1 SR 1.1 RE1 — Уникальная идентификация и аутентификация

Система управления должна обеспечивать возможность уникальной идентификации и аутентификации всех пользователей — физических лиц.

5.3.3.2 SR 1.1 RE2 — Многофакторная аутентификация для недоверенных сетей

Система управления должна обеспечивать возможность применения многофакторной аутентификации для осуществления доступа пользователей — физических лиц к системе управления через недоверенную сеть (см. 5.15, SR 1.13 — Доступ через недоверенные сети).

Примечание — См. 5.7.3.5.7.3.1, SR 1.5 — Управление аутентификаторами, RE5.7.3.1 относительно расширенного управления аутентификаторами для программных процессов.

5.3.3.3 SR 1.1 RE3 — Многофакторная аутентификация для всех сетей

Система управления должна обеспечивать возможность применения многофакторной аутентификации для осуществления доступа всех пользователей — физических лиц к системе управления.

5.3.4 Уровни безопасности

Ниже приведены требования к четырем уровням SL, относящимся к SR 1.1 — Идентификация и аутентификация людей-пользователей:

- SL-C (IAC, система управления) 1: SR 1.1;
- SL-C (IAC, система управления) 2: SR 1.1 (1);
- SL-C (IAC, система управления) 3: SR 1.1 (1) (2);
- SL-C (IAC, система управления) 4: SR 1.1 (1) (2) (3).

5.4 SR 1.2 — Идентификация и аутентификация программных процессов и устройств

5.4.1 Требование

Система управления должна обеспечивать возможность идентификации и аутентификации всех программных процессов и устройств. Эта возможность должна налагать такую идентификацию и аутентификацию на всех интерфейсах, которые обеспечивают доступ к системе управления с поддержанием минимальной привилегии в соответствии с применимыми политиками и регламентами безопасности.

5.4.2 Целесообразность и дополнительная методологическая основа

Функция идентификации и аутентификации — присвоение ID неизвестному программному процессу или устройству (далее в этом подпункте упоминаются как субъект) для его выявления перед санкционированием любого обмена данными. Если допустить отправку и получение неподконтроль-

ными субъектами данных, относящихся к системам управления, то можно спровоцировать нештатное поведение легитимной системы управления.

Все субъекты должны быть идентифицированы и аутентифицированы при получении любого доступа к системе управления. Аутентификация идентичности таких субъектов должна по возможности осуществляться с использованием таких методов, как пароли, токены или местонахождение (физическое или логическое). Это требование должно быть по возможности применимо и к локальному, и к удаленному доступу к системе управления. Однако в некоторых сценариях, когда одиночные субъекты используются в подключении к различным конечным системам (например, к удаленной поддержке поставщиков), может быть технически невозможно присвоить одному субъекту более одной персоналии. В этих случаях должны применяться компенсационные контрмеры.

Механизмы идентификации и аутентификации всех субъектов необходимы для обеспечения защиты от атак, таких как «человек посередине» или спуфинг сообщений. В некоторых случаях эти механизмы могут затрагивать более одного программного процесса, функционирующего на одном и том же физическом сервере, причем каждый процесс имеет свою собственную идентичность. В других случаях идентичность может быть привязана к физическому устройству, например когда все процессы функционируют на некотором конкретном PLC.

Следует уделять особое внимание идентификации и аутентификации портативных и подвижных устройств. Устройства этого типа являют собой известный способ внесения нежелательного сетевого трафика, вредоносного программного обеспечения и/или раскрытия информации, относящейся к системам управления, включая изолированные в обычных случаях сети.

Там, где субъекты действуют как единая группа, идентификация и аутентификация могут быть на основе ролей, групп или субъектов, при этом жизненно важно, чтобы требования идентификации или аутентификации не ограничивали локальные действия в чрезвычайных ситуациях, а также жизненно важные функции систем управления (см. раздел 4 для получения более полных сведений). Например, в рамках общих схем защиты и управления устройства из некой группы совместно исполняют функции защиты и осуществляют коммуникацию многоадресными сообщениями между устройствами в составе группы. В этих случаях обычно используется групповая аутентификация на основе разделенных учетных записей или разделенных симметричных ключей.

Для того чтобы поддерживать политики управления идентификацией и аутентификацией, как определено в соответствии с МЭК 62443-2-1, система управления в качестве первого этапа верифицирует идентичность всех субъектов. На втором этапе с субъектом ассоциируются полномочия, вмененные идентифицированному субъекту (см. 6.3, SR 2.1 — Обязательная авторизация).

5.4.3 Расширения требований

5.4.3.1 SR 1.2 RE1 — Уникальная идентификация и аутентификация

Система управления должна обеспечивать возможность уникальной идентификации и аутентификации всех программных процессов и устройств.

5.4.3.2 Пусто

5.4.4 Уровни безопасности

Далее приведены требования для уровней SL, относящихся к SR 1.2 — Идентификация и аутентификация программных процессов и устройств:

- SL-C (IAC, система управления) 1: не определены;
- SL-C (IAC, система управления) 2: SR 1.2;
- SL-C (IAC, система управления) 3: SR 1.2 (1);
- SL-C (IAC, система управления) 4: SR 1.2 (1).

5.5 SR 1.3 — Управление учетными записями

5.5.1 Требование

Система управления должна обеспечивать возможность управления всеми учетными записями авторизованных пользователей, включая добавление, активацию, изменение, деактивацию и удаление учетных записей.

5.5.2 Целесообразность и дополнительная методологическая основа

Управление учетными записями может включать в себя группировку учетных записей (например, индивидуальную, на основе ролей, устройств и в привязке к системам управления), учреждение условий для членства в группах и присвоение соответствующих авторизаций. В определенных случаях, когда индивидуальные учетные записи применительно к IACS определены как ненужные в аспекте ана-

лиза рисков и/или регламентного регулирования, допустимы разделенные учетные записи при условии, что документированы и действенны адекватные компенсационные контрмеры (например, ограниченный физический доступ или организационные меры для подтверждения).

Для учетных записей, не относящихся к пользователям — физическим лицам, иногда обозначаемых как учетные записи сервисов и применяемых для программной коммуникации процесс — процесс (например, между сервером управления и сервером-архиватором и между PLC и сервером управления), обычно необходимы политики и регламенты безопасности, отличные от таковых для учетных записей пользователей — физических лиц. Для повышения безопасности управление учетными записями следует осуществлять в соответствии с унифицированными политиками и применять локально к соответствующим компонентам системы управления. Если учетные записи, установленные по умолчанию, были использованы при первой инсталляции системы и больше не используются, то такие учетные записи должны по возможности быть удаляемыми. Повышение безопасности заключается в упрощении и последовательном применении управления учетными записями.

5.5.3 Расширения требований

5.5.3.1 SR 1.3 RE1 — Унифицированное управление учетными записями

Система управления должна обеспечивать возможность унифицированного управления учетными записями.

5.5.3.2 Пусто

5.5.4 Уровни безопасности

Далее приведены требования для уровней SL, относящихся к SR 1.3 — Управление учетными записями:

- SL-C (IAC, система управления) 1: SR 1.3;
- SL-C (IAC, система управления) 2: SR 1.3;
- SL-C (IAC, система управления) 3: SR 1.3 (1);
- SL-C (IAC, система управления) 4: SR 1.3 (1).

5.6 SR 1.4 — Управление идентификаторами

5.6.1 Требование

Система управления должна обеспечивать возможность управления идентификаторами посредством интерфейса пользователей, групп, ролей или систем управления.

5.6.2 Целесообразность и дополнительная методологическая основа

Идентификаторы следует отличать от привилегий, действие которых они санкционируют для субъекта в пределах управляющего домена или зоны конкретной системы управления (см. 6.3, SR 2.1 — Обязательная авторизация). Там, где пользователи — физические лица действуют как единая группа (например, операторы пульта управления), идентификация пользователей может быть на основе ролей, групп или устройств. Применительно к некоторым системам управления критически важна возможность беспрепятственного взаимодействия между операторами. Требования идентификации не должны ограничивать локальные действия в чрезвычайных ситуациях применительно к системе управления. Доступ к этим системам может быть сдержан соответствующими компенсационными контрмерами. Идентификаторы могут требоваться на участках системы управления, но не обязательно во всей системе управления. Например, беспроводные устройства обычно требуют идентификаторов, в то время как проводные устройства могут их и не требовать.

Управление идентификаторами будет определено локальными политиками и регламентами, учрежденными в соответствии с МЭК 62443-2-1.

5.6.3 Расширения требований

Отсутствуют.

5.6.4 Уровни безопасности

Далее приведены требования для уровней SL, относящихся к SR 1.4 — Управление идентификаторами:

- SL-C (IAC, система управления) 1: SR 1.4;
- SL-C (IAC, система управления) 2: SR 1.4;
- SL-C (IAC, система управления) 3: SR 1.4;
- SL-C (IAC, система управления) 4: SR 1.4.

5.7 SR 1.5 — Управление аутентификаторами

5.7.1 Требование

Система управления должна обеспечивать возможность:

a) инициализации содержания аутентификатора;

b) изменения всех аутентификаторов, заданных по умолчанию, после инсталляции системы управления;

c) изменения/обновления всех аутентификаторов; и

d) защиты всех аутентификаторов от неавторизованного раскрытия и изменения в ходе их ввода и передачи.

5.7.2 Целесообразность и дополнительная методологическая основа

Наряду с идентификатором (см. 5.6, SR 1.4 — Управление идентификаторами) аутентификатор необходим для подтверждения идентичности. Аутентификаторы систем управления включают в себя, но не ограничиваются этим, токены, симметричные ключи, секретные ключи (часть пары из открытого/секретного ключа), биометрические признаки, пароли, физические ключи и карточки с ключом. Пользователи — физические лица должны по возможности принимать разумные меры для обеспечения безопасности аутентификаторов, в том числе хранить при себе личные аутентификаторы, не одалживать и не использовать аутентификаторы совместно и немедленно сообщать об утрате или нарушении безопасности аутентификаторов.

Аутентификаторы имеют жизненный цикл. Когда создается учетная запись, то автоматически должен быть создан новый аутентификатор, чтобы можно было аутентифицировать держателя учетной записи. Например, в системе на основе паролей учетная запись содержит привязанный к ней пароль. Определение начального содержания аутентификатора может быть интерпретировано как определение администратором начального пароля, который система управления учетными записями устанавливает для всех новых учетных записей. Возможность конфигурации этих начальных символов усложняет для злоумышленника разгадывание пароля, установленного между созданием учетной записи и первым использованием учетной записи (что должно предполагать задание нового пароля держателем учетной записи). Некоторые системы управления инсталлируются с помощью автоматических инсталляторов, которые создают все необходимые учетные записи с паролями, устанавливаемыми по умолчанию, а некоторые встраиваемые устройства поставляются с паролями, установленными по умолчанию. Зачастую со временем эти пароли становятся всеобщим достоянием и фиксируются в Интернете. Возможность изменения паролей, оставленных по умолчанию, позволяет защитить систему от неавторизованных пользователей, которые используют пароли, оставленные по умолчанию, для получения доступа. Пароли могут быть заполучены из памяти данных или в ходе передачи данных в процессе сетевой аутентификации. Сложность этого может быть повышена посредством криптографических защит, например шифрования или хеширования, или протоколов квитирования, которые не требуют передачи пароля вообще. И все же пароли могут быть объектом атак, например, подбором методом полного перебора (методом «грубой силы») или взломом криптографической защиты паролей в момент их передачи или хранения. Окно возможности можно сузить посредством периодической смены/обновления паролей. Аналогичные соображения применимы к системам аутентификации на основе криптографических ключей. Можно добиться улучшенной защиты посредством аппаратных механизмов, например аппаратных модулей безопасности, таких как доверенные платформенные модули (TPM).

Управление аутентификаторами следует подробно документировать в действующих политиках и регламентах безопасности, например с указанием ограничений на изменение аутентификаторов, установленных по умолчанию, периодичности обновлений, детализацией защиты аутентификаторов или процедур пожарных вызовов (см. 3.1.24).

Блокирование или утрата управления вследствие мер безопасности недопустимы. Если система управления должна иметь высокий уровень работоспособности и доступности, то следует принять меры по поддержанию этого высокого уровня работоспособности и доступности (например, компенсационные физические контрмеры, дублирование ключей и обеспечение приоритетности диспетчерского управления).

Надежность механизма аутентификации зависит не только от характеристик управления аутентификаторами, определенных в настоящем требовании, но и от надежности выбранного аутентификатора (например, сложности пароля или длины ключа при аутентификации по открытому ключу) и политик валидации аутентификатора в процессе аутентификации (например, длительности действия пароля или проверок, выполняемых при валидации сертификата открытого ключа). Для наиболее простых механизмов

аутентификации аутентификация по паролю и открытому ключу (5.9, SR 1.7 — Надежность аутентификации по паролю, 5.10, SR 1.8 — Сертификаты инфраструктуры открытых ключей (PKI), и 5.11, SR 1.9 — Надежность аутентификации по открытому ключу) предусматривает дополнительные требования.

5.7.3 Расширения требований

5.7.3.1 SR 1.5 RE1 — Аппаратная безопасность для регистрационных данных идентичности программных процессов

Для пользователей программных процессов и устройств система управления должна обеспечивать возможность защиты значимых аутентификаторов посредством аппаратных механизмов.

5.7.3.2 Пусто

5.7.4 Уровни безопасности

Далее приведены требования для уровней SL, относящихся к SR 1.5 — Управление аутентификаторами:

- SL-C (IAC, система управления) 1: SR 1.5;
- SL-C (IAC, система управления) 2: SR 1.5;
- SL-C (IAC, система управления) 3: SR 1.5 (1);
- SL-C (IAC, система управления) 4: SR 1.5 (1).

5.8 SR 1.6 — Управление беспроводным доступом

5.8.1 Требование

Система управления должна обеспечивать возможность идентификации и аутентификации всех пользователей (физических лиц, программных процессов или устройств), участвующих в беспроводной коммуникации.

5.8.2 Целесообразность и дополнительная методологическая основа

Любую беспроводную технологию можно и в большинстве случаев следует рассматривать как очередную опцию протокола передачи данных, а значит, подчиняющуюся тем же требованиям безопасности IACS, что и любой другой тип коммуникации, используемой IACS. Однако с точки зрения безопасности имеется по меньшей мере одно существенное различие между проводными и беспроводными коммуникациями: контрмеры физической безопасности обычно менее эффективны при использовании беспроводной связи. По этой и, возможно, другим причинам (например, различиям в регламентном регулировании) анализ рисков может естественным образом обусловить более высокий SL-T(IAC, система управления) для беспроводных коммуникаций в противоположность SL-T для проводных протоколов, используемых в идентичных случаях.

Беспроводные технологии включают в себя, но не ограничиваются этим, микроволновую, спутниковую связь, пакетную радиосвязь, технологии Института инженеров по электротехнике и электронике (IEEE) — IEEE 802.11x, IEEE 802.15.4 (ZigBee, МЭК 62591 — WirelessHART®, ISA-100.11a), IEEE 802.15.1 (Bluetooth), мобильные маршрутизаторы беспроводных ЛВС, мобильные телефоны с тетерингом и различные технологии связи в инфракрасном диапазоне.

5.8.3 Расширения требований

5.8.3.1 SR 1.6 RE1 — Уникальная идентификация и аутентификация

Система управления должна обеспечивать возможность уникальной идентификации и аутентификации всех пользователей (физических лиц, программных процессов или устройств), участвующих в беспроводной коммуникации.

5.8.3.2 Пусто

5.8.4 Уровни безопасности

Далее приведены требования для уровней SL, относящихся к SR 1.6 — Управление беспроводным доступом:

- SL-C (IAC, система управления) 1: SR 1.6;
- SL-C (IAC, система управления) 2: SR 1.6 (1);
- SL-C (IAC, система управления) 3: SR 1.6 (1);
- SL-C (IAC, система управления) 4: SR 1.6 (1).

5.9 SR 1.7 — Надежность аутентификации по паролю

5.9.1 Требование

Применительно к системам управления, использующим аутентификацию по паролю, система управления должна обеспечивать возможность повышения надежности конфигурируемых паролей на основе минимальной длины и разнотипности символов.

5.9.2 Целесообразность и дополнительная методологическая основа

Аутентификация пользователей по имени пользователя и секретному паролю — весьма распространенный механизм. Многие атаки на такие механизмы нацелены на разгадывание пароля (например, атаки перебором по словарю или целенаправленная социальная инженерия) или взлом криптографической защиты отображения хранимого пароля (например, посредством радужных таблиц или грубого подбора хеш-коллизии).

Увеличение размера набора действительных паролей за счет увеличения количества допустимых символов затрудняет такие атаки, но лишь в том случае, если увеличенный размер набора действительно используется (обычно пользователи не склонны включать в состав пароля специальные символы, поскольку они сложны для восприятия и труднее запоминаются). Ограничение срока действия пароля сужает окно возможности для злоумышленника в плане выявления секрета, лежащего в основе отдельно взятого пароля. Для того чтобы пользователи не могли обойти эту директиву, сменив однажды свой пароль на новый и затем сразу же заменив его прежним, обычно, помимо всего прочего, устанавливается минимальный срок действия пароля. Уведомление о необходимости смены пароля до истечения срока его действия позволяет пользователю сменить пароль в удобное время с учетом рабочей обстановки.

Эта защита может быть дополнительно усилена посредством ограничения повторного использования паролей (запрещения малых наборов чередующихся паролей), что дополнительно снижает практическую пользу однократно взломанного пароля. Многофакторная аутентификация позволяет добиться дополнительной защиты, выходящей за рамки механизмов на основе паролей (см. 5.3, SR 1.1 — Идентификация и аутентификация пользователей — физических лиц, и 5.4, SR 1.2 — Идентификация и аутентификация программных процессов и устройств).

5.9.3 Расширения требований

5.9.3.1 SR 1.7 RE1 — Ограничения на генерацию паролей и сроки их действия для пользователей — физических лиц

Система управления должна обеспечивать возможность предотвращения повторного использования пароля учетной записью любого отдельно взятого пользователя — физического лица для конфигурируемого числа генераций. Кроме того, система управления должна обеспечивать возможность установления ограничений минимального и максимального сроков действия паролей для пользователей — физических лиц.

Эти возможности должны согласовываться с общепринятыми практиками индустрии безопасности.

Примечание — В соответствии с общепринятой практикой система управления обеспечивает возможность напоминания пользователю о смене пароля через конфигурируемый период времени до истечения срока его действия.

5.9.3.2 SR 1.7 RE2 — Ограничения сроков действия паролей для всех пользователей

Система управления должна обеспечивать возможность установления ограничений минимального и максимального сроков действия паролей для всех пользователей.

5.9.4 Уровни безопасности

Далее приведены требования для уровней SL, относящихся к SR 1.7 — Надежность аутентификации по паролю:

- SL-C (IAC, система управления) 1: SR 1.7;
- SL-C (IAC, система управления) 2: SR 1.7;
- SL-C (IAC, система управления) 3: SR 1.7 (1);
- SL-C (IAC, система управления) 4: SR 1.7 (1) (2).

5.10 SR 1.8 — Сертификаты инфраструктуры открытых ключей (PKI)

5.10.1 Требование

Там, где применяется PKI, система управления должна обеспечивать возможность задействовать PKI в соответствии с общепринятыми передовыми практиками или получения сертификатов открытых ключей от существующей PKI.

5.10.2 Целесообразность и дополнительная методологическая основа

Регистрация для получения сертификата открытого ключа должна включать в себя авторизацию диспетчера или ответственного должностного лица и осуществляться посредством надежной технологии, в рамках которой верифицируется идентичность держателя сертификата и обеспечивается выдача

сертификата надлежащей стороне. Любые задержки, спровоцированные использованием сертификатов открытых ключей, по возможности не должны ухудшать эксплуатационные характеристики системы управления.

Выбор подходящей PKI должен по возможности учитывать сертификационную политику организаций, которая должна по возможности базироваться на риске, соотносящемся с уязвимостью в конфиденциальности защищаемой информации. Методологическую основу к определению политики можно найти в общепризнанных стандартах и директивах, например в Запросе на комментарии (RFC) 3647 [29] Инженерного совета Интернета (IETF) для PKI на основе X.509. Например, соответствующее местонахождение центра сертификации (CA), будь то в пределах системы управления или в Интернете, и перечень доверенных CA должны по возможности быть учтены в политике и зависят от архитектуры сети (см. также МЭК 62443-2-1).

5.10.3 Расширения требований

Отсутствуют.

5.10.4 Уровни безопасности

Далее приведены требования для уровней SL, относящихся к SR 1.8 — Сертификаты инфраструктуры открытых ключей (PKI):

- SL-C (IAC, система управления) 1: не определены;
- SL-C (IAC, система управления) 2: SR 1.8;
- SL-C (IAC, система управления) 3: SR 1.8;
- SL-C (IAC, система управления) 4: SR 1.8.

