МЕЖГОСУДАРСТВЕННЫЙ СОВЕТ ПО СТАНДАРТИЗАЦИИ, МЕТРОЛОГИИ И СЕРТИФИКАЦИИ
(МГС)
INTERSTATE COUNCIL FOR STANDARDIZATION, METROLOGY AND CERTIFICATION
(ISC)

МЕЖГОСУДАРСТВЕННЫЙ СТАНДАРТ

ГОСТ 35090— 2024

АППАРАТУРА РАСПРЕДЕЛЕНИЯ И УПРАВЛЕНИЯ НИЗКОВОЛЬТНАЯ

Аспекты безопасности

(IEC TS 63208:2020, NEQ)

Издание официальное

Москва
Российский институт стандартизации
2024

gost.e-ecolog.ru

Предисловие

Цели, основные принципы и общие правила проведения работ по межгосударственной стандартизации установлены ГОСТ 1.0 «Межгосударственная система стандартизации. Основные положения» и ГОСТ 1.2 «Межгосударственная система стандартизации. Стандарты межгосударственные, правила и рекомендации по межгосударственной стандартизации. Правила разработки, принятия, обновления и отмены»

Сведения о стандарте

1 РАЗРАБОТАН Акционерным обществом «Диэлектрические кабельные системы» (АО «ДКС»)

2 ВНЕСЕН Федеральным агентством по техническому регулированию и метрологии

3 ПРИНЯТ Межгосударственным советом по стандартизации, метрологии и сертификации (протокол от 31 июля 2024 г. № 175-П)

За принятие проголосовали:

Краткое наименование страны по МК (ИСО 3166) 004—97	Код страны по МК (ИСО 3166) 004—97	Сокращенное наименование национального органа по стандартизации
Армения	AM	ЗАО «Национальный орган по стандартизации и метрологии» Республики Армения
Беларусь	BY	Госстандарт Республики Беларусь
Киргизия	KG	Кыргызстандарт
Россия	RU	Росстандарт
Узбекистан	UZ	Узбекское агентство по техническому регулированию

4 Приказом Федерального агентства по техническому регулированию и метрологии от 12 декабря 2024 г. № 1879-ст межгосударственный стандарт ГОСТ 35090—2024 введен в действие в качестве национального стандарта Российской Федерации с 1 марта 2025 г.

5 Настоящий стандарт разработан с учетом основных нормативных положений международного стандарта IEC TS 63208:2020 «Аппаратура распределения и управления низковольтная. Аспекты безопасности» («Low-voltage switchgear and controlgear — Security aspects», NEQ)

6 ВВЕДЕН ВПЕРВЫЕ

Информация о введении в действие (прекращении действия) настоящего стандарта и изменений к нему на территории указанных выше государств публикуется в указателях национальных стандартов, издаваемых в этих государствах, а также в сети Интернет на сайтах соответствующих национальных органов по стандартизации.

В случае пересмотра, изменения или отмены настоящего стандарта соответствующая информация будет опубликована на официальном интернет-сайте Межгосударственного совета по стандартизации, метрологии и сертификации в каталоге «Межгосударственные стандарты»

© Оформление. ФГБУ «Институт стандартизации», 2024

В Российской Федерации 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 и сокращения 2
4 Общие положения 6
5 Задачи информационной безопасности 6
6 Управление жизненным циклом информационной безопасности 7
7 Требования к информационной безопасности 14
8 Инструкции по установке, эксплуатации и техническому обслуживанию 18
9 Разработка и испытания 19
Приложение А (справочное) Примеры эксплуатации 20
Приложение Б (справочное) Информационная безопасность и архитектура электрических систем 30
Приложение В (справочное) Базовые аспекты информационной безопасности 33
Приложение Г (справочное) Рекомендации для потребителей (пользователей) 35
Библиография 37

Введение

Применение передачи данных в цифровом формате, в низковольтной аппаратуре, смонтированной в низковольтных комплектных устройствах, предназначенных для защиты, управления и распределения, влечет за собой увеличение рисков возникновения угроз в области информационной безопасности. Информационные технологии, связанные или интегрированные с промышленными системами, увеличивают риски угроз информационной безопасности.