5.11 SR 1.9 — Надежность аутентификации по открытому ключу

5.11.1 Требование

Применительно к системам управления, использующим аутентификацию по открытому ключу, система управления должна обеспечивать возможность:

a) валидации сертификатов посредством проверки действительности подписи того или иного сертификата;

b) валидации сертификатов посредством создания пути сертификации к общепризнанному CA или, в случае самозаверенных сертификатов, посредством проверки «листовых» сертификатов ко всем хостам, поддерживающим коммуникацию с субъектом, для которого выдан сертификат;

c) валидации сертификатов посредством проверки того или иного сертификата на предмет аннулированности;

d) учреждения контроля со стороны пользователя (физического лица, программного процесса или устройства) за соответствующим секретным ключом; и

e) присвоения аутентифицированной идентичности пользователю (физическому лицу, программному процессу или устройству).

5.11.2 Целесообразность и дополнительная методологическая основа

Криптография на открытом/частном ключе строго привязана к секрету частного ключа отдельно взятого субъекта и корректному ведению доверительных отношений. При верификации доверия между двумя субъектами на основе аутентификации по открытому ключу жизненно важно приписать сертификат частного ключа доверенному субъекту. Типичная погрешность реализации при валидации сертификатов — проверять только истинность подписи сертификата и не удостоверять доверие к подписавшемуся. В системе PKI подписавшийся является доверенным, если он представляет доверенный CA или имеет сертификат, выданный доверенным CA, поэтому все проверяющие должны идентифицировать предъявляемые им сертификаты опять же в доверенном CA. Если такая цепочка из доверенных CA не может быть зафиксирована, то представленный сертификат следует считать недоверенным.

Если вместо сертификатов PKI используются самозаверенные сертификаты, то субъект, предъявивший сертификат, сам его подписывал, а значит, доверенной третьей стороны или CA не существует вообще. Это следует компенсировать посредством наделения самозаверенными сертификатами на открытом ключе всех партнеров, которые должны удостоверить их истинность посредством защищенного иным образом механизма (например, сбора всех партнеров в доверенной обстановке). Доверенные сертификаты должны быть распределены между партнерами через защищенные каналы. В ходе проверки самозаверенный сертификат по возможности должен быть признан доверенным только тогда, когда он уже имеется в перечне доверенных сертификатов проверяющего партнера. Набор из доверенных сертификатов должен по возможности быть сконфигурирован до минимального необходимого набора.

В обоих случаях валидация должна допускать также возможность того, что сертификат недействительный. В системе PKI это обычно делается посредством ведения списков аннулированных сертификатов (CRL) или использования сервера онлайнового протокола статуса сертификата (OCSP). В случае если проверка на предмет аннулированности не доступна в силу ограничений со стороны системы управления, то такие механизмы, как укороченный срок действия сертификата, могут компенсировать отсутствие актуальной информации об аннулировании. Следует отметить, что сертификаты с укороченным сроком действия могут иногда создавать существенные проблемы эксплуатации в среде системы управления.

5.11.3 Расширения требований

5.11.3.1 SR 1.9 RE1 — Безопасность аппаратного обеспечения при аутентификации по открытому ключу

Система управления должна обеспечивать возможность защиты соответствующих частных ключей посредством аппаратных механизмов в соответствии с общепризнанными практиками и рекомендациями индустрии безопасности.

5.11.3.2 Пусто

5.11.4 Уровни безопасности

Далее приведены требования для уровней SL, относящихся к SR 1.9 — Надежность аутентификации по открытому ключу:

- SL-C (IAC, система управления) 1: не определены;
- SL-C (IAC, система управления) 2: SR 1.9;
- SL-C (IAC, система управления) 3: SR 1.9 (1);
- SL-C (IAC, система управления) 4: SR 1.9 (1).

5.12 SR 1.10 — Обратная связь при аутентификации

5.12.1 Требование

Система управления должна обеспечивать возможность сокрытия обратной связи в передаче аутентификационной информации в процессе аутентификации.

5.12.2 Целесообразность и дополнительная методологическая основа

Сокрытие обратной связи препятствует возможному использованию информации неавторизованными лицами; например, отображение звездочек или других случайных символов, когда пользователь — физическое лицо печатает пароль, скрывает обратную связь в передаче аутентификационной информации. Другие примеры включают в себя ввод ключей по алгоритму WEP, ввод токена по протоколу безопасной оболочки (SSH) и одноразовые пароли по RSA. Аутентифицирующий субъект по возможности не должен давать какие-либо подсказки, например, в случае неудачной аутентификации, такие как «неизвестное имя пользователя».

5.12.3 Расширения требований

Отсутствуют.

5.12.4 Уровни безопасности

Далее приведены требования для уровней SL, относящихся к SR 1.10 — Обратная связь при аутентификации:

- SL-C (IAC, система управления) 1: SR 1.10;
- SL-C (IAC, система управления) 2: SR 1.10;
- SL-C (IAC, система управления) 3: SR 1.10;
- SL-C (IAC, система управления) 4: SR 1.10.

5.13 SR 1.11 — Неудачные попытки входа в систему

5.13.1 Требование

Система управления должна обеспечивать возможность установки предела конфигурируемого числа последовательных неудачных попыток получения доступа любым пользователем (физическим лицом, программным процессом или устройством) в течение конфигурируемого промежутка времени. Система управления должна обеспечивать возможность отказа в доступе на заданный промежуток времени или до разблокирования доступа администратором, когда этот предел превышен.

Применительно к учетным записям системы, под которыми функционируют критически важные сервисы или серверы, система управления должна обеспечивать возможность запрещения диалоговых входов в систему.

5.13.2 Целесообразность и дополнительная методологическая основа

В силу возможности отказа в доступе число последовательных неудачных попыток получения доступа может быть ограничено. Если это разрешено, система управления может автоматически обнулять число попыток получения доступа через заданный промежуток времени, устанавливаемый действующими политиками и регламентами безопасности. Обнуление попыток получения доступа позволит получать доступ пользователям (физическим лицам, программным процессам или устройствам), если они владеют корректным идентификатором для входа в систему. Не следует применять автоматический отказ в доступе для рабочих станций операторов или узлов систем управления, если требуются незамедлительные ответные действия операторов в аварийных ситуациях. Все механизмы блокирования должны по возможности учитывать функциональные требования непрерывности процессов, чтобы можно было минимизировать неблагоприятные эксплуатационные условия при отказе в доступе, которые могут привести к полному отказу системы или травматизму персонала. Если допустить возможность диалогового входа в систему применительно к учетной записи, используемой для критически важных сервисов, то можно спровоцировать тенденцию отказов в сервисах или других неблагоприятных последствий из-за неправильного обращения с системой.

5.13.3 Расширения требований

Отсутствуют.

5.13.4 Уровни безопасности

Далее приведены требования для уровней SL, относящихся к SR 1.11 — Неудачные попытки получения доступа:

- SL-C (IAC, система управления) 1: SR 1.11;
- SL-C (IAC, система управления) 2: SR 1.11;
- SL-C (IAC, система управления) 3: SR 1.11;
- SL-C (IAC, система управления) 4: SR 1.11.

5.14 SR 1.12 — Уведомление об использовании системы

5.14.1 Требование

Система управления должна обеспечивать возможность отображения перед аутентификацией уведомительного сообщения об использовании системы. Уведомительное сообщение об использовании системы должно предусматривать его конфигурирование авторизованным персоналом.

5.14.2 Целесообразность и дополнительная методологическая основа

Политики и регламенты приватности и безопасности должны согласовываться с действующими законодательными нормами, директивами, политиками, регламентными нормами, стандартами и методологическими основами. Зачастую главным аргументом в пользу этого требования является судебное преследование злоумышленников и доказательство умышленного нарушения. Таким образом, эта характеристика необходима для соответствия требованиям политик, но не улучшает безопасность IACS. Уведомительные сообщения об использовании системы могут быть реализованы в виде предупредительных баннеров, отображаемых при входе пользователей — физических лиц в систему управления. Предупредительный баннер в виде физического уведомления, вывешенного на оборудовании системы управления, не устраняет проблем, связанных с удаленным входом в систему.

Далее перечислены примеры элементов, подлежащих включению в уведомительное сообщение об использовании системы:

a) то, что пользователь получает доступ к специализированной системе управления;

b) то, что использование системы может отслеживаться, фиксироваться и подвергаться аудиту;

c) то, что несанкционированное использование системы запрещено и влечет уголовные и/или административные санкции; и

d) то, что использование системы означает согласие на мониторинг и фиксацию.

5.14.3 Расширения требований

Отсутствуют.

5.14.4 Уровни безопасности

Далее приведены требования для уровней SL, относящихся к SR 1.12 — Уведомление об использовании системы:

- SL-C (IAC, система управления) 1: SR 1.12;
- SL-C (IAC, система управления) 2: SR 1.12;
- SL-C (IAC, система управления) 3: SR 1.12;
- SL-C (IAC, система управления) 4: SR 1.12.

5.15 SR 1.13 — Доступ через недоверенные сети

5.15.1 Требование

Система управления должна обеспечивать возможность отслеживания и контроля всех способов получения доступа к системе управления через недоверенные сети.

5.15.2 Целесообразность и дополнительная методологическая основа

Примеры получения доступа к системе управления через недоверенные сети обычно включают в себя методы получения удаленного доступа (такие, как вызов по номеру, получение широкополосного доступа и беспроводного доступа), а также установление соединений из корпоративной сети (не относящейся к системам управления) организации. Система управления должна по возможности ограничивать доступ, устанавливаемый через коммутируемые соединения (например, ограничивать доступ исходя из вида источника запроса), а также предотвращать установление неавторизованных соединений или разрыв авторизованных соединений (например, посредством технологии виртуальных частных сетей). Получение доступа через недоверенные сети к географически удаленным участкам с компонентами систем управления (например, к центрам управления и промежуточным станциям) должно по возможности быть санкционировано только тогда, когда этот доступ необходим и аутентифицирован. Политики и регламенты безопасности могут требовать многофакторную аутентификацию для предоставления удаленного доступа пользователям к системе управления.

5.15.3 Расширения требований

5.15.3.1 SR 1.13 RE1 — Принятие явного запроса на доступ

Система управления должна обеспечивать возможность отклонения запросов на доступ через недоверенные сети, если только это не допустимо в рамках установленной роли.

5.15.3.2 Пусто

5.15.4 Уровни безопасности

Далее приведены требования для уровней SL, относящихся к SR 1.13 — Доступ через недоверенные сети:

- SL-C (IAC, система управления) 1: SR 1.13;
- SL-C (IAC, система управления) 2: SR 1.13 (1);
- SL-C (IAC, система управления) 3: SR 1.13 (1);
- SL-C (IAC, система управления) 4: SR 1.13 (1).

6 FR 2 — Контроль использования

6.1 Назначение и описания SL-C(UC)

Контролировать соблюдение привилегий, закрепленных за аутентифицированным пользователем (физическим лицом, программным процессом или устройством), на выполнение запрашиваемого действия применительно к IACS и отслеживать использование этих привилегий.

- SL 1 — ограничивать использование IACS в соответствии с установленными привилегиями для предотвращения случайного или непредумышленного злоупотребления;
- SL 2 — ограничивать использование IACS в соответствии с установленными привилегиями для предотвращения обходных действий субъектов с использованием простых средств при незначительных ресурсах, посредственных навыках и низкой мотивации;
- SL 3 — ограничивать использование IACS в соответствии с установленными привилегиями для предотвращения обходных действий субъектов с использованием изощренных средств при умеренных ресурсах, наличии специальных познаний в IACS и умеренной мотивации;
- SL 4 — ограничивать использование IACS в соответствии с установленными привилегиями для предотвращения обходных действий субъектов с использованием изощренных средств при обширных ресурсах, наличии специальных познаний в IACS и высокой мотивации.

6.2 Целесообразность

Как только пользователь идентифицирован и аутентифицирован, система управления должна разграничить допустимые действия по авторизованному использованию системы управления. Собственники имущественных объектов и системные интеграторы должны будут установить для каждого пользователя (физического лица, программного процесса или устройства), группы, роли и т. д. (см. 5.6, SR 1.4 — Управление идентификаторами) привилегии, определяющие авторизованное использование IACS. Цель контроля использования — предотвращение неавторизованных действий с ресурсами си-

стем управления посредством проверки факта наделения пользователя необходимыми привилегиями до санкционирования выполнения пользователем действий. Примерами действий являются считывание или запись данных, загрузка программ и задание конфигураций. Рекомендации и директивы должны по возможности включать в себя механизмы, которые будут функционировать в смешанных режимах. Например, одни ресурсы системы управления требуют надежной защиты контролем их использования, например ограничительных привилегий, а другие — нет. Что касается расширений, требования к контролю использования должны затрагивать и данные в местах их хранения. Привилегии пользователей могут варьироваться с учетом времени суток/даты, места и средств осуществления доступа.

6.3 SR 2.1 — Контроль выполнения авторизаций

6.3.1 Требование

На всех интерфейсах система управления должна обеспечивать возможность контроля выполнения авторизаций, обязательных для всех пользователей — физических лиц, для контроля использования системы управления с поддержанием ранжирования обязанностей и минимальной привилегии.

6.3.2 Целесообразность и дополнительная методологическая основа

Политики контроля использования (например, политики на основе идентичности, политики на основе ролей и политики на основе правил) и привязанные к ним механизмы контроля осуществления доступа к считыванию/записи данных (например, списки контроля осуществления доступа, матрицы контроля осуществления доступа и криптография) применяются для контроля обращения между пользователями (физическими лицами, программными процессами и устройствами) и объектами (например, устройствами, файлами, записями, программными процессами, программами и доменами).

После того как система управления верифицировала идентичность пользователя (физического лица, программного процесса или устройства) (см. 5.3, SR 1.1 — Идентификация и аутентификация пользователей — физических лиц, и 5.4, SR 1.2 — Идентификация и аутентификация программных процессов и устройств), она должна также верифицировать правомерность запрашиваемой операции в рамках установленных политик и регламентов безопасности. Например, в случае политики управления доступом на основе ролей система управления проверит, какие роли закреплены за верифицированным пользователем или объектом и какие привилегии приписаны этим ролям: если полномочия распространяются на запрашиваемую операцию, то она выполняется, в противном случае запрос отклоняется. Это позволяет контролировать соблюдение ранжирования обязанностей и минимальных привилегий. По возможности не должно допускаться, чтобы механизмы контроля выполнения обращений отрицательно воздействовали на эксплуатационные характеристики системы управления.

Плановые или внеплановые изменения в компонентах системы управления могут существенно отражаться на общей безопасности системы управления. Поэтому желательно, чтобы только квалифицированные и авторизованные лица получали доступ к использованию компонентов системы управления с целью инициирования изменений, включая модернизацию и модификацию.

6.3.3 Расширения требований

6.3.3.1 SR 2.1 RE1 — Контроль выполнения авторизаций для всех пользователей

На всех интерфейсах система управления должна обеспечивать возможность выполнения обязательных авторизаций применительно ко всем пользователям (физическим лицам, программным процессам и устройствам) в целях контроля использования системы управления с поддержанием ранжирования обязанностей и минимальной привилегии.

6.3.3.2 SR 2.1 RE2 — Соотнесение полномочий с ролями

Система управления должна обеспечивать возможность для того или иного авторизованного пользователя или роли определять и корректировать соответствия полномочий ролям применительно ко всем пользователям — физическим лицам.

Примечание 1 — В соответствии с общепризнанной практикой роли не сводятся к фиксированным разветвленным иерархиям, при которых роль более высокого уровня включает в себя как подмножества менее привилегированные роли. Например, на системного администратора вполне могут не распространяться привилегии оператора.

Примечание 2 — Это RE применимо в равной мере к программным процессам и устройствам.

6.3.3.3 SR 2.1 RE3 — Приоритетность диспетчерского управления

Система управления должна поддерживать обеспечение приоритетности ручного диспетчерского управления текущими авторизациями пользователей — физических лиц для конфигурируемого момента времени или последовательности событий.

Примечание — Зачастую необходима реализация управляемой и аудируемой приоритетности ручного управления автоматизированными механизмами в случае события из разряда аварийных или других серьезных событий. Благодаря этому диспетчер может позволить оператору быстро среагировать на нештатные обстоятельства без закрытия текущего сеанса и открытия нового от имени пользователя — физического лица с более высокой привилегией.

6.3.3.4 SR 2.1 RE 4 — Двойное подтверждение

Система управления должна поддерживать двойное подтверждение на случай, если то или иное действие может серьезно отразиться на производственном процессе.

Примечание — Общепринятой практикой является ограничение двойного подтверждения в пользу действий, требующих очень высокого уровня достоверности, что они будут выполнены надежно и корректно. Требование двойного подтверждения подчеркивает серьезность последствий в случае неуспешного, но корректного действия. Примером ситуации, при которой требуется двойное подтверждение, является смена уставки для критически важного промышленного процесса. Общепризнанной практикой является отказ от применения механизмов двойного подтверждения в случае, если требуется мгновенная реакция для предупреждения последствий, относящихся к HSE, например аварийной остановки промышленного процесса.

6.3.4 Уровни безопасности

Далее приведены требования для уровней SL, относящихся к SR 2.1 — Контроль выполнения авторизаций:

- SL-C (UC, система управления) 1: SR 2.1;
- SL-C (UC, система управления) 2: SR 2.1 (1) (2);
- SL-C (UC, система управления) 3: SR 2.1 (1) (2) (3);
- SL-C (UC, система управления) 4. SR 2.1 (1) (2) (3) (4).

6.4 SR 2.2 — Контроль беспроводного использования

6.4.1 Требование

Система управления должна обеспечивать возможность авторизации, отслеживания и установления ограничений на обращения применительно к возможностям беспроводного взаимодействия с системой управления в соответствии с общепринятыми практиками индустрии безопасности.

6.4.2 Целесообразность и дополнительная методологическая основа

Любая беспроводная технология может и в большинстве случаев должна по возможности рассматриваться как еще одна опция протокола передачи данных, а значит, она подчиняется тем же требованиям безопасности IACS, что и любой другой тип коммуникации, используемый IACS. Однако, по результатам анализа рисков, может потребоваться, чтобы беспроводные компоненты IACS поддерживали более широкие возможности контроля использования, чем те, которые обычно требуются от проводных систем для того же случая применения и SL-T. Различия в регламенте также могут обуславливать различия в требуемых возможностях между проводными и беспроводными коммуникациями.

Как отмечено в 5.8, SR 1.6 — Управление беспроводным доступом, беспроводные технологии включают в себя, но не ограничиваются этим, микроволновую, спутниковую связь, пакетную радиосвязь, технологии IEEE 802.11x, IEEE 802.15.4 (ZigBee, МЭК 62591 — WirelessHART®, ISA-100.11a), IEEE 802.15.1 (Bluetooth), мобильные маршрутизаторы беспроводных ЛВС, мобильные телефоны с тетерингом и различные технологии связи в инфракрасном диапазоне.

6.4.3 Расширения требований

6.4.3.1 SR 2.2 1 — Идентификация и сообщение о неавторизованных беспроводных устройствах

Система управления должна обеспечивать возможность идентификации и сообщения о неавторизованных беспроводных устройствах, передающих сигналы в пределах физической среды систем управления.

6.4.3.2 Пусто

6.4.4 Уровни безопасности

Далее приведены требования для четырех уровней SL, относящихся к SR 2.2 — Контроль беспроводного использования:

- SL-C (UC, система управления) 1: SR 2.2;
- SL-C (UC, система управления) 2: SR 2.2;
- SL-C (UC, система управления) 3: SR 2.2 (1);
- SL-C (UC, система управления) 4: SR 2.1 (1).

6.5 SR 2.3 — Контроль использования портативных и подвижных устройств

6.5.1 Требование

Система управления должна обеспечивать возможность автоматического выдвижения конфигурируемых ограничений на обращения, включающих в себя:

a) запрет на использование портативных и мобильных устройств;

b) требование авторизации, обусловленной контекстом; и

c) ограничение на передачу кодов и данных от/на портативные и мобильные устройства.

6.5.2 Целесообразность и дополнительная методологическая основа

Портативные и мобильные устройства могут вносить нежелательный сетевой трафик, вредоносное программное обеспечение и/или провоцировать раскрытие информации, поэтому следует предусмотреть специальный контроль, связанный с их применением в типичной среде систем управления. Политики и регламенты безопасности могут не допускать те или иные функции или операции, выполняемые посредством портативных и/или подвижных устройств. В МЭК 62443-2-1 приведена методологическая основа на предмет того, когда и где следует допускать обращения с участием портативных и подвижных устройств.

Защита информации, базирующейся на портативных и мобильных устройствах (например, применение криптографических механизмов защиты конфиденциальности и целостности информации в момент ее хранения и передачи за пределами контролируемых участков) освещена в других фрагментах (см. раздел 8, FR 4 — Конфиденциальность данных).

6.5.3 Расширения требований

6.5.3.1 SR 2.3 RE 1 — Ужесточение статуса безопасности портативных и подвижных устройств

Система управления должна обеспечивать возможность проверки того, что портативные или мобильные устройства, пытающиеся соединиться с зоной, соответствуют требованиям безопасности этой зоны.

6.5.3.2 Пусто

6.5.4 Уровни безопасности

Далее приведены требования для уровней SL, относящихся к SR 2.3 — Контроль использования портативных и мобильных устройств:

- SL-C (UC, система управления) 1: SR 2.3;
- SL-C (UC, система управления) 2: SR 2.3;
- SL-C (UC, система управления) 3: SR 2.3 (1);
- SL-C (UC, система управления) 4: SR 2.3 (1).

6.6 SR 2.4 — Мобильный код

6.6.1 Требование

Система управления должна обеспечивать возможность выдвижения ограничений на обращения с использованием технологий мобильного кода исходя из риска нанесения ущерба системе управления, и эти ограничения включают в себя:

a) запрещение выполнения мобильного кода;

b) запрос соответствующей аутентификации и авторизации для источника кода;

c) ограничение передачи мобильного кода к системе управления и от нее; и

d) отслеживание использования мобильного кода.

6.6.2 Целесообразность и дополнительная методологическая основа

Технологии на основе мобильных кодов включают в себя, но не ограничиваются этим, Java, JavaScript, ActiveX, формат переносимых документов (PDF), Postscript видеофрагменты Shockwave, Flash-анимации и VBScript. Ограничения на обращения относятся как к выбору и использованию мобильного кода, инсталлируемого на серверах, так и к выбору и использованию мобильного кода, загружаемого и выполняемого на отдельных рабочих станциях. Регламенты управления по возможности должны запрещать разработку, принятие или внесение недопустимого мобильного кода в пределах системы управления. Например, могут быть запрещены передачи мобильных кодов непосредственно к системе управления, но разрешены в контролируемой смежной среде, обслуживаемой персоналом IACS.

6.6.3 Расширения требований

6.6.3.1 SR 2.4 RE 1 — Проверка целостности мобильного кода

Система управления должна обеспечивать возможность верификации целостности мобильного кода до разрешения выполнения кода.

6.6.3.2 Пусто

6.6.4 Уровни безопасности

Далее приведены требования для уровней SL, относящихся к SR 2.4 — Мобильный код:

- SL-C (UC, система управления) 1: SR 2.4;
- SL-C (UC, система управления) 2: SR 2.4,
- SL-C (UC, система управления) 3: SR 2.4 (1);
- SL-C (UC, система управления) 4: SR 2.4 (1).

6.7 SR 2.5 — Блокировка сеанса

6.7.1 Требование

Система управления должна обеспечивать возможность предотвращения доступа посредством инициации блокировки сеанса через конфигурируемый временной промежуток отсутствия активности или посредством ручной инициации. Блокировка сеанса должна оставаться в силе до тех пор, пока пользователь (физическое лицо), учредивший сеанс, или другой авторизованный пользователь — физическое лицо восстановит доступ посредством соответствующих процедур идентификации и аутентификации.

6.7.2 Целесообразность и дополнительная методологическая основа

Субъект, отвечающий за систему управления, должен по возможности применять блокировку сеансов для предотвращения доступа к конкретным рабочим станциям или узлам. Система управления по возможности должна автоматически активировать механизмы блокировки сеанса через конфигурируемый промежуток времени для определенных рабочих станций или узлов. В некоторых случаях не рекомендована блокировка сеансов для рабочих станций операторов или узлов систем управления (например, сеансов, необходимых для принятия операторами незамедлительных ответных мер в нештатных ситуациях). Блокировка сеансов — не замена завершения сеансов в системе управления. В ситуациях, когда система управления не может поддерживать блокировку сеансов, ответственный субъект должен по возможности применять соответствующие компенсационные контрмеры (например, обеспечение улучшенной физической безопасности, безопасности персонала и принятие мер по аудиту).

6.7.3 Расширения требований

Отсутствуют.

6.7.4 Уровни безопасности

Далее приведены требования для уровней SL, относящихся к SR 2.5 — Блокировка сеансов:

- SL-C (UC, система управления) 1: SR 2.5;
- SL-C (UC, система управления) 2: SR 2.5;
- SL-C (UC, система управления) 3: SR 2.5;
- SL-C (UC, система управления) 4: SR 2.5.

6.8 SR 2.6 — Прерывание удаленных сеансов

6.8.1 Требование

Система управления должна обеспечивать возможность прерывания удаленного сеанса либо автоматически, после конфигурируемого периода отсутствия активности, либо вручную пользователем, который инициировал сеанс.

6.8.2 Целесообразность и дополнительная методологическая основа

Удаленный сеанс инициируется всякий раз, когда к системе управления получают доступ через границу зоны, определенной собственником объектов на основе оценки их рисков. Это требование может быть ограничено в пользу сеансов, которые используются для операций мониторинга и обслуживания системы управления (но не критически важных операций) на основе оценки рисков для системы управления, а также политик и регламентов безопасности. Некоторые системы управления или компоненты могут не допускать прерывание сеансов.

6.8.3 Расширения требований

Отсутствуют.

6.8.4 Уровни безопасности

Далее приведены требования для уровней SL, относящихся к SR 2.6 — Прерывание удаленных сеансов:

- SL-C (UC, система управления) 1: не определено;
- SL-C (UC, система управления) 2: SR 2.6;

- SL-C (UC, система управления) 3: SR 2.6;
- SL-C (UC, система управления) 4: SR 2.6.

6.9 SR 2.7 — Контроль параллельных сеансов

6.9.1 Требование

Система управления должна обеспечивать возможность ограничения числа параллельных сеансов на интерфейс для того или иного пользователя (физического лица, программного процесса или устройства) до конфигурируемого числа сеансов.

6.9.2 Целесообразность и дополнительная методологическая основа

Если не налагать ограничения, то может произойти отказ в обслуживании из-за нехватки ресурсов. Существует компромисс между потенциальной блокировкой соответствующего пользователя и блокировкой всех пользователей и сервисов из-за нехватки ресурсов системы управления. По-видимому, требуется методологическая основа от поставщиков продуктов и/или системных интеграторов для предоставления достаточной информации о порядке установления максимального числа сессий.

6.9.3 Расширения требований

Отсутствуют.

6.9.4 Уровни безопасности

Далее приведены требования для уровней SL, относящихся к SR 2.7 — Контроль параллельных сеансов:

- SL-C (UC, система управления) 1: не определено;
- SL-C (UC, система управления) 2: не определено;
- SL-C (UC, система управления) 3: SR 2.7;
- SL-C (UC, система управления) 4: SR 2.7.

6.10 SR 2.8 — События, подлежащие аудиту

6.10.1 Требование

Система управления должна обеспечивать возможность генерации записей аудита, относящихся к безопасности, для следующих категорий: управление доступом, ошибки запроса, события операционной системы, события системы управления, события дублирования и замещения, изменения в конфигурациях, потенциальная разведывательная активность и события журнала регистрации аудита. Отдельно взятые записи аудита должны включать в себя временную метку, источник (исходное устройство, программный процесс или учетную запись пользователя — физического лица), категорию, тип, ID события и результат события.

6.10.2 Целесообразность и дополнительная методологическая основа

Цель этого требования — фиксация наступления важных событий, которые необходимо подвергать аудиту как существенные и значимые для безопасности системы управления. Аудит активности пользователей может отражаться на функционировании систем управления. Функцию аудита безопасности обычно координируют с функцией мониторинга работоспособности и состояния сети, которая может быть реализована и принадлежать другой зоне безопасности. При составлении перечня событий, подлежащих аудиту, следует учитывать общепризнанные и одобренные формы и руководства по конфигурированию. Политики и регламенты безопасности по возможности должны определять те события, подлежащие аудиту, которые допускают поддержание исследований постфактум инцидентов безопасности. Кроме того, желательно, чтобы записей аудита было достаточно для отслеживания эффективности и корректного функционирования механизмов безопасности, применяемых для обеспечения соответствия требованиям настоящего стандарта.

Следует отметить, что требование фиксации событий применимо в контексте функциональности конкретной системы, точнее, в контексте требований безопасности конкретной системы для отдельно взятого уровня. Например, требование фиксации событий аутентификации (в категории управления доступом) в системе с SL 1 применимо только к уровню функциональности аутентификации, требуемому для SL 1 в соответствии с требованиями раздела 5. События могут наступать в любом компоненте системы управления (например, события входа в систему) или отслеживаться посредством специализированных мониторов. Например, сканирование портов может быть зафиксировано системой обнаружения несанкционированных проникновений (IDS) или системой предотвращения несанкционированных проникновений (IPS).

6.10.3 Расширения требований

6.10.3.1 SR 2.8 RE 1 — Централизованно управляемый системный журнал аудита

Система управления должна обеспечивать возможность централизованного управления событиями аудита и компоновки записей аудита, поступающих от множества компонентов в пределах системы управления в журнал коррелированного во времени аудита масштаба системы (логической или физической). Система управления должна обеспечивать возможность экспорта этих записей аудита в форматах промышленных стандартов для их анализа посредством стандартных коммерческих инструментов анализа файлов регистрации, например средств управления информацией и событиями безопасности (SIEM).

6.10.3.2 Пусто

6.10.4 Уровни безопасности

Далее приведены требования для четырех уровней SL, относящихся к SR 2.8 — События, подлежащие аудиту:

- SL-C (UC, система управления) 1: SR 2.8;
- SL-C (UC, система управления) 2: SR 2.8;
- SL-C (UC, система управления) 3: SR 2.8 (1);
- SL-C (UC, система управления) 4: SR 2.8 (1).

6.11 SR 2.9 — Емкость систем хранения данных аудита

6.11.1 Требование

Система управления должна выделять достаточную емкость для системы хранения записей аудита в соответствии с общепризнанными рекомендациями по управлению файлами регистрации и конфигурированию систем. Система управления должна предусматривать такие механизмы аудита, которые снижают вероятность переполнения хранилища.

6.11.2 Целесообразность и дополнительная методологическая основа

Система управления по возможности должна обеспечивать емкость носителя данных аудита, достаточную с учетом политики хранения, выполняемого аудита и требований онлайн-обработки данных аудита. Директивы, подлежащие учету, могут включать в себя NIST Special Publication (SP) 800-92 [27]. Емкость носителя данных аудита по возможности должна быть достаточной для сохранения файлов регистрации в течение периода времени, обусловленного действующими политиками и нормами или бизнес-требованиями.

6.11.3 Расширения требований

6.11.3.1 T 2.9 RE 1 — Предупреждение при достижении порога емкости носителя записей аудита

Система управления должна обеспечивать возможность подачи предупредительного сигнала, когда выделенный объем носителя данных для записей аудита достиг заданного (конфигурируемого) процента от максимальной емкости носителя записей аудита.

6.11.3.2 Пусто

6.11.4 Уровни безопасности

Далее приведены требования для уровней SL, относящихся к SR 2.9 — Емкость носителя данных аудита:

- SL-C (UC, система управления) 1: SR 2.9;
- SL-C (UC, система управления) 2: SR 2.9;
- SL-C (UC, система управления) 3: SR 2.9 (1);
- SL-C (UC, система управления) 4: SR 2.9 (1).

6.12 Ответные действия в случае сбоев обработки данных аудита

6.12.1 Требование

Система управления должна обеспечивать возможность оповещения персонала о сбое и предотвращения утраты жизненно важных сервисов и функций в случае сбоя обработки данных аудита. Система управления должна обеспечивать возможность поддержания соответствующих действий в ответ на сбой обработки данных аудита в соответствии с общепринятыми промышленными практиками и рекомендациями.

6.12.2 Целесообразность и дополнительная методологическая основа

Инициация аудита обычно происходит на источнике события. Обработка данных аудита включает в себя пересылку записей аудита, возможное снабжение записей дополнительной информацией (на-

пример, добавление временной метки) и передачу записей на постоянное хранение. Сбои обработки данных аудита включают в себя, например, программные или аппаратные ошибки, сбои в механизмах сбора данных аудита и заполнение или превышение емкости носителя данных аудита. Руководящие материалы, которые следует учитывать при разработке соответствующих ответных действий, могут включать в себя требования NIST SP800-92. Следует отметить, что перезапись самых первых записей аудита или приостановка генерации файлов регистрации аудита являются возможными ответными действиями в случае превышения емкости носителя данных аудита, однако эти действия влекут потерю потенциально существенной информации для экспертного анализа.

6.12.3 Расширения требований

Отсутствуют.

6.12.4 Уровни безопасности

Далее приведены требования для четырех уровней SL, относящихся к SR 2.10 — Ответные действия в случае сбоев обработки данных аудита:

- SL-C (UC, система управления) 1: SR 2.10;
- SL-C (UC, система управления) 2: SR 2.10;
- SL-C (UC, система управления) 3: SR 2.10;
- SL-C (UC, система управления) 4: SR 2.10.

6.13 SR 2.11 — Временные метки

6.13.1 Требование

Система управления должна предусматривать использование временных меток при генерации записей аудита.

6.13.2 Целесообразность и дополнительная методологическая основа

Временные метки (включающие в себя дату и время) записей аудита должны по возможности генерироваться с использованием внутрисистемных тактовых генераторов. При отсутствии системной синхронизации времени (что типично для многих установок), потребуются известные события в качестве точки отсчета при анализе последовательности событий. Кроме того, синхронизация сгенерированных системой записей аудита с внешними событиями, скорее всего, потребует синхронизации с общеизвестным внешним источником синхросигналов (таким, как GPS, ГЛОНАСС и Галилео). Источник синхросигналов по возможности должен быть защищен от неавторизованного изменения.

6.13.3 Расширения требований

6.13.3.1 SR 2.11 RE 1 — Внутрисистемная синхронизация времени

Система управления должна обеспечивать возможность синхронизации внутрисистемного тактового генератора на конфигурируемой частоте.

6.13.3.2 SR 2.11 RE 2 — Защита целостности источника синхроимпульсов

Источник синхроимпульсов должен быть защищен от неавторизованного изменения и инициировать событие аудита при его изменении.

6.13.4 Уровни безопасности

Далее приведены требования для уровней SL, относящихся к SR 2.11 — Временные метки:

- SL-C (UC, система управления) 1: не определено;
- SL-C (UC, система управления) 2: SR 2.11;
- SL-C (UC, система управления) 3: SR 2.11 (1);
- SL-C (UC, система управления) 4: SR 2.11 (1) (2).

6.14 SR 2.12 — Защита от непризнания участия

6.14.1 Требование

Система управления должна обеспечивать возможность выявления факта совершения тем или иным пользователем — физическим лицом определенного действия.

6.14.2 Целесообразность и дополнительная методологическая основа

Примеры конкретных действий, совершаемых пользователем, включают в себя выполнение действий оператора, изменение конфигураций системы управления, создание информации, отправку сообщения, подтверждение информации (например, выставление метки о согласии) и прием сообщения. Защита от непризнания участия позволяет пресечь последующие ложные заявления: пользователя — о том, что он не выполнял определенного действия; автора — что он не помечал авторство конкретного документа; отправителя — что он не отправлял сообщения; получателя — что он не получал сообще-

ния, или подписанта — что он не подписывал документ. Сервисы защиты от непризнания участия могут использоваться для определения того, исходила ли информация от пользователя, совершал ли пользователь конкретные действия (например, отправлял ли он сообщение по электронной почте и подтверждал ли рабочий заказ, получал ли он конкретную информацию). Сервисы защиты от непризнания участия получаются посредством применения разнообразных технологий или механизмов (например, цифровых подписей, подтверждений получения цифровых сообщений и временных меток).

6.14.3 Расширения требований

6.14.3.1 SR 2.12 RE 1 — Защита от непризнания участия для всех пользователей

Система управления должна обеспечивать возможность выявления факта совершения тем или иным пользователем (физическим лицом, программным процессом или устройством) конкретного действия.

6.14.3.2 Пусто

6.14.4 Уровни безопасности

Далее приведены требования для уровней SL, относящихся к SR 2.12 — Защита от непризнания участия:

- SL-C (UC, система управления) 1: не определено;
- SL-C (UC, система управления) 2: не определено;
- SL-C (UC, система управления) 3: SR 2.12;
- SL-C (UC, система управления) 4: SR 2.12 (1).

7 FR 3 — Целостность системы

7.1 Назначение и описания SL-C(SI)

Обеспечивать целостность IACS для предотвращения неавторизованных манипуляций:

- SL 1 — защищать целостность IACS посредством предотвращения случайных или непреднамеренных манипуляций;
- SL 2 — защищать целостность IACS посредством предотвращения манипуляций со стороны кого-либо, кто использует простые средства, имеет незначительные ресурсы, посредственные навыки и низкую мотивацию;
- SL 3 — защищать целостность IACS посредством предотвращения манипуляций со стороны кого-либо, кто использует изощренные средства, имеет умеренные ресурсы, специальные познания в IACS и умеренную мотивацию;
- SL 4 — защищать целостность IACS посредством предотвращения манипуляций со стороны кого-либо, кто использует изощренные средства и имеет обширные ресурсы, специальные познания в IACS и высокую мотивацию.

7.2 Целесообразность

IACS зачастую проходят множество циклов испытаний (тестирование на уровне модулей, FAT, SAT, сертификацию, пуско-наладку и т. д.) для удостоверения того, что системы будут функционировать надлежащим образом еще до их запуска. Как только объекты введены в эксплуатацию, их собственники отвечают за поддержание целостности IACS. Используя собственную методологию оценки рисков, собственники объектов могут устанавливать различные уровни защиты целостности для различных систем, коммуникационных каналов и информации в их IACS. Целостность физических объектов следует поддерживать как в условиях их эксплуатации, так и в случае их пребывания в нерабочем состоянии, например, во время производства, в ходе хранения или в продолжение остановки на техобслуживание. Целостность логических объектов следует поддерживать в ходе их передачи или хранения, например в ходе пересылки объектов по сети или их хранения в хранилище данных.

7.3 SR 3.1 — Целостность коммуникации

7.3.1 Требование

Система управления должна обеспечивать возможность защиты целостности передаваемой информации.

7.3.2 Целесообразность и дополнительная методологическая основа

Многие типичные сетевые атаки основаны на манипуляциях с данными в момент их передачи, например на манипуляциях с сетевыми пакетами. Коммутируемые или маршрутизируемые сети от-

крывают дополнительные возможности для злоумышленников в плане манипуляций с пакетами, поскольку осуществить незаметный доступ к этим сетям обычно проще, а сами механизмы коммутации и маршрутизации также могут подвергаться манипуляциям для получения дополнительного доступа к передаваемой информации. Манипуляции в контексте системы управления могут включать в себя изменение измеренных значений, передаваемых от датчика к приемнику, или изменение параметров команд, пересылаемых от управляющего приложения к исполнительному механизму.

Допустимые и целесообразные механизмы будут варьироваться в зависимости от контекста (например, передачи в пределах сегмента локальной сети или передачи через недоверенные сети) и типа сети, используемого при передаче (например, TCP/IP или локальных последовательных линий связи). В малой сети с непосредственными связями (точка — точка) защиты физического доступа ко всем узлам может быть достаточно при низких SL, если целостность конечной точки защищена в той же степени (см. 7.6, SR 3.4 — Целостность программного обеспечения и информации), в то время как в сети, рассредоточенной на участках с регулярным физическим присутствием персонала, или в глобальной вычислительной сети физический доступ, скорее всего, неосуществим. Если для обеспечения коммуникационных сервисов используется коммерческая служба как отдельный продукт, нежели полностью выделенная служба (например, выделенная линия вместо Т1-тракта), то может быть труднее получить необходимые гарантии относительно реализации необходимых элементов управления безопасностью для целостности коммуникации (например, из-за нормативно-правовых ограничений). Если невозможно или нецелесообразно обеспечить соответствие необходимым требованиям безопасности, то может быть целесообразно реализовать соответствующие компенсационные контрмеры или явно принять дополнительный риск.