Настоящий стандарт содержит общие принципы по организации мер обеспечения информационной безопасности при проектировании и обслуживании коммутационных аппаратов, таких как автоматические выключатели или другие низковольтные аппараты, в том числе реле перегрузки и бесконтактные реле, оснащенные интерфейсом передачи данных для локального или удаленного подключения к логическому контроллеру или дисплею, для предоставления доступа к таким данным, как фактические параметры электропитания, данные мониторинга, регистрация данных и удаленное обновление.

Для применения в системах распределения электроэнергии необходимо применять базовые меры обеспечения информационной безопасности для поддержания функций защитного отключения/переключения (в результате перегрузки, короткого замыкания, протекания тока утечки на землю, изменения уровня напряжения ниже/выше допустимого или его пропадания) на необходимом уровне, с целью обеспечения безопасности. Такие требования должны ограничить уязвимость интерфейсов обмена данными. Чтобы сохранить максимальную свободу для обновлений, соответствующие требования для определенного применения желательно определять с помощью систематического подхода к оценке рисков.

В настоящем стандарте рассматриваются следующие аспекты информационной безопасности:

а) повышение осведомленности о рисках угроз информационной безопасности, связанных с непреднамеренным срабатыванием и потерей защитных функций;

б) определение базовых мер обеспечения информационной безопасности низковольтной аппаратуры и низковольтных комплектных устройств, снижения вероятности непреднамеренного срабатывания/несрабатывания и потери защитных функций в низковольтных комплектных устройствах и системах управления технологическими процессами;

в) предоставление рекомендаций, позволяющих избежать ухудшения функциональности низковольтной аппаратуры во всех режимах работы в результате реализации мер обеспечения информационной безопасности.

В настоящем стандарте приведено руководство по применению мер обеспечения информационной безопасности низковольтной аппаратуры и низковольтных комплектных устройств (аппаратные средства, прошивки, сетевой интерфейс, контроль доступа, система), а также по дополнительным мерам, которые необходимо учитывать при внедрении низковольтной аппаратуры и использовать в инструкциях по ее эксплуатации.

М Е Ж Г О С У Д А Р С Т В Е Н Н Ы Й С Т А Н Д А Р Т

АППАРАТУРА РАСПРЕДЕЛЕНИЯ И УПРАВЛЕНИЯ НИЗКОВОЛЬТНАЯ

Аспекты безопасности

Low-voltage switchgear and controlgear.
Security aspects

Дата введения — 2025—03—01

1 Область применения

Настоящий стандарт применим к основным функциям низковольтной аппаратуры и низковольтных комплектных устройств (НКУ), связанным с информационной безопасностью (ИБ), в течение всего жизненного цикла низковольтной аппаратуры и НКУ. Это применимо к проводным и беспроводным средствам передачи данных, физической доступности низковольтной аппаратуры и НКУ в зависимости от условий их размещения.

Настоящий стандарт предназначен для повышения осведомленности об аспектах безопасности и содержит рекомендации и требования по соответствующим мерам защиты от угроз, связанных с уязвимостями.

В частности, он концентрирует внимание на возможных угрозах, связанных с уязвимостями в результате:

- случайного срабатывания низковольтной аппаратуры, которое может привести к опасным ситуациям;
- недоступности защитных функций (сверхток, ток утечки на землю и т. д.).

Настоящий стандарт охватывает соответствующие меры обеспечения информационной безопасности с учетом [1][1)] для применения низковольтной аппаратуры и НКУ.

Настоящий стандарт включает в себя распространенные примеры из эксплуатации, приведенные в приложении А.

Настоящий стандарт не охватывает в полном объеме требования безопасности для следующих информационных систем:

- системы промышленной автоматизации и управления (IACS);
- географическая информационная система (ГИС);
- информационная система персональных данных (ИСПД);
- системы объектов критической информационной инфраструктуры (КИИ);
- системы автоматического контроля и учета электрической энергии (АСКУЭ).