Промышленное оборудование часто бывает подвержено воздействиям окружающей среды, что может приводить к нарушениям целостности и/или инцидентам с ложноположительными срабатываниями. Как это часто бывает, окружающая среда — источник взвешенных частиц, влаги, вибрации, газов, радиации и электромагнитных помех, которые могут вызывать условия, отражающиеся на целостности проводки и сигналов коммуникационной связи. Сетевую инфраструктуру следует разрабатывать с целью минимизации этих физических/внешних воздействий на целостность коммуникации. Например, если взвеси, влага и/или газы являют собой проблему, то может быть необходимо использовать изолированное стандартное гнездо 45 (RJ-45) или разъем М12 вместо привычного разъема RJ-45 проводки. Сам провод может требовать использования другой оболочки, которая рассчитана, среди прочего, на взаимодействие с взвешенными частицами, влагой и/или газом. В случаях, когда проблему являет собой вибрация, могут потребоваться разъемы М12 во избежание отсоединения пружинных штырей на разъеме RJ-45. В случаях, когда проблему являют собой радиация и/или электромагнитные помехи, может потребоваться использование экранированной витой пары или волоконных кабелей для предотвращения любых воздействий на сигналы связи. Может потребоваться также проведение анализа спектра беспроводных сигналов на этих участках, если запланировано беспроводное сетевое взаимодействие, для удостоверения целесообразности этого решения.

7.3.3 Расширения требований

7.3.3.1 SR 3.1 RE 1 — Защита целостности средствами криптографии

Система управления должна обеспечивать возможность применения криптографических механизмов для выявления изменений в информации, произошедших в ходе ее передачи.

Примечание — Общепринятой практикой является определение должного использования криптографических механизмов для аутентификации и обеспечения целостности сообщений после тщательного анализа нужд безопасности и потенциальных последствий для функционирования системы и возможности восстановления после системного сбоя.

7.3.3.2 Пусто

7.3.4 Уровни безопасности

Далее приведены требования для уровней SL, относящихся к SR 3.1 — Целостность коммуникации:

- SL-C (SI, система управления) 1: SR 3.1;
- SL-C (SI, система управления) 2: SR 3.1;
- SL-C (SI, система управления) 3: SR 3.1 (1);
- SL-C (SI, система управления) 4: SR 3.1 (1).

7.4 SR 3.2 — Защита от вредоносного кода

7.4.1 Требование

Система управления должна обеспечивать возможность применения защитных механизмов для предотвращения, обнаружения, смягчения воздействий и сообщения о вредоносном коде или неавторизованном программном обеспечении. Система управления должна обеспечивать возможность обновления защитных механизмов.

7.4.2 Целесообразность и дополнительная методологическая основа

Система управления по возможности должна использовать защитные механизмы для предотвращения, обнаружения, смягчения воздействий и сообщения о случаях передачи вредоносного кода (например, вирусов, червей, троянских коней и шпионского программного обеспечения) через электронную почту, вложения электронной почты, доступ в Интернет, съемные носители (например, устройства на базе универсальной последовательной шины (USB), дискеты или компакт-диски), документы PDF, веб-службы, сетевые соединения и инфицированные лэптопы или другие известные средства.

Механизмы обнаружения по возможности должны быть способны обнаруживать нарушения целостности двоичных файлов и файлов с данными. Технологии могут включать в себя, но не ограничиваются этим, технологии мониторинга целостности двоичного файла и его атрибутов, хеширования и технологии подписей. Технологии смягчения воздействий могут включать в себя, но не ограничиваются этим, очистку файлов, помещение файлов на карантин, ликвидацию файлов, ограничение на коммуникацию с хостами и системы IPS.

Упреждающие технологии могут включать в себя, но не ограничиваются этим, технологии внесения приложений в черный и белый списки, контроль съемных носителей, технологии песочниц и механизмы специальных вычислительных платформ (например, ограниченные возможности обновления встроенного программного обеспечения, No Execute (NX) bit, DEP, рандомизация распределения адресного пространства (ASLR), обнаружение повреждения стеков и элементы мандатного управления доступом). В 10.4, SR 6.2 — Непрерывный мониторинг, представлено соответствующее требование, затрагивающее инструменты и технологии мониторинга систем управления.

Механизмы предотвращения и смягчения воздействий могут включать в себя механизмы, рассчитанные для хост-элементов (таких, как компьютеры и серверы), и механизмы на базе сетей (такие, как системы IDS и IPS), а также механизмы, ориентированные на специальные компоненты систем управления (такие, как контроллеры PLC и интерфейсы HMI).

7.4.3 Расширения требований

7.4.3.1 SR 3.2 RE 1 — Защита от вредоносного кода на входах и выходах

Система управления должна обеспечивать возможность применения механизмов защиты от вредоносного кода на всех входах и выходах.

Примечание — Такие механизмы обычно предусматриваются на съемных носителях, межсетевых экранах, однонаправленных шлюзах, веб-серверах, прокси-серверах или серверах удаленного доступа.

7.4.3.2 SR 3.2 RE 2 — Централизованное управление и отчетность для защиты от вредоносного кода

Система управления должна обеспечивать возможность управления механизмами защиты от вредоносного кода.

Примечание — Такие механизмы обычно представлены централизованным управлением инфраструктурой оконечных точек или решениями SIEM.

7.4.4 Уровни безопасности

Далее приведены требования для уровней SL, относящихся к SR 3.2 — Защита от вредоносного кода:

- SL-C (SI, система управления) 1: SR 3.2;
- SL-C (SI, система управления) 2: SR 3.2 (1);
- SL-C (SI, система управления) 3: SR 3.2 (1) (2);
- SL-C (SI, система управления) 4: SR 3.2 (1) (2).

7.5 SR 3.3 — Верификация функциональности безопасности

7.5.1 Требование

Система управления должна обеспечивать возможность поддержания верификации предполагаемого действия функций безопасности и сообщать об обнаружении аномалий в ходе FAT, SAT и пла-

нового техобслуживания. Эти функции безопасности должны включать в себя все те функции, которые необходимы для поддержания требований безопасности, определенных в настоящем стандарте.

7.5.2 Целесообразность и дополнительная методологическая основа

Поставщик продуктов и/или системный интегратор по возможности должны предоставлять методологическую основу на предмет того, как тестировать разработанные элементы управления безопасностью. Собственники объектов должны быть осведомлены о возможных последствиях проведения этих верификационных тестов во время штатных операций. Подробности реализации этих верификаций должны быть определены с тщательным учетом требований непрерывности операций (например, планирования или предварительного уведомления).

Примеры функций верификации безопасности включают в себя:

- верификацию антивирусных мер посредством тестирования файловой системы системы управления с помощью тестового файла EICAR. Антивирусное программное обеспечение по возможности должно обнаружить этот файл, и по возможности должны быть инициированы соответствующие процедуры обработки инцидентов;
- верификацию мер идентификации, аутентификации и мер контроля использования посредством осуществления попыток доступа с неавторизованной учетной записью (для некоторой функциональности это может быть автоматизировано);
- верификацию систем IDS как элемента управления безопасностью посредством включения определенного правила в IDS, которое срабатывает при регистрации нестандартного, но известного невредоносного трафика. После этого может быть проведен тест посредством внесения трафика, который инициирует это правило и соответствующие процедуры IDS по отслеживанию и обработке инцидентов;
- подтверждение того, что регистрация аудита происходит в соответствии с требованиями политик и регламентов безопасности и не деактивирована внутренним или внешним субъектом.

7.5.3 Расширения требований

7.5.3.1 SR 3.3 RE 1 — Автоматизированные механизмы верификации функциональности безопасности

Система управления должна обеспечивать возможность применения автоматизированных механизмов для поддержания управления верификацией безопасности во время FAT, SAT и планового техобслуживания.

7.5.3.2 SR 3.3 RE 2 — Верификация функциональности безопасности во время штатной работы

Система управления должна обеспечивать возможность поддержания верификации предполагаемого действия функций безопасности во время штатных операций.

Примечание — Общепринятой практикой является точная реализация данного требования во избежание отрицательных последствий. Зачастую данное требование считается неподходящим для систем, связанных с физической безопасностью.

7.5.4 Уровни безопасности

Далее приведены требования для уровней SL, относящихся к SR 3.3 — Верификация функциональности безопасности:

- SL-C (SI, система управления) 1: SR 3.3;
- SL-C (SI, система управления) 2: SR 3.3;
- SL-C (SI, система управления) 3: SR 3.3 (1);
- SL-C (SI, система управления) 4: SR 3.3 (1) (2).

7.6 SR 3.4 — Целостность программного обеспечения и информации

7.6.1 Требование

Система управления должна обеспечивать возможность обнаружения, фиксации, противодействия и сообщения о неавторизованных изменениях программного обеспечения и информации во время их хранения.

7.6.2 Целесообразность и дополнительная методологическая основа

Неавторизованные изменения — это изменения, на которые субъект, предпринимающий попытку изменения, не имеет необходимых полномочий. Данное SR дополняет родственные SR из FR 1 и 2. FR 1 и 2 распространяются на установление ролей, привилегий и шаблонов использования в соответствии с проектом. Методы верификации целостности применяются для обнаружения, фиксации, противодействия и сообщения о нарушениях целостности программного обеспечения и информации,

которые могут происходить в случае преодоления других механизмов защиты (таких, как обязательная авторизация). Система управления по возможности должна использовать формализованные или рекомендованные механизмы обеспечения целостности (такие, как криптографические хеши). Например, такие механизмы могут использоваться для мониторинга периферийных устройств на предмет последней информации об их конфигурациях, чтобы обнаружить бреши в защите (включая неавторизованные изменения).

7.6.3 Расширения требований

7.6.3.1 SR 3.4 RE 1 — Автоматизированное уведомление о злоумышленных нарушениях целостности

Система управления должна обеспечивать возможность использования автоматизированных инструментов, которые предоставляют уведомления для конфигурируемой совокупности получателей после обнаружения несоответствий в ходе верификации целостности.

7.6.3.2 Пусто

7.6.4 Уровни безопасности

Далее приведены требования для уровней SL, относящихся к SR 3.4 — Целостность программного обеспечения и информации:

- SL-C (SI, система управления) 1: SR 3.4;
- SL-C (SI, система управления) 2: SR 3.4;
- SL-C (SI, система управления) 3: SR 3.4 (1);
- SL-C (SI, система управления) 4: SR 3.4 (1).

7.7 SR 3.5 — Валидация входных данных

7.7.1 Требование

Система управления должна выполнять валидацию синтаксической структуры и содержания любых входных данных, которые служат входными данными управления производственными процессами или входными данными, непосредственно воздействующими на работу системы управления.

7.7.2 Целесообразность и дополнительная методологическая основа

Должны по возможности действовать правила проверки актуальности синтаксической структуры входных данных системы управления, например уставок, для верификации того факта, что эта информация не была искажена и согласуется со спецификацией. Входные данные, поступившие к интерпретаторам, по возможности должны проходить предварительную проверку для предотвращения случайной интерпретации содержания как команд. Следует отметить, что это — SR безопасности и потому не учитывает человеческий фактор, например подачу правомерного целого числа, которое лежит вне ожидаемого диапазона.

Общепринятые промышленные практики для валидации входных данных распространяются на значения вне допустимого диапазона для определенного типа поля, недопустимые символы в полях данных, отсутствующие или неполные данные и переполнение буферов. Другие примеры, когда недопустимые входные данные провоцируют проблемы безопасности систем, включают в себя атаки с внедрением SQL-кода, межсайтовый скриптинг или искаженные пакеты (обычно генерируемые тестерами протоколов (protocol fuzzers)). Руководящие материалы, которые следует учитывать, могут включать в себя требования Open Web Application Security Project (OWASP) [31] Code Review Guide.

7.7.3 Расширения требований

Отсутствуют.

7.7.4 Уровни безопасности

Далее приведены требования для уровней SL, относящихся к SR 3.5 — Валидация входных данных:

- SL-C (SI, система управления) 1: SR 3.5;
- SL-C (SI, система управления) 2: SR 3.5;
- SL-C (SI, система управления) 3: SR 3.5;
- SL-C (SI, система управления) 4: SR 3.5.

7.8 SR 3.6 — Детерминированный поток выходных сигналов

7.8.1 Требование

Система управления должна обеспечивать возможность приведения потоков выходных сигналов к заданному режиму, если в результате атаки не может поддерживаться штатное функционирование.

7.8.2 Целесообразность и дополнительная методологическая основа

Важной характеристикой в обеспечении целостности штатных операций является детерминированный режим потоков выходных сигналов системы управления в результате угрожающих действий по отношению к системе управления. В идеальном случае в процессе атаки система управления продолжает функционировать в штатном режиме, но если система управления не может поддерживать штатное функционирование, то поток выходных сигналов системы управления должен снизиться до заданного уровня. Заданный режим потока выходных сигналов системы управления привязан к приложениям и может соответствовать одной из следующих опций, конфигурируемых пользователем.

- пассивный — поток выходных данных падает до пассивного уровня;
- удержания — поток выходных сигналов падает до последнего удачного уровня;
- фиксированный — поток выходных данных падает до фиксированного уровня, который определяется собственником объекта или приложением.

7.8.3 Расширения требований

Отсутствуют.

7.8.4 Уровни безопасности

Далее приведены требования для уровней SL, относящихся к SR 3.6 — Детерминирование потока выходных сигналов:

- SL-C (SI, система управления) 1: SR 3.6;
- SL-C (SI, система управления) 2: SR 3.6;
- SL-C (SI, система управления) 3: SR 3.6;
- SL-C (SI, система управления) 4: SR 3.6.

7.9 SR 3.7 — Обработка ошибок

7.9.1 Требование

Система управления должна идентифицировать и обрабатывать условия, указывающие на ошибки, так, чтобы осуществлялось эффективное устранение ошибок и их последствий. Это должно выполняться таким образом, чтобы не выдавалась информация, которой могут воспользоваться злоумышленники для атак на IACS, если только раскрытие этой информации не требуется для своевременного урегулирования проблем.

7.9.2 Целесообразность и дополнительная методологическая основа

Структура и содержание сообщений об ошибках по возможности должны тщательно учитываться поставщиком продуктов и/или системным интегратором. Сообщения об ошибках, сгенерированные системой управления, по возможности должны предоставлять своевременную и полезную информацию без раскрытия потенциально вредоносной информации, которой могут воспользоваться злоумышленники для неправомерного использования IACS. Может быть не очевидно, является ли отдельно взятое условие, указывающее на ошибку, следствием события безопасности, поэтому все сообщения об ошибках должны быть легкодоступны в ходе реагирования на инциденты. Раскрытие этой информации по возможности должно быть обосновано необходимостью своевременного урегулирования условий, указывающих на ошибки. Руководящие материалы, которые следует учитывать, могут включать в себя требования OWASP Code Review Guide [31].

7.9.3 Расширения требований

Отсутствуют.

7.9.4 Уровни безопасности

Далее приведены требования для уровней SL, относящихся к SR 3.7 — Обработка ошибок:

- SL-C (SI, система управления) 1: не определено;
- SL-C (SI, система управления) 2: SR 3.7;
- SL-C (SI, система управления) 3: SR 3.7;
- SL-C (SI, система управления) 4: SR 3.7.

7.10 SR 3.8 — Целостность сеанса

7.10.1 Требование

Система управления должна обеспечивать возможность защиты целостности сеансов. Система управления должна отказывать в каком-либо использовании некорректных ID сеанса.

7.10.2 Целесообразность и дополнительная методологическая основа

Этот элемент управления нацелен на защиту коммуникаций на уровне сессий в противоположность уровню пакетов. Функция этого элемента управления — создание на каждом конце коммуникаци-

онного сеанса оснований для уверенности в текущей идентичности другой стороны и в действительности передаваемой информации. Например, этот элемент управления затрагивает атаки типа «человек посередине», включая перехват сеанса, внедрение в сеанс ложной информации или атаки повторного воспроизведения. Использование механизмов целостности сеанса может быть сопряжено с существенными непроизводственными издержками, а значит, их использование следует рассматривать в свете требований к коммуникациям в реальном масштабе времени.

7.10.3 Расширения требований

7.10.3.1 SR 3.8 RE 1 — Аннулирование идентификаторов ID сеанса после завершения сеанса

Система управления должна обеспечивать возможность аннулирования идентификаторов ID сеанса после выхода пользователя из системы или иного завершения сеанса (включая сеансы с использованием браузеров).

7.10.3.2 SR 3.8 RE 2 — Генерация уникального ID сеанса

Система управления должна обеспечивать возможность генерации уникального ID для каждого сеанса и признания всех непредусмотренных ID сеанса недействительными.

7.10.3.3 SR 3.8 RE 3 — Случайный характер ID сеансов

Система управления должна обеспечивать возможность генерации уникальных ID сеансов посредством общепризнанных источников случайных значений.

Примечание — В ходе перехватов сеанса и других атак типа «человек посередине» или внедрений ложной информации зачастую используют легко разгадываемые ID сеансов (ключи или другие разделенные секреты) или используются ID сеансов, которые не были должным образом аннулированы после завершения сеансов. Поэтому срок действия аутентификатора сеанса должен быть жестко привязан к продолжительности сеанса. Применение случайных значений при генерации уникальных ID сеансов позволяет предотвратить атаки перебором для определения ID будущих сеансов.

7.10.4 Уровни безопасности

Далее приведены требования для уровней SL, относящихся к SR 3.8 — Целостность сеанса:

- SL-C (SI, система управления) 1: не определено;
- SL-C (SI, система управления) 2: SR 3.8;
- SL-C (SI, система управления) 3: SR 3.8 (1) (2);
- SL-C (SI, система управления) 4: SR 3.8 (1) (2) (3).

7.11 SR 3.9 — Защита информации аудита

7.11.1 Требование

Система управления должна защищать информацию аудита и инструменты аудита (в случае их наличия) от неавторизованного доступа, модификации и уничтожения.

7.11.2 Целесообразность и дополнительная методологическая основа

Информация аудита включает в себя всю информацию (например, записи аудита, настройки аудита и отчеты аудита), необходимую для успешного аудита активности системы управления. Информация аудита важна для коррекции ошибок, восстановления после нарушений безопасности, исследований и связанных с ними действий. Механизмы для улучшенной защиты от модификации и уничтожения включают в себя запись информации аудита на аппаратных неперезаписываемых носителях.

7.11.3 Расширения требований

7.11.3.1 SR 3.9 RE 1 — Записи аудита на неперезаписываемых носителях

Система управления должна обеспечивать возможность создания записей аудита на аппаратных неперезаписываемых носителях.

7.11.3.2 Пусто

7.11.4 Уровни безопасности

Далее приведены требования для уровней SL, относящихся к SR 3.9 — Защита информации аудита:

- SL-C (SI, система управления) 1: не определено;
- SL-C (SI, система управления) 2: SR 3.9;
- SL-C (SI, система управления) 3: SR 3.9;
- SL-C (SI, система управления) 4: SR 3.9 (1).

8 FR 4 — Конфиденциальность данных

8.1 Назначение и описания SL-C(DC)

Обеспечивать конфиденциальность информации в коммуникационных каналах и в хранилищах данных для предотвращения ее неавторизованного раскрытия:

- SL 1 — предотвращать неавторизованное раскрытие информации посредством ее несанкционированного извлечения или случайного обнародования;
- SL 2 — предотвращать неавторизованное раскрытие информации субъекту, активно ее ищущему с использованием простых средств, при незначительных ресурсах, посредственных навыках и низкой мотивации;
- SL 3 — предотвращать неавторизованное раскрытие информации субъекту, активно ее ищущему с использованием изощренных средств, при умеренных ресурсах, наличии специальных познаний в IACS и умеренной мотивации;
- SL 4 — предотвращать неавторизованное раскрытие информации субъекту, активно ее ищущему с использованием изощренных средств, при обширных ресурсах, наличии специальных познаний в IACS и высокой мотивации.

8.2 Целесообразность

Некоторая информация, генерируемая системами управления, либо хранящаяся, либо передаваемая, носит конфиденциальный или важный характер. Это предполагает, что некоторые коммуникационные каналы и хранилища данных нуждаются в защите от несанкционированного извлечения данных и неавторизованного доступа к ним.

8.3 SR 4.1 — Конфиденциальность информации

8.3.1 Требование

Система управления должна обеспечивать возможность защиты конфиденциальности информации, для которой поддерживается явная авторизация на осуществление операции чтения, будь то хранящаяся или передаваемая информация.

8.3.2 Целесообразность и дополнительная методологическая основа

Защита информации, как хранящейся, так и передаваемой, может обеспечиваться с помощью физических средств, секционирования или шифрования, а также других технологий. Крайне существенно, что та или иная технология выбирается с учетом ее потенциального воздействия на функционирование системы управления и возможности восстановления после системного сбоя или атаки.

Решение о том, следует ли защищать конфиденциальность отдельно взятого фрагмента информации, зависит от контекста и не может быть принято в ходе разработки продукта. Однако тот факт, что организация ограничивает доступ к информации посредством конфигурации явной авторизации на осуществление операции чтения в системе управления, означает, что организация причисляет эту информацию к конфиденциальной. Таким образом, вся информация, для которой система управления поддерживает возможность выдвижения явной авторизации на осуществление операции чтения, по возможности должна причисляться к потенциально конфиденциальной, а значит, система управления по возможности должна также обеспечивать возможность ее защиты.

Различные организации и отрасли промышленности могут требовать разных уровней надежности шифрования для разных категорий информации, в зависимости от степени важности информации, а также промышленных стандартов и регламентных требований (см. 8.5, SR 4.3 — Использование криптографии). В некоторых ситуациях конфиденциальной может считаться информация о конфигурации сети, фиксируемая и обрабатываемая в коммутаторах и маршрутизаторах.

Коммуникации, предполагающие открытую передачу информации, могут быть уязвимы перед несанкционированным извлечением информации или другими несанкционированными вмешательствами. Если система управления привязана к провайдеру сервисов внешних коммуникаций, то может быть сложнее получить необходимые гарантии относительно реализации необходимых требований безопасности для конфиденциальности коммуникации. В таких случаях может быть целесообразно реализовать компенсационные контрмеры или явно принять дополнительный риск.

Субъекты должны быть также по возможности осведомлены о конфиденциальности информации, когда используются портативные и мобильные устройства (например, инженерные лэптопы и USB-накопители).

В соответствии с требованиями 5.7, SR 1.5 — Управление аутентификаторами, аутентификационная информация, такая как пароли, по возможности должна причисляться к конфиденциальной и поэтому никогда не пересылаться в незашифрованном виде.

8.3.3 Требования безопасности

8.3.3.1 SR 4.1 RE 1 — Защита конфиденциальности информации в ходе ее хранения или передачи через недоверенные сети

Система управления должна обеспечивать возможность защиты конфиденциальности информации в ходе ее хранения и сеансов удаленного доступа через недоверенную сеть.

Примечание — Криптография — типичный механизм обеспечения конфиденциальности информации.

8.3.3.2 SR 4.1 RE 2 — Защита конфиденциальности при пересечении границ зон

Система управления должна обеспечивать возможность защиты конфиденциальности информации, пересекающей любую границу зоны.

8.3.4 Уровни безопасности

Далее приведены требования для уровней SL, относящихся к SR 4.1 — Конфиденциальность информации:

- SL-C (DC, система управления) 1: SR 4.1;
- SL-C (DC, система управления) 2: SR 4.1 (1);
- SL-C (DC, система управления) 3: SR 4.1 (1);
- SL-C (DC, система управления) 4: SR 4.1 (1) (2).

8.4 SR 4.2 — Сохранность информации

8.4.1 Требование

Система управления должна обеспечивать возможность удаления всей информации, для которой поддерживается явная авторизация на чтение, из компонентов, которые предстоит вывести из активного сервиса и/или эксплуатации.

8.4.2 Целесообразность и дополнительная методологическая основа

Вывод компонента системы управления из активного сервиса не должен создавать возможность случайного раскрытия информации, для которой поддерживается явная авторизация на осуществление операции чтения. Примеры такой информации включают в себя «ключи подключения» (в случае некоторых беспроводных периферийных устройств), хранящиеся в энергонезависимой памяти, или другую криптографическую информацию, которая может способствовать неавторизованной или вредоносной активности.

Информация, созданная действиями пользователя или роли (или действиями программного процесса, действующего от имени пользователя или роли), по возможности не должна бесконтрольно раскрываться другому пользователю или роли. Контроль информации системы управления или сохранности данных препятствует случайному раскрытию информации, хранящейся на разделяемом ресурсе, и ее передаче обратно в систему управления после отключения этого ресурса.

8.4.3 Расширения требований

8.4.3.1 SR 4.2 RE 1 — Удаление ресурсов на базе разделяемой памяти

Система управления должна обеспечивать возможность предотвращения неавторизованной и непредусмотренной передачи информации посредством ресурсов на базе энергозависимой разделяемой памяти.

Примечание — Ресурсы на базе энергозависимой памяти — это ресурсы, которые, как правило, не сохраняют информацию после их отключения для управления памятью. Однако существуют атаки на RAM, способные приводить к извлечению ключевого материала или других конфиденциальных данных до их фактической перезаписи. Поэтому общепринятой практикой является удаление всех уникальных данных и связей с уникальными данными из энергозависимой разделяемой памяти при отключении этой памяти и перенос их обратно в систему управления для использования другим пользователем, так чтобы эти данные были не видны или не доступны для нового пользователя.

8.4.3.2 Пусто

8.4.4 Уровни безопасности

Далее приведены требования для уровней SL, относящихся к SR 4.2 — Сохранность информации:

- SL-C (DC, система управления) 1: не определено;
- SL-C (DC, система управления) 2: SR 4.2;

- SL-C (DC, система управления) 3: SR 4.2 (1);
- SL-C (DC, система управления) 4: SR 4.2 (1).

8.5 SR 4.3 — Использование криптографии

8.5.1 Требование

Если необходима криптография, то система управления должна использовать криптографические алгоритмы, длину ключей и механизмы для создания и управления ключами в соответствии с общепринятыми практиками и рекомендациями индустрии безопасности.

8.5.2 Целесообразность и дополнительная методологическая основа

Выбор криптографической защиты по возможности должен сопоставляться с ценностью защищаемой информации, последствиями нарушения конфиденциальности информации, временным промежутком, в течение которого информация конфиденциальна, и ограничениями на эксплуатацию системы управления. Это может относиться к хранящейся и/или передаваемой информации. Следует отметить, что резервные копии являются примером хранящейся информации, при этом резервные копирования должны по возможности рассматриваться как часть процесса оценки конфиденциальности данных. Поставщик продуктов систем управления по возможности должен документировать практики и процедуры, относящиеся к созданию и управлению криптографическими ключами. Система управления по возможности должна использовать общепринятые и протестированные алгоритмы шифрования и хеширования, например, серии улучшенного стандарта шифрования (AES) и безопасного алгоритма хеширования (SHA), и размеры ключей на основе установленного стандарта. Генерация ключей должна осуществляться с использованием эффективного генератора случайных чисел. Политики и регламенты безопасности для управления ключами должны учитывать периодические смены ключей, уничтожение ключей, распределение ключей и дублирование ключей шифрования в соответствии с установленными стандартами. Общепринятые практики и рекомендации можно найти в таких документах, как NIST SP800-57 [25]. Требования по реализации можно найти, например, в ИСО/МЭК 19790 [12].

Это SR, а также 5.10, SR 1.8 — Сертификаты инфраструктуры открытых ключей (PKI), могут быть применимы в ходе обеспечения соответствия многим другим требованиям, определенным в настоящем стандарте.

8.5.3 Расширения требований

Отсутствуют.

8.5.4 Уровни безопасности

Далее приведены требования для уровней SL, относящихся к SR 4.3 — Использование криптографии:

- SL-C (DC, система управления) 1: SR 4.3;
- SL-C (DC, система управления) 2: SR 4.3;
- SL-C (DC, система управления) 3: SR 4.3;
- SL-C (DC, система управления) 4: SR 4.3.

9 FR 5 — Ограничение потока данных

9.1 Назначение и описания SL-C(RDF)

Сегментировать систему управления на зоны и тракты для ограничения ненужного потока данных:

- SL 1 — предотвращать случайный или непредумышленный обход сегментации на зоны и тракты;
- SL 2 — предотвращать умышленный обход сегментации на зоны и тракты субъектами, которые используют простые средства, имеют незначительные ресурсы, посредственные навыки и низкую мотивацию;
- SL 3 — предотвращать умышленный обход сегментации на зоны и тракты субъектами, которые используют изощренные средства, имеют умеренные ресурсы, специальные познания в IACS и умеренную мотивацию;
- SL 4 — предотвращать умышленный обход сегментации на зоны и тракты субъектами, которые используют изощренные средства, имеют обширные ресурсы, специальные познания в IACS и высокую мотивацию.

9.2 Целесообразность

Используя собственную методологию оценки рисков, собственники имущественных объектов должны определять необходимые ограничения на поток информации, а значит, в качестве дополнения, и определять конфигурацию трактов, используемых для передачи этой информации. Производные регламентированные рекомендации и директивы по возможности должны затрагивать механизмы, начиная от отсоединения сетей систем управления от корпоративных или общедоступных сетей и заканчивая использованием однонаправленных шлюзов, межсетевых экранов с отслеживанием состояния соединений и зон ДМЗ, для управления потоком информации.

9.3 SR 5.1 — Сегментация сети

9.3.1 Требование

Система управления должна обеспечивать возможность логического разграничения сетей систем управления относительно сетей, не относящихся к системам управления, и логического разграничения критически важных сетей систем управления относительно других сетей систем управления.

9.3.2 Целесообразность и дополнительная методологическая основа

Организации используют сегментацию сетей по ряду причин, включая кибербезопасность. Основными причинами сегментирования сетей являются снижение возможности раскрытия информации о сетевом трафике за пределы системы управления или возможности поступления сетевого трафика в систему управления извне, а также снижение возможностей распространения или выхода сетевого трафика за пределы системы управления. Это повышает общее быстродействие и надежность системы, а также являет собой меру киберзащиты. Кроме того, это позволяет разграничить различные сетевые сегменты в системе управления, включая критически важные системы управления и системы обеспечения безопасности относительно других систем для обеспечения дополнительного уровня защиты.

Доступ из системы управления во всемирную паутину (WWW) по возможности должен быть явно регламентирован на основе требований к эксплуатации системы управления.

Сегментация сети и уровень защиты, который она обеспечивает, будут сильно варьироваться в зависимости от общей архитектуры сети, используемой собственником на объекте, а также от системного интегратора и применяемых им систем управления. Логическая сегментация сетей на основе их функциональности обеспечивает некоторую степень защиты, но в то же время может порождать единые точки отказа, если нарушена безопасность сетевого устройства. Физическая сегментация сетей обеспечивает другой уровень защиты за счет устранения этой предпосылки единых точек отказа, но обуславливает более сложный и дорогостоящий проект сети. Эти преимущества и недостатки должны быть проанализированы в ходе проектирования сети (см. МЭК 62443-2-1).

В случае инцидента в качестве ответной меры может потребоваться разрыв соединения между различными сегментами сетей. При этом событии сервисы, необходимые для поддержания жизненно важных процессов, по возможности должны продолжать работу таким образом, чтобы устройства могли функционировать корректно и/или отключились надлежащим образом. При этом может потребоваться дублирование некоторых серверов в сети систем управления для поддержания стандартных сетевых компонентов, например DHCP, DNS или локальных CA. Это может также означать, что некоторые критически важные системы управления и системы обеспечения безопасности необходимо с самого начала проектировать с учетом их полной изоляции от других сетей.

9.3.3 Расширения требований

9.3.3.1 SR 5.1 RE 1 — Физическая сегментация сети

Система управления должна обеспечивать возможность физического разграничения сетей систем управления относительно сетей, не относящихся к системам управления, и физического разграничения критически важных сетей систем управления относительно некритически важных сетей систем управления.

9.3.3.2 SR 5.1 RE 2 — Независимость от сетей, не относящихся к системам управления

Система управления должна иметь возможность поставки сетевых сервисов в сети систем управления, как критически важные, так и нет, без соединения с сетями, не относящимися к системам управления.

9.3.3.3 SR 5.1 RE 3 — Логическая и физическая изоляция критически важных сетей

Система управления должна обеспечивать возможность логической и физической изоляции сетей критически важных систем управления от не критически важных сетей систем управления.

9.3.4 Уровни безопасности

Далее приведены требования для уровней SL, относящихся к SR 5.1 — Сегментация сети:

- SL-C (RDF, система управления) 1: SR 5.1;
- SL-C (RDF, система управления) 2: SR 5.1 (1);
- SL-C (RDF, система управления) 3: SR 5.1 (1) (2);
- SL-C (RDF, система управления) 4: SR 5.1 (1) (2) (3).

9.4 SR 5.2 — Защита границ зоны

9.4.1 Требование

Система управления должна обеспечивать возможность мониторинга и управления коммуникациями на границах зон для обеспечения секционирования, определенного в модели зон и трактов, основанной на рисках.

9.4.2 Целесообразность и дополнительная методологическая основа

Любые соединения с внешними сетями или другими системами управления по возможности должны осуществляться посредством управляемых интерфейсов, состоящих из соответствующих устройств защиты границ (например, прокси-серверов, шлюзов, маршрутизаторов, межсетевых экранов, однонаправленных шлюзов, стражей и зашифрованных туннелей), размещенных в соответствии с эффективной архитектурой (например, межсетевые экраны, защищающие шлюзы приложений, базирующиеся в ДМЗ). Средства защиты границ систем управления, расположенные на любых выделенных альтернативных участках обработки сигналов, должны по возможности обеспечивать те же уровни защиты, что и уровень защиты на границах основного участка.

Как часть стратегии эшелонированной защиты, высокоэффективные системы управления по возможности должны быть подразделены на отдельные зоны, использующие тракты, для ограничения или запрещения сетевого доступа в соответствии с политиками и регламентами безопасности и оценкой риска. Классификация SL-T(система) служит руководством к определению подходящих вариантов для подразделения на зоны (см. МЭК 62443-3-2 [8]).

9.4.3 Расширения требований

9.4.3.1 SR 5.2 RE 1 — Отказ по умолчанию, разрешение по исключению

Система управления должна обеспечивать возможность сброса сетевого трафика по умолчанию и пропуска сетевого трафика по исключению (соответствующие названия — «сбросить все», «разрешить по исключению»).

9.4.3.2 SR 5.2 RE 2 — Островной режим

Система управления должна обеспечивать возможность предотвращения любых коммуникаций через границу системы управления (так называемый островной режим).

Примечание — Эта возможность может быть применена, например, в случае обнаружения нарушения и/или бреши в безопасности системы управления, или совершающейся атаки на уровне предприятия (см. также 4.2, Поддержка жизненно важных функций).

9.4.3.3 SR 5.2 RE 3 — Закрытие при отказе

Система управления должна обеспечивать возможность предотвращения любых коммуникаций через границу системы управления в случае эксплуатационного отказа механизмов защиты границ (соответствует понятию «закрытие при отказе»). Эта функциональность «закрытие при отказе» должна быть рассчитана таким образом, чтобы быть совместимой с работой SIS или другими функциями по обеспечению безопасности.

Примечание — Примеры применения этой возможности включают в себя сценарии, при которых аппаратный сбой или сбой электропитания провоцирует работу устройств защиты границ в режиме ограниченной функциональности или полный отказ этих устройств (см. также 4.2, Поддержка жизненно важных функций).

9.4.4 Уровни безопасности

Далее приведены требования для уровней SL, относящихся к SR 5.2 — Защита границ зоны:

- SL-C (RDF, система управления) 1: SR 5.2;
- SL-C (RDF, система управления) 2: SR 5.2 (1);
- SL-C (RDF, система управления) 3: SR 5.2 (1) (2) (3);
- SL-C (RDF, система управления) 4: SR 5.2 (1) (2) (3).

9.5 SR 5.3 — Ограничения на передачу общецелевой информации «абонент — абонент»

9.5.1 Требование

Система управления должна обеспечивать возможность предотвращения получения общецелевых сообщений «абонент — абонент» пользователями или системами, находящимися за пределами системы управления.

9.5.2 Целесообразность и дополнительная методологическая основа

Системы передачи общецелевой информации «абонент — абонент» включают в себя, но не ограничиваются этим: системы обмена электронной корреспонденцией, разного рода социальные медиа (Твиттер, Фейсбук, галереи изображений и т. д.) или любые системы обмена сообщениями, допускающие передачу исполнимых файлов любых типов. Эти системы обычно используются в личных целях, которые никак не связаны с операциями систем управления, а потому риски, привносимые этими системами, обычно превалируют над любой кажущейся пользой.

Такого рода системы передачи общецелевой информации являют собой векторы атак, широко используемые для внедрения вредоносного программного обеспечения в систему управления, передачи информации, для которой существует авторизация на осуществление операции чтения, на участки за пределами системы управления, и внесения в сеть чрезмерной нагрузки, которая может быть использована для создания проблем безопасности или осуществления атак на систему управления. Адекватные компенсационные контрмеры для соответствия этому требованию может обеспечить применение широкого спектра других системных требований, затрагивающих, например, ограничения использования и ограничение потока данных, как описано в других местах настоящего стандарта, для систем передачи общецелевой информации «абонент — абонент».

Система управления может обеспечивать возможность применения такого рода систем двусторонней связи, но только между серверами и/или рабочими станциями в составе системы управления. Следует отметить, что это SR должно поддерживать требования, соотносящиеся с 8.3, SR 4.1 — Конфиденциальность информации.

Система управления может также ограничивать электронную почту или иные решения для обмена сообщениями, обеспечивающие связь от внутренних компьютеров к внешним компьютерам посредством исходящих сообщений. Эти соединения могут быть ограничены в целях отправки системных уведомлений или других информационных сообщений, генерируемых компьютером, пользователям или системам за пределами системы управления. Для предотвращения передачи информации, для которой поддерживается явная авторизация на осуществление операции чтения, следует использовать преконфигурируемые сообщения (возможно, с возможностью включения в них некоторого ограниченного количества текста) для передачи уведомлений или информации о состоянии. Пользователи не должны наделяться возможностью присоединения файлов или другой информации к этим сугубо исходящим сообщениям во время создания сообщений системой.

9.5.3 Расширения требований

9.5.3.1 SR 5.3 RE 1 — Запрет на любую передачу общецелевой информации «абонент — абонент»

Система управления должна обеспечивать возможность предотвращения как передачи, так и приема общецелевых сообщений «абонент — абонент».

9.5.3.2 Пусто

9.5.4 Уровни безопасности

Далее приведены требования для уровней SL, относящихся к SR 5.3 — Ограничения на передачу общецелевой информации «абонент — абонент»:

- SL-C (RDF, система управления) 1: SR 5.3;
- SL-C (RDF, система управления) 2: SR 5.3;
- SL-C (RDF, система управления) 3: SR 5.3 (1);
- SL-C (RDF, система управления) 4: SR 5.3 (1).

9.6 SR 5.4 — Разбиение приложений

9.6.1 Требование

Система управления должна обеспечивать возможность поддержания разделения данных, приложений и сервисов на основе степени их важности для обеспечения реализации модели зонирования.

9.6.2 Целесообразность и дополнительная методологическая основа

Разделение может осуществляться с помощью физических или логических средств с использованием различных компьютеров, различных центральных процессорных устройств, различных реали-

заций операционной системы, различных сетевых адресов и комбинаций этих или других методов в случае необходимости. Примеры прикладных систем и сервисов, которые могут рассматриваться в качестве различных сегментов, включают в себя, но не ограничиваются этим, аварийные системы и/или системы физической безопасности, прикладные системы управления по замкнутому контуру, а также рабочие станции операторов и инженеров.

9.6.3 Расширения требований

Отсутствуют.

9.6.4 Уровни безопасности

Далее приведены требования для уровней SL, относящихся к SR 5.4 — Разбиение приложений;

- SL-C (RDF, система управления) 1: SR 5.4;
- SL-C (RDF, система управления) 2: SR 5.4;
- SL-C (RDF, система управления) 3: SR 5.4;
- SL-C (RDF, система управления) 4: SR 5.4.

10 FR 6 — Своевременный отклик на события

10.1 Назначение и описания SL-C(TRE)

Реагирование на нарушения безопасности посредством уведомления соответствующего ответственного лица или органа, приведения необходимых свидетельств нарушения и осуществления своевременного корректирующего действия, когда выявлены инциденты:

- SL 1 — отслеживать функционирование IACS и реагировать на выявленные инциденты посредством сбора и предоставления данных об инциденте в случае их запроса;
- SL 2 — отслеживать функционирование IACS и реагировать на выявленные инциденты посредством активного сбора и периодического представления данных об инциденте;
- SL 3 — отслеживать функционирование IACS и реагировать на выявленные инциденты посредством активного сбора и доведения данных об инциденте до сведения соответствующего ответственного лица или органа;
- SL 4 — отслеживать функционирование IACS и реагировать на выявленные инциденты посредством активного сбора и доведения данных об инциденте до сведения соответствующего ответственного лица или органа практически в режиме реального времени.

10.2 Целесообразность

Используя свою методологию оценки рисков, собственники имущественных объектов по возможности должны устанавливать политики и регламенты безопасности, а также должные пути взаимодействия и управления, необходимые для реагирования на нарушения безопасности. Полученные предписания и директивы по возможности должны предусматривать механизмы для сбора, представления, сохранения и автоматического сопоставления данных об инциденте для осуществления своевременного корректирующего действия. Использование инструментов и технологий мониторинга по возможности не должно отрицательно сказываться на эксплуатационных характеристиках системы управления.

10.3 SR 6.1 — Доступность файлов регистрации аудита

10.3.1 Требование

Система управления должна обеспечивать возможность доступа авторизованных физических лиц и/или инструментов к файлам регистрации аудита в режиме «только чтение».