2 Нормативные ссылки

В настоящем стандарте использованы нормативные ссылки на следующие межгосударственные стандарты:

ГОСТ 2.701 Единая система конструкторской документации. Схемы. Виды и типы. Общие требования к выполнению

[1)] В Российской Федерации действует ГОСТ Р ИСО/МЭК 27001—2021 «Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования».

Издание официальное

ГОСТ 2.702 Единая система конструкторской документации. Правила выполнения электрических схем

ГОСТ 34.10[1)] Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи

ГОСТ 31282 Устройства пломбировочные. Классификация

ГОСТ IEC 60947-1 Аппаратура распределения и управления низковольтная. Часть 1. Общие правила

Примечание — При пользовании настоящим стандартом целесообразно проверить действие ссылочных стандартов и классификаторов на официальном интернет-сайте Межгосударственного совета по стандартизации, метрологии и сертификации (gost.e-ecolog.ru по указателям национальных стандартов, издаваемым в государствах, указанных в предисловии, или на официальных сайтах соответствующих национальных органов по стандартизации. Если на документ дана недатированная ссылка, то следует использовать документ, действующий на текущий момент, с учетом всех внесенных в него изменений. Если заменен ссылочный документ, на который дана датированная ссылка, то следует использовать указанную версию этого документа. Если после принятия настоящего стандарта в ссылочный документ, на который дана датированная ссылка, внесено изменение, затрагивающее положение, на которое дана ссылка, то это положение применяется без учета данного изменения. Если ссылочный документ отменен без замены, то положение, в котором дана ссылка на него, рекомендуется применять в части, не затрагивающей эту ссылку.

3 Термины, определения и сокращения

3.1 Термины и определения

В настоящем стандарте применены следующие термины с соответствующими определениями:

3.1.1 **журнал аудита** (audit log): Хронологическая фиксация записей произошедших событий и их хранение определенный период времени с целью последующего использования.

Примечания

1 Журналы аудита хранятся в течение согласованного периода времени для помощи в проведении последующих расследований.

2 Журналы аудита допускается использовать для анализа риска и выявления инцидентов угроз информационной безопасности или контроля функционирования объекта.

3.1.2 **атака** (attack): Попытка уничтожения, раскрытия, изменения, блокирования, кражи, получения несанкционированного доступа к активу или его несанкционированного использования.

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

3.1.4 **вектор атаки** (attack vector): Путь или средство, при помощи которого инициирующее атаку лицо может получить доступ к устройству, чтобы инициировать атаку.

3.1.5 **аутентификация** (authentication): Действия по проверке подлинности субъекта доступа и/или объекта доступа, а также по проверке принадлежности субъекту доступа и/или объекту доступа предъявленного идентификатора доступа и аутентификационной информации.

3.1.6 **подлинность** (authenticity): Свойство, гарантирующее, что субъект или ресурс идентичен заявленному.

3.1.7 **авторизация** (authorization): Предоставление субъекту доступа прав доступа, а также предоставление доступа в соответствии с установленными правилами управления доступом.

Примечание — Положительный результат идентификации и аутентификации является одним из оснований для авторизации субъекта доступа.

3.1.8 **доступность** (availability): Свойство, определяющее возможность использования объекта авторизованным субъектом по запросу.

3.1.9 **конфиденциальность** (confidentiality): Свойство, определяющее, что информация не предоставляется или не раскрывается неавторизованным лицам, организациям или процессам.

3.1.10 **контрмера** (countermeasure): Действие, устройство или метод, которые снижают уровень угрозы, уязвимости или противодействуют атаке путем ее отражения или нейтрализации, или миними-

[1)] В Российской Федерации действует также ГОСТ Р 34.10—2012.

зации ущерба, который она способна нанести, или путем ее обнаружения и сообщения о ней, для принятия корректирующего действия.

3.1.11 **информационная безопасность** (information security): Все аспекты, связанные с определением, достижением и поддержанием конфиденциальности, целостности, доступности, недоказуемости, подотчетности, аутентичности и достоверности информации или средств ее обработки.