10.3.2 Целесообразность и дополнительная методологическая основа

Система управления генерирует записи аудита о событиях, происходящих в системе (см. 6.10, SR 2.8 — События, подлежащие аудиту). Доступ к этим файлам регистрации аудита необходим для отбора файлов регистрации аудита, выявления и удаления избыточной информации, анализа и представления информации об активности в ходе исследований постфактум инцидентов безопасности. Этот доступ по возможности не должен приводить к изменению исходных записей аудита. В общем случае предварительная обработка данных и генерация отчетов аудита по возможности должны осуществляться в отдельной информационной системе. Ручного доступа к записям аудита (таким, как экранные изображения или распечатки) достаточно для обеспечения выполнения базового требования, но не достаточно с точки зрения более высоких SL. Программный доступ обычно используется для подачи

информации из файлов регистрации аудита к механизмам анализа, таким как SIEM. В разделах 5, 6 и 9 представлены родственные SR, касающиеся создания, защиты и доступа к файлам регистрации аудита.

10.3.3 Расширения требований

10.3.3.1 SR 6.1 RE 1 — Программный доступ к файлам регистрации аудита

Система управления должна обеспечивать программный доступ к записям аудита посредством интерфейса программирования приложений (API).

10.3.3.2 Пусто

10.3.4 Уровни безопасности

Далее приведены требования для уровней SL, относящихся к SR 6.1 — Доступность файлов регистрации аудита:

- SL-C (TRE, система управления) 1: SR 6.1;
- SL-C (TRE, система управления) 2: SR 6.1;
- SL-C (TRE, система управления) 3: SR 6.1 (1),
- SL-C (TRE, система управления) 4: SR 6.1 (1).

10.4 SR 6.2 — Непрерывный мониторинг

10.4.1 Требование

Система управления должна обеспечивать возможность непрерывного мониторинга функционирования всех механизмов безопасности посредством общепринятых практик и рекомендаций индустрии безопасности для оперативного обнаружения, описания и информирования о брешах в безопасности.

Примечание — Время реагирования — вопрос частный и выходит за рамки настоящего стандарта.

10.4.2 Целесообразность и дополнительная методологическая основа

Возможность мониторинга системы управления может быть достигнута посредством самых разнообразных инструментов и технологий (например, систем IDS, IPS, механизмов защиты от вредоносного кода и механизмов мониторинга сети). Поскольку атаки становятся все более изощренными, эти инструменты и технологии мониторинга также должны усложняться и включать в себя, например, IDS/IPS на основе анализа поведения.

С точки зрения стратегии устройства мониторинга по возможности должны применяться внутри системы управления (например, на определенных участках периметра и вблизи серверных ферм, поддерживающих критически важные приложения) для сбора жизненно важной информации. Механизмы мониторинга могут быть применены и на нерегламентированных участках внутри системы управления для отслеживания конкретных трансакций.

Мониторинг по возможности должен включать в себя использование подходящих механизмов отчетности для обеспечения своевременного реагирования на события. Для того, чтобы поддерживать сфокусированность отчетности, а объем представляемой информации — на уровне, при котором она может быть обработана получателями, обычно применяются такие механизмы, как SIEM, для соотнесения отдельных событий с общими отчетами, предоставляющими более обширный контекст, в котором произошли исходные события.

Кроме того, эти механизмы могут использоваться для отслеживания эффекта изменений в безопасности системы управления (см. 6.10 SR 2.8 — События, подлежащие аудиту). Предварительная установка инструментов экспертного анализа может помочь в анализе инцидентов.

10.4.4 Уровни безопасности

Далее приведены требования для уровней SL, относящихся к SR 6.2 — Непрерывный мониторинг:

- SL-C (TRE, система управления) 1: не определено;
- SL-C (TRE, система управления) 2: SR 6.2;
- SL-C (TRE, система управления) 3: SR 6.2;
- SL-C (TRE, система управления) 4: SR 6.2.

11 FR 7 — Работоспособность и доступность ресурсов

11.1 Назначение и описания SL-C(RA)

Обеспечивать работоспособность и доступность системы управления в противовес ухудшению ее функциональности или отказу в жизненно важных сервисах:

- SL 1 — обеспечить, чтобы система управления функционировала надежно при штатных условиях производства и предотвращала ситуации типа DoS, вызванные случайными или непредумышленными действиями субъекта;
- SL 2 — обеспечить, чтобы система управления функционировала надежно при штатных и нештатных условиях производства и предотвращала ситуации типа DoS, спровоцированные субъектами, использующими простые средства при незначительных ресурсах, посредственных навыках и низкой мотивации;
- SL 3 — обеспечить, чтобы система управления функционировала надежно при штатных, нештатных и экстремальных условиях производства и предотвращала ситуации типа DoS, спровоцированные субъектами, использующими изощренные средства при умеренных ресурсах, наличии специальных познаний в IACS и умеренной мотивации;
- SL 4 — обеспечить, чтобы система управления функционировала надежно при штатных, нештатных и экстремальных условиях производства и предотвращала ситуации типа DoS, спровоцированные субъектами, использующими изощренные средства при обширных ресурсах, наличии специальных познаний в IACS и высокой мотивации.

11.2 Целесообразность

Цель этой серии SR — гарантировать, что система управления устойчива к разного рода событиям DoS. Они включают в себя частичную или полную недоступность функциональности системы на различных уровнях. В частности, инциденты безопасности в системе управления по возможности не должны затрагивать функции SIS или другие функции по обеспечению физической безопасности.

11.3 SR 7.1 — Защита от отказа в обслуживании

11.3.1 Требование

Система управления должна обеспечивать возможность функционирования в режиме ограниченной функциональности в ходе события DoS.

11.3.2 Целесообразность и дополнительная методологическая основа

Существует ряд технологий для ограничения или, в некоторых случаях, исключения последствий ситуаций типа DoS. Например, устройства защиты границ позволяют отфильтровывать те или иные типы пакетов для защиты устройств в составе внутренней, доверенной сети от непосредственного воздействия событий DoS или исключения строго однонаправленного потока информации. В частности, как отмечено в разделе 4, событие DoS в системе управления по возможности не должно отрицательно сказываться на каких-либо системах обеспечения физической безопасности.

11.3.3 Расширения требований

11.3.3.1 SR 7.1 RE 1 — Регулировать загрузки линий связи

Система управления должна обеспечивать возможность регулировки загрузок линий связи (например, ограничения интенсивности использования) для смягчения последствий разного рода лавинной адресации информации в ходе событий DoS.

11.3.3.2 SR 7.1 RE 2 — Ограничить последствия DoS для других систем или сетей

Система управления должна обеспечивать возможность ограничения возможности всех пользователей (физических лиц, программных процессов и устройств) провоцировать события DoS, которые затрагивают другие системы управления или сети.

11.3.4 Уровни безопасности

Далее приведены требования для уровней SL, относящихся к SR 7.1 — Защита от отказа в обслуживании:

- SL-C (RA, система управления) 1: SR 7.1;
- SL-C (RA, система управления) 2: SR 7.1 (1);
- SL-C (RA, система управления) 3: SR 7.1 (1) (2);
- SL-C (RA, система управления) 1: SR 7.1 (1) (2).

11.4 SR 7.2 — Управление ресурсами

11.4.1 Требование

Система управления должна обеспечивать возможность ограничения использования ресурсов посредством функций безопасности для предотвращения истощения ресурсов.

11.4.2 Целесообразность и дополнительная методологическая основа

Управление ресурсами (например, сегментация сети или схемы приоритетов) препятствует задержке программного процесса с более низким приоритетом или его непредусмотренному взаимодействию с системой управления, обслуживающей какой-либо программный процесс с более высоким приоритетом. Например, инициирование сканирований сети, внесение в нее патчей и/или антивирусные проверки в привязке к действующей системе могут спровоцировать серьезный сбой штатных процессов. В качестве смягчающей технологии следует по возможности рассматривать схемы ограничения интенсивности трафика.

11.4.3 Расширения требований

Отсутствуют.

11.4.4 Уровни безопасности

Далее приведены требования для уровней SL, относящихся к SR 7.2 — Управление ресурсами:

- SL-C (RA, система управления) 1: SR 7.2;
- SL-C (RA, система управления) 2: SR 7.2;
- SL-C (RA, система управления) 3: SR 7.2;
- SL-C (RA, система управления) 4: SR 7.2.

11.5 SR 7.3 — Резервирование в системе управления

10.5.1 Требование

Система управления должна поддерживать идентичность и расположение критически важных файлов, а также возможность проведения резервирований информации уровня пользователя и уровня системы (включая информацию о состоянии системы) без воздействия на штатные процессы производственного объекта.

11.5.2 Целесообразность и дополнительная методологическая основа

Доступность актуальных резервных копий жизненно важна для восстановления после сбоя системы управления и/или ошибок в конфигурациях. Автоматизация этой функции гарантирует запись всех необходимых файлов, что снижает объем служебных операций операторов. Хотя этого обычно не требуется для восстановления системы управления, информация, необходимая для постинцидентной экспертной деятельности (например, файлы регистрации аудита), по возможности должна быть специально включена в резервную копию (см. 10.4, SR 6.2 — Непрерывный мониторинг).

Если полученные резервные копии содержат конфиденциальную информацию, то следует предусмотреть шифрование (см. 8.5, SR 4.3 — Использование криптографии).

11.5.3 Расширения требований

11.5.3.1 SR 7.3 RE 1 — Верификация резервирования

Система управления должна обеспечивать возможность верификации надежности механизмов резервирования.

11.5.3.2 SR 7.3 RE 2 — Автоматизация резервирования

Система управления должна обеспечивать возможность автоматизации функции резервирования на основе конфигурации частоты создания резервных копий.

11.5.4 Уровни безопасности

Далее приведены требования для уровней SL, относящихся к SR 7.3 — Резервирование в системе управления:

- SL-C (RA, система управления) 1: SR 7.3;
- SL-C (RA, система управления) 2: SR 7.3 (1);
- SL-C (RA, система управления) 3: SR 7.3 (1) (2);
- SL-C (RA, система управления) 4: SR 7.3 (1) (2).

11.6 SR 7.4 — Восстановление и воссоздание системы управления

11.6.1 Требование

Система управления должна обеспечивать возможность ее восстановления и воссоздания до известного безопасного состояния после сбоя или отказа.

11.6.2 Целесообразность и дополнительная методологическая основа

Восстановление и воссоздание системы управления до известного безопасного состояния означают, что все параметры системы (установленные по умолчанию или конфигурируемые) устанавливаются на безопасные значения, переустанавливаются патчи, критически важные для безопасности,

восстанавливаются значения параметров конфигурации, относящиеся к безопасности, делаются доступными системная документация и рабочие регламенты, переинсталлируется прикладное и системное программное обеспечение, которое при этом конфигурируется с учетом параметров безопасности, загружается информация из самых последних, достоверно безопасных резервных копий, полностью тестируется система, после чего ее можно считать полностью функциональной.

11.6.3 Расширения требований

Отсутствуют.

11.6.4 Уровни безопасности

Далее приведены требования для уровней SL, относящихся к SR 7.4 — Восстановление и воссоздание системы управления:

- SL-C (RA, система управления) 1: SR 7.4;
- SL-C (RA, система управления) 2: SR 7.4;
- SL-C (RA, система управления) 3: SR 7.4;
- SL-C (RA, система управления) 4: SR 7.4.

11.7 SR 7.5 — Аварийное питание

11.7.1 Требование

Система управления должна обеспечивать возможность ее подключения к аварийному источнику питания и отключения от него без воздействия на существующее состояние безопасности или наличие предусмотренного и документированного режима ограниченной функциональности.

11.7.2 Целесообразность и дополнительная методологическая основа

Могут возникать ситуации, при которых на компенсационные контрмеры, такие как физический контроль доступа на входе-выходе, может влиять отключение основного питания, поэтому на такой случай должно быть по возможности предусмотрено аварийное питание соответствующих систем. Если это невозможно, то во время такой аварийной ситуации могут потребоваться другие компенсационные контрмеры.

11.7.3 Расширения требований

Отсутствуют.

11.7.4 Уровни безопасности

Далее приведены требования для уровней SL, относящихся к SR 7.5 — Аварийное питание:

- SL-C (RA, система управления) 1: SR 7.5;
- SL-C (RA, система управления) 1: SR 7.5;
- SL-C (RA, система управления) 1: SR 7.5;
- SL-C (RA, система управления) 1: SR 7.5.

11.8 SR 7.6 — Параметры конфигурации сети и безопасности

11.8.1 Требование

Система управления должна обеспечивать возможность ее конфигурирования в соответствии с рекомендованными конфигурациями сети и безопасности, как описано в руководящих документах, предоставленных поставщиком системы управления. Система управления должна обеспечивать интерфейс для текущих параметров конфигурации сети и безопасности.

11.8.2 Целесообразность и дополнительная методологическая основа

Эти параметры конфигурации — регулируемые параметры компонентов системы управления. Для того, чтобы было возможно отслеживать и корректировать любые отклонения от утвержденных и/или рекомендованных параметров конфигурации, система управления должна поддерживать мониторинг и управление изменениями параметров конфигурации в соответствии с политиками и регламентами безопасности. Для повышения безопасности может выполняться автоматическая проверка, при которой текущие параметры автоматически собираются агентом и сравниваются с утвержденными параметрами.

11.8.3 Расширения требований

11.8.3.1 SR 7.6 RE 1 — Машиночитаемая отчетность о текущих параметрах безопасности

Система управления должна обеспечивать возможность генерации отчета с перечнем текущих параметров безопасности в машиночитаемом формате.

11.8.3.2 Пусто

11.8.4 Уровни безопасности

Далее приведены требования для уровней SL, относящихся к SR 7.6 — Параметры конфигурации сети и безопасности:

- SL-C (RA, система управления) 1: SR 7.6;
- SL-C (RA, система управления) 2: SR 7.6;
- SL-C (RA, система управления) 3: SR 7.6 (1);
- SL-C (RA, система управления) 4: SR 7.6 (1).

11.9 SR 7.7 — Минимальная функциональность

11.9.1 Требование

Система управления должна обеспечивать возможность избирательного запрещения и/или ограничения использования ненужных функций, портов, протоколов и/или сервисов.

11.9.2 Целесообразность и дополнительная методологическая основа

Системы управления способны предоставлять широкий спектр функций и сервисов. Некоторые из предоставляемых функций и сервисов могут не требоваться для поддержания жизненно важных функций. Поэтому функции, выходящие за рамки базовой конфигурации, должны быть по возможности деактивированы по умолчанию. Кроме того, иногда целесообразно предоставлять более одного сервиса из одного компонента системы управления, однако в результате возрастает риск превышения предельного количества сервисов, предоставляемых отдельно взятым компонентом. Многие функции и сервисы, обычно предоставляемые COTS, могут претендовать на исключение, например электронная почта, IP-телефония, IM, FTP, HTTP и совместный доступ к файлам.

11.9.3 Расширения требований

Отсутствуют.

11.9.4 Уровни безопасности

Далее приведены требования для уровней SL, относящихся к SR 7.7 — Минимальная функциональность:

- SL-C (RA, система управления) 1: SR 7.7;
- SL-C (RA, система управления) 2: SR 7.7;
- SL-C (RA, система управления) 3: SR 7.7;
- SL-C (RA, система управления) 4: SR 7.7.

11.10 SR 7.8 — Инвентаризация компонентов системы управления

11.10.1 Требование

Система управления должна обеспечивать возможность предоставления отчетов с актуальными перечнями установленных компонентов и соответствующих им свойств.

11.10.2 Целесообразность и дополнительная методологическая основа

Инвентарная ведомость компонентов системы управления может содержать, но не ограничивается этим, ID компонентов, а также потенциальный и пересмотренный уровни. Инвентарная ведомость компонентов по возможности должна соотноситься с рассматриваемой системой. По возможности должен применяться формализованный процесс управления конфигурацией для отслеживания изменений в исходной инвентарной ведомости компонентов (см. МЭК 62443-2-1).

11.10.3 Расширения требований

Отсутствуют.

11.10.4 Уровни безопасности

Далее приведены требования для уровней SL, относящихся к SR 7.8 — Инвентаризация компонентов системы управления:

SL-C (RA, система управления) 1: не определено;

SL-C (RA, система управления) 2: SR 7.8;

SL-C (RA, система управления) 3: SR 7.8;

SL-C (RA, система управления) 4: SR 7.8 .

Приложение А
(справочное)

Описание вектора SL

Примечание 1 — Данное приложение основано на документе «Уровни обеспечения безопасности: векторный подход к описанию требований безопасности» [28]. Содержание этого исходного документа преобразовано в содержание данного приложения в соответствии с изменениями в серии МЭК 62443 и комментариями, полученными от рецензентов.

Примечание 2 — Первоисточниками большей части материала, содержащегося в данном приложении, являются МЭК 62443-1-1 и МЭК 62443-3-2. На момент публикации настоящего документа эти документы разрабатывались и/или перерабатывались и не содержали материала по вектору SL. Данное приложение приведено в целях разъяснения читателю концепции вектора SL. Материал данного приложения — информативный и может быть замещен любым обязательным содержимым вышеперечисленных стандартов.

А.1 Обзор

Системы физической безопасности используют концепцию SIL уже почти двадцать лет. Это позволяет представить потенциальную целостность физической безопасности того или иного компонента или уровень целостности физической безопасности применяемой системы одним числом, которое характеризует коэффициент защищенности, необходимый для обеспечения охраны труда и безопасности людей или среды на основе вероятности отказа этого компонента или системы. Процесс определения необходимого фактора защищенности для системы физической безопасности хоть и сложен, но осуществим, поскольку вероятность отказа компонента или системы из-за случайных отказов аппаратного обеспечения может быть измерена в количественном отношении. Общий риск может быть рассчитан на основе потенциальных последствий этих отказов для HSE.

Системы информационной безопасности характеризуются значительно более широкой применимостью, более широким набором последствий и значительно большим набором возможных обстоятельств, ведущих к возможному событию. Подразумевается, что системы информационной безопасности служат для защиты HSE, но также и самого производственного процесса, проприетарной информации организации, общественного доверия и государственной безопасности, наряду с другими вещами в ситуациях, когда случайные отказы аппаратного обеспечения не могут быть основной причиной. В одних случаях виновником может быть благонамеренный сотрудник, допускающий ошибку, а в других — злоумышленник, стремящийся спровоцировать событие и скрыть улики. Возрастающая сложность систем информационной безопасности значительно затрудняет описание фактора защищенности одним числом.

А.2 Уровни безопасности

А.2.1 Определение

Далее приведена выдержка из МЭК/ТС 62443-1-1:2009 (см. 5.11.1), в которой в наглядной форме объясняется, что такое уровни SL и как их можно использовать.

Уровни безопасности обеспечивают качественный подход к рассмотрению безопасности зоны. Как качественный метод определение уровня безопасности применяется для сравнения и управления безопасностью зон внутри организации. По мере доступности новых данных и разработки математических моделей риска, угроз и инцидентов безопасности эта концепция уступит место количественному подходу к выбору и верификации SL. Этот подход будет целесообразно применять как организациям конечных пользователей, так и поставщикам продуктов IACS и безопасности. Этот подход будет служить для выбора устройств IACS и контрмер, применяемых внутри зоны, а также для выявления и сравнения безопасности зон в различных организациях отраслевых сегментов.

На своем первом этапе разработки серия стандартов МЭК 62443 оперирует больше качественными SL, используя такие термины, как «низкий», «средний» и «высокий». От собственника объекта потребуется представить собственное определение того, что значат эти классификации применительно к его конкретной прикладной системе. Долгосрочная цель серии МЭК 62443 — свести как можно больше уровней и требований безопасности к количественным описаниям, требованиям и системам показателей для создания условий повторной применимости стандарта в пределах группы организаций и отраслей промышленности. Достижение этой цели займет время, поскольку потребуется приобретение дополнительного опыта применения стандартов и данных к промышленным системам безопасности для мотивирования количественного подхода.

При соотнесении требований с различными SL разработчикам стандартов необходима некая система критериев, описывающая значение различных SL и их взаимные отличия. Задача данного приложения — предложить такую систему критериев.

А.2.2 Типы SL

SL разбиты на три различных типа: целевые, достигнутые и потенциальные. Эти типы, будучи взаимосвязаны, затрагивают разные аспекты жизненного цикла безопасности:

- **целевые SL (SL-T)** — это желаемые уровни безопасности для отдельно взятой системы. Эти уровни обычно определяются посредством выполнения оценки рисков для системы и установления того, что она нуждается в конкретном уровне безопасности для гарантированного обеспечения своего корректного функционирования;
- **достигнутые SL (SL-A)** — это фактические уровни безопасности для отдельно взятой системы. Эти уровни измеряются после доступности проекта системы или когда система установлена и действует. Они служат для установления того, что система безопасности отвечает целям, которые были с самого начала обозначены в целевых SL;
- **потенциальные SL (SL-C)** — это уровни безопасности, которые могут обеспечивать компоненты или системы, будучи корректно сконфигурированными. Эти уровни указывают, что тот или иной компонент или система изначально способны соответствовать целевым SL без помощи дополнительных компенсационных контрмер, будучи корректно сконфигурированными и интегрированными.

Каждый из этих SL рассчитан на использование на разных этапах жизненного цикла безопасности в соответствии с серией МЭК 62443. Начиная с формулировки цели для конкретной системы: организации потребуется разработать проект, который освещал бы потенциальные возможности для достижения желаемого результата. Другими словами, команде разработчиков сначала предстоит разработать целевой SL, необходимый для конкретной системы. Затем им предстоит разработать систему, отвечающую этим целям, как правило — методом итерационного подхода, при котором после каждой итерации достигнутые SL выдвинутого проекта определяются и сравниваются с целевыми SL. В качестве составляющей такого подхода разработки разработчикам предстоит выбрать компоненты и системы, для которых необходимые потенциальные SL должны соответствовать требованиям целевых SL, или же, в случае недоступности таких систем и компонентов, дополнить доступные компоненты и системы компенсационными контрмерами. После сдачи системы в эксплуатацию предстоит определить фактический SL, являющий собой достигнутый SL, и сравнить его с целевым SL.

А.2.3 Применение уровней SL

При разработке новой системы (зеленое поле) или пересмотре безопасности существующей системы (коричневое поле) первым шагом необходимо разбить систему на разные зоны и определить тракты, связывающие эти зоны между собой там, где это необходимо. Подробности по осуществлению этого приведены в МЭК 62443-3-2. Как только установлена зональная модель системы, каждой зоне и тракту присваивается целевой SL, на основе анализа последствий, который описывает желаемую безопасность для соответствующей зоны или тракта. Во время этого исходного анализа зон и трактов не нужно завершать детальный проект системы. Достаточно описать функциональность, которую по возможности должны обеспечивать объекты в зоне, и соединения между зонами, чтобы достигались цели безопасности.

Рисунки А.1 и А.2 иллюстрируют общие примеры систем, разбитых на зоны, соединенные между собой трактами. На рисунке А.1 представлено графическое изображение системы управления станцией загрузки цистерны с хлорином. Полный сценарий использования, дополняющий этот рисунок, будет рассмотрен в МЭК/ТТ 62443-1-4. На рисунке показано пять зон: BPCS, SIS, центр управления, DMZ производственного объекта и предприятие. И BPCS, и SIS используют контроллеры PLC для управления различными аспектами станции загрузки, при этом SIS использует специальный PLC функциональной безопасности (PLC-FS), рассчитанный на использование в системах физической безопасности. Оба PLC соединены между собой через немаршрутизируемое последовательное или Интернет-соединение с использованием устройства защиты границ. Каждый из PLC соединен с местным коммутатором, который осуществляет переключение между рабочей станцией инженера, предназначенной для программирования, и устройством HMI, предназначенным для управления. Зоны с BPCS и SIS содержат также IAMS, предназначенную для снятия показаний с контрольно-измерительных приборов и их поверки. Центр управления, содержащий серию рабочих станций, и BPCS соединены с DMZ производственного объекта. DMZ производственного объекта может содержать самые разнообразные компоненты и системы, например сервер-архиватор и рабочую станцию техобслуживания, как показано на рисунке. DMZ производственного объекта показана в соединении с корпоративными системами, которые содержат корпоративную WLAN и веб-сервер. На рисунке показано несколько контроллеров домена и устройств защиты границ для обозначения некоторых контрмер, которые могут применяться для повышения безопасности.

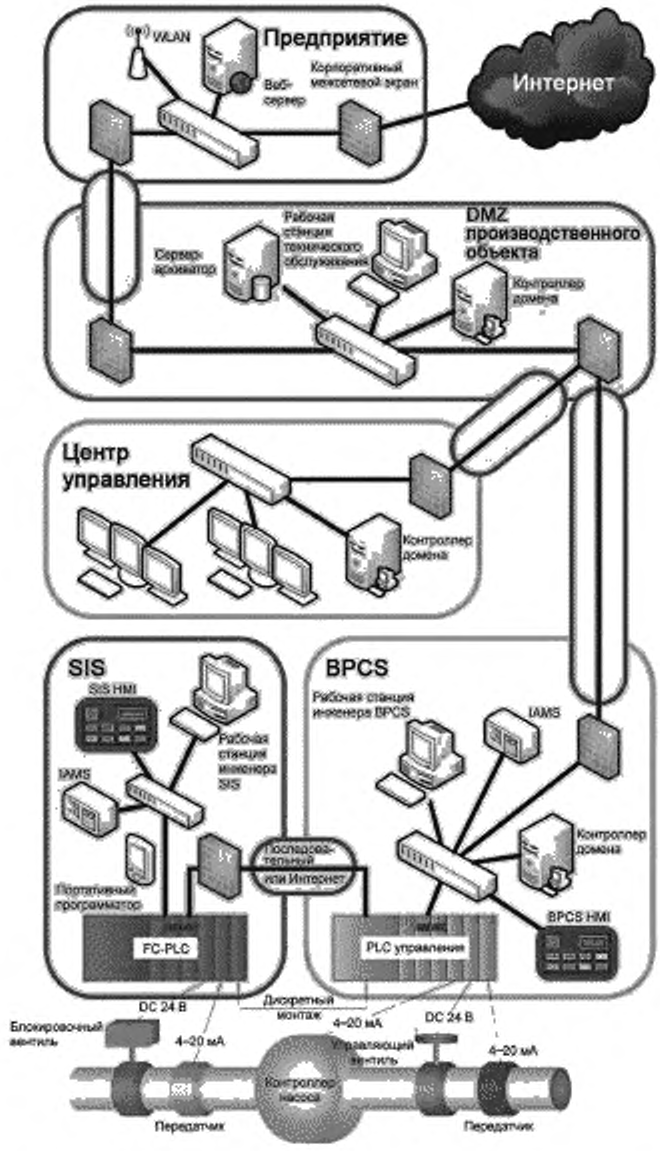

Рисунок А.1 — Общий пример из обрабатывающей промышленности, иллюстрирующий зоны и тракты

На рисунке А.2 представлено графическое изображение производственного объекта. Он содержит четыре обозначенные зоны: корпоративную сеть, промышленно-корпоративную DMZ и две промышленные сети. Корпоративная инфраструктура включает в себя WLAN и соединение с Интернетом. Многие организации используют DMZ между важными частями их систем, предназначенную для изоляции сетевого трафика. В данном конкретном примере каждая промышленная сеть функционирует относительно независимо от другой промышленной сети и при этом содержит свой PLC, периферийные устройства и HMI.

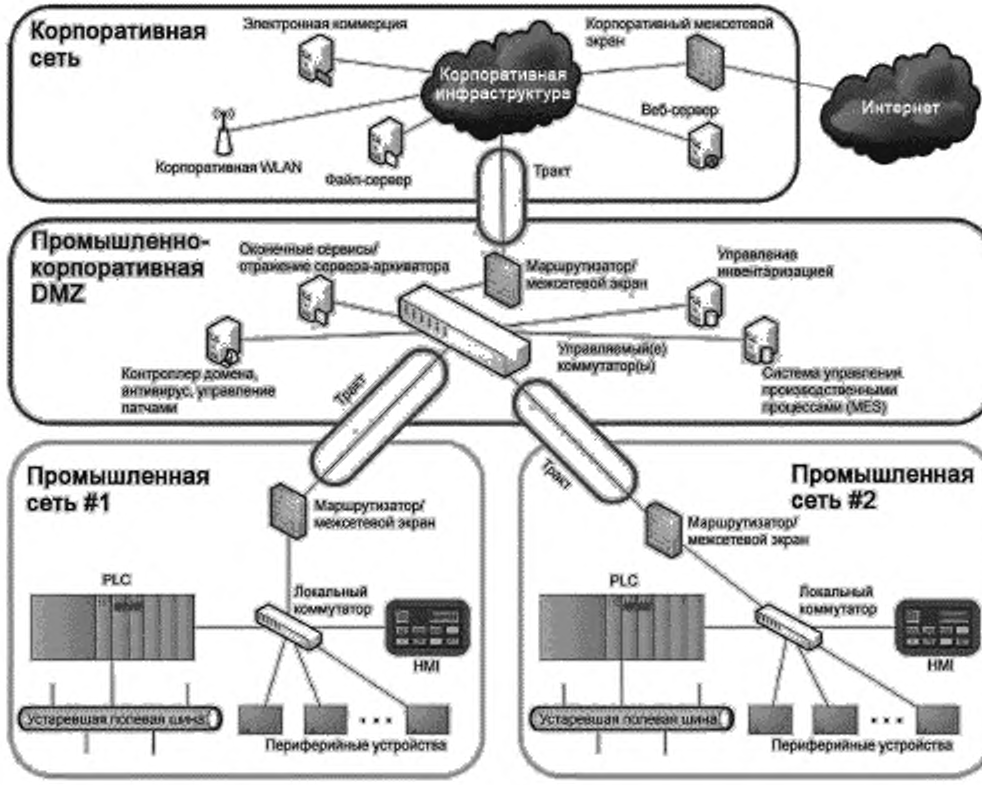

Рисунок А.2 — Общий пример производства, иллюстрирующий зоны и тракты

После определения целевых SL система может быть разработана (зеленое поле) или переработана (коричневое поле) в целях соответствия этим целевым SL. Процесс разработки обычно являет собой итеративный подход, при котором проект системы сравнивается с целью несколько раз в процессе его разработки. Ряд частей серии МЭК 62443 содержит методологическую основу по различным аспектам программных и технических требований, которые появляются в процессе разработки. МЭК 62443-2-1 предоставляет методологическую основу по программным аспектам процесса разработки, в то время как МЭК 62443-3-3 (настоящий стандарт) и МЭК 62443-4-2 [10] обозначают требования технической безопасности уровня системы и уровня компонентов и соотносят их с различными потенциальными SL.

В процессе разработки системы необходимо оценить характеристики безопасности различных компонентов и подсистем. Поставщики продуктов должны будут предоставлять эти характеристики в виде потенциальных SL для их компонентов или систем, сопоставив признаки и характеристики с требованиями, определенными в серии МЭК 62443 для различных потенциальных SL. Эти потенциальные SL могут служить для определения того, может ли тот или иной компонент или система соответствовать целевому SL системы. Поставщик продуктов или системный интегратор должен будет также предоставить методологическую основу по конфигурированию компонента или системы для их соответствия заявленным SL.

Вероятно, что в отдельно взятом проекте будет ряд компонентов или систем, которые не могут полностью соответствовать целевому SL. В случае, если потенциальный SL компонента или системы ниже целевого SL, должны быть предусмотрены компенсационные контрмеры для обеспечения соответствия желаемому целевому SL. Компенсационные контрмеры могут включать в себя изменение проекта компонента или системы для улучшения их характеристик, подбор другого компонента или системы для обеспечения соответствия целевому SL или добавление дополнительных компонентов или систем для обеспечения соответствия целевому SL. После каждой итерации в процессе разработки достигнутые SL проекта системы следует анализировать повторно для определения того, как они соотносятся с целевыми SL системы.

После утверждения и реализации проекта системы она должна быть проанализирована для предотвращения или смягчения последствий снижения уровня безопасности системы. Ее следует анализировать во время или после модификаций системы и на систематической основе. МЭК 62443-2-1 предоставляет методологическую основу по необходимой последовательности действий для ведения программы безопасности и оценке ее эффективности. После определения достигнутых SL потребуется оценить, соответствует ли система изначальным целевым SL (например, используя системные требования из МЭК 62443-3-3). Если система не соответствует этим требованиям, на то может быть несколько причин, включая недостаточное сопровождение программы или необходимость переработки частей системы.

В сущности, характеристики безопасности системы управления определяются независимо от контекста отдельно взятого использования, но используются в отдельно взятом контексте для достижения целевого SL архитектуры, зон и/или трактов соответствующей системы (см. рисунок А.3).

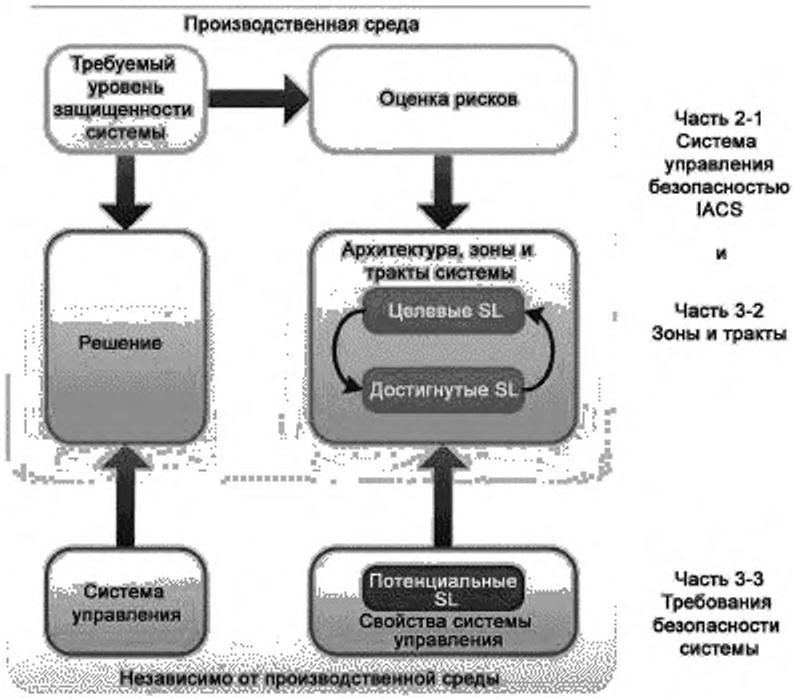

Рисунок А.3 — Схема взаимосвязей использования различных типов SL

А.3 Вектор SL

А.3.1 Фундаментальные требования

Уровни SL основаны на семи FR безопасности, определенных в МЭК 62443-1-1:

1) управление идентификацией и аутентификацией (IAC);
2) контроль использования (UC);
3) целостность системы (SI);
4) конфиденциальность данных (DC);
5) ограничение потока данных (RDF);
6) своевременный отклик на события (TRE) и
7) работоспособность и доступность ресурсов (RA).

Вместо сведения уровней SL к общему знаменателю можно использовать вектор уровней SL, который использует семь вышеуказанных FR в противоположность одному фактору защищенности. Этот вектор SL допускает задание разграничений между SL, соответствующими различным FR, с помощью набора символов. Этот набор символов может быть основан на дополнительных следствиях, привязанных к системам безопасности, или различных посягательствах на цели безопасности, затрагиваемые требованиями FR. Набор символов, используемый

в определениях SL, может раскрывать практические обоснования того, чем одна система безопаснее другой, без необходимости соотнесения всего с последствиями для HSE.

А.3.2 Определения уровней

А.3.2.1 Обзор

Стандарты серии МЭК 62443 определяют уровни SL с точки зрения пяти различных уровней (0, 1, 2, 3 и 4) по степени возрастания безопасности. Актуальная модель для определения SL соотносится с угрозой, которая непрерывно усложняется, и незначительно разнится в зависимости от типа SL, к которому она привязана. Применительно к SL-C это означает, что собственник объекта или системный интегратор способны сконфигурировать конкретный компонент или систему для отражения непрерывно усложняющейся угрозы. Применительно к SL-T это означает, что собственник объекта или системный интегратор определили посредством анализа рисков, что должны защищать данную конкретную зону, систему или компонент от угрозы этого уровня. Применительно к SL-A это означает, что собственник объекта, системный интегратор, поставщик продуктов и/или любое их объединение сконфигурировали зону, систему или компонент для их соответствия конкретным требованиям безопасности, определенным для этого SL.

В формулировках для каждого SL используются такие термины, как «случайный», «непредумышленный», «простой», «изощренный» и «обширный». Эти формулировки умышленно абстрактны, чтобы одни и те же базовые формулировки можно было использовать для всех документов серии МЭК 62443. Каждый отдельный документ серии будет определять требования для уровней SL, которые соотносятся с его конкретными назначениями.

Хотя требования для каждого SL будут различны на протяжении всей серии МЭК 62443, необходимо иметь общее представление о том, от чего по возможности должен защищать каждый SL. Следующие фрагменты предоставят некоторую методологическую основу к разграничению уровней SL.

А.3.2.2 SL 0: Не требуется специальных требований или защиты безопасности

SL 0 имеет несколько значений, зависящих от ситуации, в которой он применяется. В рамках определения SL-C он будет означать, что компонент или система не могут удовлетворять некоторым из требований SL 1 для данного конкретного FR. С наибольшей вероятностью это будет относиться к компонентам или системам, являющимся частью обширной зоны, в которой другие компоненты или системы будут обеспечивать компенсационные контрмеры. При определении SL-T для отдельно взятой зоны он означает, что собственник объектов определил следующее: результаты анализа рисков показывают, что для данного конкретного FR к данному компоненту или системе необходимы специальные требования уровня меньшего, чем полный SL 1. Это будет скорее относиться к отдельным компонентам внутри системы или зоны, никак не влияющим на конкретные FR. При определении SL-A он будет означать, что отдельно взятая зона не может удовлетворять некоторым требованиям SL 1 для данного конкретного FR.

А.3.2.3 SL 1: Защита от случайного или непредумышленного нарушения безопасности

Случайные или непредумышленные нарушения безопасности обычно происходят вследствие нестрогой реализации политик безопасности. Эти нарушения могут быть спровоцированы хорошо осведомленными сотрудниками с вероятностью, сопоставимой с вероятностью угроз от аутсайдеров. Многие из этих нарушений относятся к программе безопасности и смогут быть улажены посредством ужесточения политик и регламентов.

В соответствии с рисунком А.1 простым примером будет оператор, способный изменить уставку на инженерной станции в зоне BPCS до значения, не соответствующего условиям, которые определены инженерным персоналом. Система не установила должных ограничений на аутентификацию и контроль использования, чтобы оператор не смог внести изменения. Также в соответствии с рисунком А.1, другим примером будет пароль, высылаемый открытым текстом по тракту между зоной BPCS и зоной DMZ, что позволяет сетевому инженеру видеть пароль в процессе устранения неполадок в системе. Система не установила должной конфиденциальности данных для защиты пароля. В соответствии с рисунком А.2 третьим примером будет инженер, который собирается получить доступ к PLC в Промышленной сети #1, но в результате получает доступ к PLC в Промышленной сети #2. Система не установила должного ограничения потока данных, что предотвратило бы получение инженером доступа к ошибочной системе.

А.3.2.4 SL 2: Защита от умышленного нарушения безопасности с использованием простых средств при незначительных ресурсах, посредственных навыках и низкой мотивации

Простые средства не требуют обширных познаний со стороны злоумышленника. От злоумышленника не требуется досконального знания безопасности, домена или отдельно взятой системы, на которую совершается атака. Эти векторы атаки хорошо известны, и автоматизированные инструменты могут оказать помощь злоумышленнику. Эти инструменты рассчитаны, среди прочего, для атаки на широкий спектр систем и не ориентированы на одну конкретную систему, поэтому от злоумышленника не требуется значительного уровня мотивации или подручных ресурсов.

В соответствии с рисунком А.1 примером будет вирус, который инфицирует рабочую станцию техобслуживания в DMZ производственного объекта, откуда распространяется на рабочую станцию инженера BPCS, поскольку обе они используют одинаковую универсальную операционную систему. В соответствии с рисунком А.2 другим примером будет злоумышленник, нарушающий безопасность веб-сервера в корпоративной сети посредством эксплойта, загруженного из Интернета, в случае общеизвестной уязвимости в универсальной операционной системе веб-сервера. Злоумышленник использует веб-сервер в качестве отправной точки атаки на другие системы корпоративной сети, а также промышленной сети. Также в соответствии с рисунком А.2 третьим примером будет опера-

тор, просматривающий сайт на HMI, расположенном в Промышленной сети #1, который загружает троян, и этот троян открывает в маршрутизаторах и межсетевых экранах лазейку в Интернет.

А.3.2.5 SL 3: Защита от умышленного нарушения безопасности с использованием изощренных средств, при умеренных ресурсах, наличии специальных познаний в IACS и умеренной мотивации

Изощренные средства подразумевают продвинутые знания безопасности, продвинутые знания доменов, продвинутые знания целевой системы или любую их комбинацию. Злоумышленник, избравший целью систему с SL 3, скорее всего, будет использовать векторы атаки, которые приспособлены к конкретной целевой системе. Для нарушения безопасности системы злоумышленник может использовать эксплойты в операционных системах, которые недостаточно распространены, уязвимости в промышленных протоколах, специальную информацию о конкретной цели или другие средства, требующие наличия мотивации, а также опыта и знаний больших, чем требуются для SL 1 или SL 2.

Примером изощренных средств могут быть инструменты для взлома паролей или ключей, основанные на хеш-таблицах. Эти инструменты доступны для загрузки, но их применение требует знания системы (например, хеша взламываемого пароля). В соответствии с рисунком А.1 примером будет злоумышленник, который получает доступ к PLC-FS через последовательный тракт после получения доступа к управляющему PLC через уязвимость в контроллере Интернет. В соответствии с рисунком А.2 третьим примером будет злоумышленник, который получает доступ к серверу-архиватору через межсетевой экран промышленно-корпоративной ДМЗ посредством атаки перебором, инициированной из корпоративной беспроводной сети.

А.3.2.6 SL 4: Защита от умышленного нарушения безопасности с использованием изощренных средств, при обширных ресурсах, наличии специальных познаний в IACS и высокой мотивации

SL 3 и SL 4 очень схожи в том, что оба предполагают использование изощренных средств для обхождения требований безопасности системы. Различие данных уровней происходит от степени мотивации злоумышленника и обширности доступных ему ресурсов. Они могут включать в себя высокоэффективные вычислительные ресурсы, большое количество компьютеров или значительные отрезки времени.

Примером изощренных средств при обширных ресурсах будет использование супер-ЭВМ или кластеров ЭВМ для осуществления взлома паролей методом перебора с использованием обширных хеш-таблиц. Другим примером будет ботнет, используемый для атаки на систему одновременно с помощью нескольких векторов атак. Третьим примером будет организованная преступная группировка, имеющая достаточную мотивацию и ресурсы, чтобы недели подряд пытаться анализировать систему и разрабатывать собственные эксплойты «нулевого дня».

А.3.3 Формат вектора SL

Для описания требований безопасности зоны, тракта, компонента или системы может использоваться вектор как лучшая альтернатива единичному номеру. Данный вектор может содержать либо требование конкретного SL, либо нулевое значение для каждого из фундаментальных требований (см. А.3.1).

ФОРМАТ → SL-? ([FR.] домен) = {IAC UC SI DC RDF TRE RA},

где SL-? = (Требуемый) Тип SL (см. А.2.2). Возможны следующие форматы:

- SL-T = Целевой SL;
- SL-A = Достигнутый SL;
- SL-C = Потенциальный SL.

[FR.] = (При необходимости) Поле, обозначающее FR, к которому относится значение SL. FR записываются в форме текстового сокращения, а не чисел для удобства чтения.

Домен = (Обязательно) Подходящий домен, на который распространяется SL. Домены могут относиться к зонам, системам управления, подсистемам или компонентам. Вот некоторые примеры различных доменов, которые представлены на рисунке А.1: зона SIS, зона BPCS, зона HMI BPCS, контроллер домена DMZ производственного объекта, тракт от DMZ производственного объекта к Центру управления и последовательный тракт от SIS к BPCS. В данном конкретном стандарте все требования относятся к системе управления, поэтому термин «домен» здесь не используется в противоположность другим документам серии МЭК 62443.

Примеры –

1 SL-T(Зона BPCS) = {2 2 0 1 3 1 3}

2 SL-C(АСБ Рабочая станция инженера) {3 3 2 3 0 0 1}

3 SL-C(RA, PLC-FS) = 4

Примечание — Последний пример раскрывает только компонент RA 7-значного SL-C.

Приложение В
(справочное)

Соотнесение SR и RE с уровнями SL 1 — 4 FR

В.1 Обзор

Задача данного приложения — предоставить пользователю общую методологическую основу по дифференциации уровней SL 0 — 4 на базе FR посредством обозначенных SR и соответствующих им RT.

В.2 Таблица соотнесения SL

Таблица В.1 иллюстрирует соответствие требований уровня системы требованиям FR для отдельно взятого потенциального SL системы — SL-C(xx, система управления). Для отдельно взятого FR соответствие необходимых требований уровня системы отдельно взятому SL-C показано галочкой. Так, например, характеристики безопасности системы SL = 1 для FR 5 (или SL-C(RDF, система управления) = 1) будут включать в себя базовые требования всех четырех обозначенных SR. Система, не способная удовлетворить всем четырем SR, будет иметь SL-C(RDF, система управления) = 0. Для соответствия SL-C(RDF, система управления) = 2 система должна поддерживать базовые требования этих четырех SR плюс RE(1) SR 5.1 и SR 5.2. В качестве другого примера: необходимо только базовое требование SR 6.1 для соответствия SL-C(TRE, система управления) = 1, но оба обозначенных SR необходимы для соответствия SL-C(TRE, система управления) = 2. А.3.3 раскрывает порядок обозначения общего вектора SL.

Таблица В.1 — Соотнесение SR и RE с уровнями SL 1— 4 FR (одним из четырех)

SR и RE		SL 1	SL 2	SL 3	SL 4
FR 1 — Управление идентификацией и аутентификацией (IAC)					
SR 1.1 — Идентификация и аутентификация пользователя — физического лица	5.3	√	√	√	√
SR 1.1 RE 1 — Уникальная идентификация и аутентификация	5.3.3.1		√	√	√
SR 1.1 RE 2 — Многофакторная аутентификация для недоверенных сетей	5.3.3.2			√	√
SR 1.1 RE 3 — Многофакторная аутентификация для всех сетей	5.3.3.3				√
SR 1.2 — Идентификация и аутентификация программных процессов и устройств	5.4		√	√	√
SR 1.2 RE 1 — Уникальная идентификация и аутентификация	5.4.3.1			√	√
SR 1.3 — Управление учетными записями	5.5	√	√	√	√
SR 1.3 RE 1 — Унифицированное управление учетными записями	5.5.3.1			√	√
SR 1.4 — Управление идентификаторами	5.6	√	√	√	√
SR 1.5 — Управление аутентификаторами	5.7	√	√	√	√
SR 1.5 RE 1 — Аппаратная безопасность для регистрационных данных идентичности программных процессов	5.7.3.1			√	√
SR 1.6 — Управление беспроводным доступом	5.8	√	√	√	√
SR 1.6 RE 1 — Уникальная идентификация и аутентификация	5.8.3.1		√	√	√
SR 1.7 — Надежность аутентификации по паролю	5.9	√	√	√	√
SR 1.7 RE 1 — Ограничения на генерацию паролей и сроки их действия для пользователей — физических лиц	5.9.3.1			√	√
SR 1.7 RE 2 — Ограничения сроков действия паролей для всех пользователей	5.9.3.2				√

Продолжение таблицы В.1

SR и RE		SL 1	SL 2	SL 3	SL 4
SR 1.8 — Сертификаты инфраструктуры открытых ключей (PKI)	5.10		√	√	√
SR 1.9 — Надежность аутентификации по открытому ключу	5.11		√	√	√
SR 1.9 RE 1 — Безопасность аппаратного обеспечения при аутентификации по открытому ключу	5.11.3.1			√	√
SR 1.10 — Обратная связь при аутентификации	5.12	√	√	√	√
SR 1.11 — Неудачные попытки входа в систему	5.13	√	√	√	√
SR 1.12 — Уведомление об использовании системы	5.14	√	√	√	√
SR 1.13 — Доступ через недоверенные сети	5.15	√	√	√	√
SR 1.13 RE 1 — Принятие явного запроса на доступ	5.15.3.1		√	√	√
FR 2 — Контроль использования (UC)					
SR 2.1 — Контроль выполнения авторизаций	6.3	√	√	√	√
SR 2.1 RE 1 — Контроль выполнения авторизаций для всех пользователей	6.3.3.1		√	√	√
SR 2.1 RE 2 — Соотнесение полномочий с ролями	6.3.3.2		√	√	√
SR 2.1 RE 3 — Приоритетность диспетчерского управления	6.3.3.3			√	√
SR 2.1 RE 4 — Двойное подтверждение	6.3.3.4				√
SR 2.2 — Контроль беспроводного использования	6.4	√	√	√	√
SR 2.2 RE 1 — Идентификация и сообщение о неавторизованных беспроводных устройствах	6.4.3.1			√	√
SR 2.3 — Контроль использования портативных и подвижных устройств	6.5	√	√	√	√
SR 2.3 RE 1 — Ужесточение статуса безопасности портативных и подвижных устройств	6.5.3.1			√	√
SR 2.4 — Мобильный код	6.6	√	√	√	√
SR 2.4 RE 1 — Проверка целостности мобильного кода	6.6.3.1			√	√
SR 2.5 — Блокировка сеанса	6.7	√	√	√	√
SR 2.6 — Прерывание удаленных сеансов	6.8		√	√	√
SR 2.7 — Контроль параллельных сеансов	6.9			√	√
SR 2.8 — События, подлежащие аудиту	6.10	√	√	√	√
SR 2.8 RE 1 — Централизованно управляемый системный журнал аудита	6.10.3.1			√	√
SR 2.9 — Емкость систем хранения данных аудита	6.11	√	√	√	√
SR 2.9 RE 1 — Предупреждение при достижении порога емкости носителя записей аудита	6.11.3.1			√	√
SR 2.10 — Реакция на технологические сбои аудита	6.12	√	√	√	√
SR 2.11 — Временные метки	6.13		√	√	√
SR 2.11 RE 1 — Внутрисистемная синхронизация времени	6.13.3.1			√	√
SR 2.11 RE 2 — Защита целостности источника синхроимпульсов	6.13.3.2				√

Продолжение таблицы В.1

SR и RE		SL 1	SL 2	SL 3	SL 4
SR 2.12 — Защита от непризнания участия	6.14			√	√
SR 2.12 RE 1 — Защита от непризнания участия для всех пользователей	6.14.3.1				√
FR 3 — Целостность системы (SI)					
SR 3.1 — Целостность коммуникации	7.3	√	√	√	√
SR 3.1 RE 1 — Защита целостности средствами криптографии	7.3.3.1			√	√
SR 3.2 — Защита от вредоносного кода	7.4	√	√	√	√
SR 3.2 RE 1 — Защита от вредоносного кода на входах и выходах	7.4.3.1		√	√	√
SR 3.2 RE 2 — Централизованное управление и отчетность для защиты от вредоносного кода	7.4.3.2				√
SR 3.3 — Верификация функциональности безопасности	7.5	√	√	√	√
SR 3.3 RE 1 — Автоматизированные механизмы верификации функциональности безопасности	7.5.3.1			√	√
SR 3.3 RE 2 — Верификация функциональности безопасности во время штатной работы	7.5.3.2				√
SR 3.4 — Целостность программного обеспечения и информации	7.6	√	√	√	√
SR 3.4 RE 1 — Автоматизированное уведомление о злоумышленных нарушениях целостности	7.6.3.1			√	√
SR 3.5 — Валидация входных данных	7.7	√	√	√	√
SR 3.6 — Детерминированный поток выходных сигналов	7.8	√	√	√	√
SR 3.7 — Обработка ошибок	7.9		√	√	√
SR 3.8 — Целостность сеанса	7.10		√	√	√
SR 3.8 RE 1 — Аннулирование идентификаторов ID сеанса после завершения сеанса	7.10.3.1			√	√
SR 3.8 RE 2 — Генерация уникального ID сеанса	7.10.3.2			√	√
SR 3.8 RE 3 — Случайный характер ID сеансов	7.10.3.3				√
SR 3.9 — Защита информации аудита	7.11		√	√	√
SR 3.9 RE 1 — Записи аудита на неперезаписываемых носителях	7.11.3.1				√
FR 4 — Конфиденциальность данных (DC)					
SR 4.1 — Конфиденциальность информации	8.3	√	√	√	√
SR 4.1 RE 1 — Защита конфиденциальности информации в ходе ее хранения или передачи через недоверенные сети	8.3.3.1		√	√	√
SR 4.1 RE 2 — Защита конфиденциальности при пересечении границ зон	8.3.3.2				√
SR 4.2 — Сохранность информации	8.4		√	√	√
SR 4.2 RE 1 — Удаление ресурсов на базе разделяемой памяти	8.4.3.1			√	√
SR 4.3 — Использование криптографии	8.5	√	√	√	√

Окончание таблицы В.1

SR и RE		SL 1	SL 2	SL 3	SL 4
FR 5 — Ограничение потока данных (RDF)					
SR 5.1 — Сегментация сети	9.3	√	√	√	√
SR 5.1 RE 1 — Физическая сегментация сети	9.3.3.1		√	√	√
SR 5.1 RE 2 — Независимость от сетей, не относящихся к системам управления	9.3.3.2			√	√
SR 5.1 RE 3 — Логическая и физическая изоляция критически важных сетей	9.3.3.3				√
SR 5.2 — Защита границ зоны	9.4	√	√	√	√
SR 5.2 RE 1 — Отказ по умолчанию, разрешение по исключению	9.4.3.1		√	√	√
SR 5.2 RE 2 — Островной режим	9.4.3.2			√	√
SR 5.2 RE 3 — Закрытие при отказе	9.4.3.3			√	√
SR 5.3 Ограничения на передачу общецелевой информации «абонент — абонент»	9.5	√	√	√	√
SR 5.3 RE 1 — Запрет на любую передачу общецелевой информации «абонент — абонент»	9.5.3.1			√	√
SR 5.4 — Разбиение приложений	9.6	√	√	√	√
FR 6 — Своевременный отклик на события (TRE)					
SR 6.1 — Доступность файлов регистрации аудита	10.3	√	√	√	√
SR 6.1 RE 1 — Программный доступ к файлам регистрации аудита	10.3.3.1			√	√
SR 6.2 — Непрерывный мониторинг	10.4		√	√	√
FR 7 — Работоспособность и доступность ресурсов (RA)					
SR 7.1 — Защита от отказа в обслуживании	11.3	√	√	√	√
SR 7.1 RE 1 — Регулировать загрузки линий связи	11.3.3.1		√	√	√
SR 7.1 RE 2 — Ограничить последствия DoS для других систем или сетей	11.3.3.2			√	√
SR 7.2 — Управление ресурсами	11.4	√	√	√	√
SR 7.3 — Резервирование в системе управления	11.5	√	√	√	√
SR 7.3 RE 1 — Верификация резервирования	11.5.3.1		√	√	√
SR 7.3 RE 2 — Автоматизация резервирования	11.5.3.2			√	√
SR 7.4 — Восстановление и воссоздание системы управления	11.6	√	√	√	√
SR 7.5 — Аварийное питание	11.7	√	√	√	√
SR 7.6 — Параметры конфигурации сети и безопасности	11.8	√	√	√	√
SR 7.6 RE 1 — Машиночитаемая отчетность о текущих параметрах безопасности	11.8.3.1			√	√
SR 7.7 — Минимальная функциональность	11.9	√	√	√	√
SR 7.8 — Инвентаризация компонентов системы управления	11.10		√	√	√

Приложение ДА
(справочное)

Сведения о соответствии ссылочных международных стандартов ссылочным национальным стандартам Российской Федерации

Таблица ДА.1

Обозначение ссылочного международного стандарта	Степень соответствия	Обозначение и наименование соответствующего национального стандарта
IEC 62443-1-1:2009	IDT	ГОСТ Р МЭК 62443-1-1 «Сети промышленной коммуникации. Безопасность сетей и систем. Часть 1-1. Терминология, концепции и модели»
IEC 62443-2-1	IDT	ГОСТ Р МЭК 62443-2-1 «Сети промышленной коммуникации. Безопасность сетей и систем. Часть 2-1. Учреждение программы безопасности систем промышленной автоматизации и контроля»
Примечание — В настоящей таблице использовано следующее условное обозначение степени соответствия стандартов: - IDT — идентичные стандарты.		

Библиография

Примечание 1 — Данная библиография включает в себя ссылки на источники, использованные в ходе создания настоящего стандарта, а также ссылки на источники, которые помогут читателю лучше понять, что такое кибербезопасность в целом и процесс разработки системы управления кибербезопасностью. Не все ссылки в данной библиографии приводятся в тексте настоящего стандарта. Ссылки сгруппированы в различные категории на основе их источника.

Ссылки на другие части — как существующие, так и на стадии производства — серии МЭК 62443:

Примечание 2 — Не все ссылки отражают опубликованные документы; некоторые документы все еще на стадии разработки. Они перечислены здесь для дополнения перечня имеющих на данный момент силу частей стандартов серии МЭК 62443.

[1] IEC/TR 62443-1-2, Industrial communication networks — Network and system security — Part 1-2: Master glossary of terms and abbreviations[1)]

[2] IEC/TS 62443-1-3, Industrial communication networks — Network and system security — Part 1-3: System security compliance metrics[2)]

[3] IEC/TR 62443-1-4, Industrial communication networks — Network and system security — Part 1-4: IACS security lifecycle and use-case[3)]

[4] IEC/TR 62443-2-2, Industrial communication networks — Network and system security — Part 2-2: Implementation guidance for an IACS security management system[4)]

[5] IEC/TR 62443-2-3, Industrial communication networks — Network and system security — Part 2-3: Patch management in the IACS environment[5)]

[6] IEC 62443-2-4, Industrial communication networks — Network and system security — Part 2-4: Installation and maintenance requirements for IACS suppliers[6)]

[7] IEC/TR 62443-3-1, Industrial communication networks — Network and system security — Part 3-1: Security technologies for industrial automation and control systems

[8] IEC 62443-3-2, Industrial communication networks — Network and system security — Part 3-2: Security levels for zones and conduits[7)]

[9] IEC 62443-4-1, Industrial communication networks — Network and system security — Part 4-1: Product development requirements[8)]

[10] IEC 62443-4-2, Industrial communication networks — Network and system security — Part 4-2: Technical security requirements for IACS components[9)]

Ссылки на другие стандарты:

[11] ISO/IEC Directives, Part 2:2011, Rules for the structure and drafting of International Standards

[12] ISO/IEC 19790, Information technology — Security techniques — Security requirements for cryptographic modules

[13] ISO/IEC 27002, Information technology — Security techniques — Code of practice for information security management

[1)] На рассмотрении.

[2)] Готовится к изданию.

[3)] На рассмотрении.

[4)] На рассмотрении.

[5)] На рассмотрении.

[6)] Готовится к изданию.

[7)] На рассмотрении.

[8)] На рассмотрении.

[9)] На рассмотрении.

[14] NERC CIP-002, Cyber Security — Critical Cyber Asset Identification

[15] NERC CIP-003, Cyber Security — Security Management Controls

[16] NERC CIP-004, Cyber Security — Personnel & Training

[17] NERC CIP-005, Cyber Security — Electronic Security Perimeter(s)

[18] NERC CIP-006, Cyber Security — Physical Security of Critical Cyber Assets

[19] NERC CIP-007, Cyber Security — Systems Security Management

[20] NERC CIP-008, Cyber Security — Incident Reporting and Response Planning

[21] NERC CIP-009, Cyber Security — Recovery Plans for Critical Cyber Assets

[22] NIST FIPS 199, Standards for Security Categorization of Federal Information and Information Systems

[23] NIST SP800-52, Guidelines for the Selection and Use of Transport Layer Security (TLS) Implementations

[24] NIST SP800-53 Rev. 3, Recommended Security Controls for Federal Information Systems and Organizations

[25] NIST SP800-57, Recommendation for Key Management

[26] NIST SP800-82, Guide to Industrial Control Systems (ICS) Security

[27] NIST SP800-92, Guide to Computer Security Log Management

Другие документы и опубликованные ресурсы:

[28] Gilsinn, J.D., Schierholz, R., Security Assurance Levels: A Vector Approach to Describing Security Requirements, NIST Publication 906330, October 20, 2010.

[29] IETF RFC 3647, Internet X.509 Public Key Infrastructure, Certificate Policy and Certification Practices Framework

[30] Digital Bond Bandolier project, available at gost.e-ecolog.ru

[31] Open Web Application Security Project (OWASP), available at gost.e-ecolog.ru

УДК 004.056.5:006.354 ОКС 25.040.40; 35.110 IDT

Ключевые слова: безопасность, сети и системы, уровни безопасности, сети промышленной коммуникации, система промышленной автоматики и контроля

Редактор *Л.А. Кудрявцева*
Технический редактор *В.Н. Прусакова*
Корректор *Л.С. Лысенко*
Компьютерная верстка *Е.А. Кондрашовой*

Сдано в набор 06.06.2016. Подписано в печать 28.06.2016. Формат 60×84¼. Гарнитура Ариал.
Усл. печ. л. 7,91. Уч.-изд. л. 6,33 Тираж 29 экз Зак. 1568.

Подготовлено на основе электронной версии, предоставленной разработчиком стандарта

Издано и отпечатано во ФГУП «СТАНДАРТИНФОРМ», 123995 Москва. Гранатный пер., 4.
gost.e-ecolog.ru gost.e-ecolog.ru

gost.e-ecolog.ru