Примечание — Цель состоит в снижении уровня риска персональной или общественной угрозы, потери доверия общества или потребителей, раскрытия конфиденциальных активов, незащищенности бизнес-активов или несоблюдения нормативных требований. Эти понятия применяются к любой системе в производственном процессе, и они включают как автономные, так и сетевые компоненты. Связь между системами может осуществляться либо посредством внутреннего обмена сообщениями, либо посредством любых человеческих или машинных интерфейсов, которые проводят аутентификацию, работу, контроль или обмен данными с любой из этих систем управления. Информационная безопасность включает в себя понятия идентификации, аутентификации, авторизации, обслуживаемости и конфиденциальности.

3.1.12 **целостность данных** (data integrity): Свойство, гарантирующее, что данные не были изменены, уничтожены или потеряны из-за несанкционированных действий или случайно.

Примечание — Термин затрагивает неизменность значений данных, но не информацию, которую отражают эти значения, и ненадежность источника значений.

3.1.13 **эшелонированная [многоуровневая] защита** (defence in depth): Наличие нескольких уровней защиты с целью предотвращения или хотя бы сдерживания атаки.

Примечание — Эшелонированная (многоуровневая) защита предполагает наличие уровней безопасности и защиты, в том числе в отдельных системах, и обладает следующими признаками:

- создание преград для злоумышленников (инициаторы атак) по незаметному прохождению или обхождению каждого уровня;
- наличие бреши на одном из уровней можно компенсировать возможностями других уровней;
- общая безопасность системы обеспечивается уровнями защиты каждой отдельной системы.

3.1.14 **целостность системы** (system integrity): Свойство системы выполнять предусмотренную для нее функцию в нормальном режиме, защищенном от преднамеренного или случайного несанкционированного воздействия.

3.1.15 **отказ в обслуживании** (denial of service): Предотвращение авторизованного доступа к ресурсам или задержка операций, критичных по времени.

3.1.16 **опасная ситуация** (hazardous situation): Обстоятельства, в которых люди, имущество или окружающая среда подвергаются одной или нескольким опасностям.

3.1.17 **аудиторская проверка информационной безопасности** (security audit): Независимое исследование и проверка записей и действий системы для определения адекватности мер обеспечения защиты системы, обеспечения их соответствия заданной политике безопасности и заданному перечню методов, выявления уязвимых мест в сервисах безопасности и подготовки рекомендаций по любым необходимым изменениям мер обеспечения информационной безопасности.

3.1.18 **основная функция, связанная с информационной безопасностью** (security related main function): Функция низковольтной аппаратуры и низковольтных комплектных устройств, неисправность которой может привести к ложному срабатыванию, которое приводит к возникновению опасных ситуаций, утрате или нарушению защитной функции, утрате или нарушению функциональных возможностей, определенных изготовителем.

Примечание — Когда дополнительная функция, такая как контроль электрической цепи низковольтной аппаратуры, может быть подвергнута атаке, ведущей к нарушению основной функции, связанной с безопасностью, такой как защита от короткого замыкания, эта дополнительная функция считается основной функцией, связанной с безопасностью.

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

3.1.20 **политика информационной безопасности** (security policy): Перечень правил и методик, которые регламентируют или регулируют способ предоставления сервисов безопасности системой или организацией для защиты ее объектов.

3.1.21 **уязвимость информационной системы** (security vulnerability): Слабое место в информационной системе системных мер обеспечения информационной безопасности, внутреннего контроля при его реализации, которое может быть использовано или спровоцировано угрозой.

3.1.22 **оценка риска угроз информационной безопасности** (security risk assessment): Процесс систематического выявления потенциальных уязвимостей значимых ресурсов системы и угроз для этих ресурсов, количественной оценки потенциального ущерба и последствий на основе вероятностей их возникновения и (в случае необходимости) разработки рекомендаций по выделению ресурсов для организации обеспечения информационной безопасности с целью минимизации общей уязвимости.

3.1.23 **умное производство** (smart manufacturing): Электронная коммуникационная среда интегрированных продуктов, процессов и ресурсов (информационных, физических, человеческих) для создания и предоставления продуктов и услуг, которая также взаимодействует с другими информационными средами (цифровыми и электронными) во внутренних и внешних цепочках коммуникации предприятия с постоянным улучшением производительности.

Примечания

1 Аспекты производительности включают гибкость, эффективность, безопасность, защищенность, устойчивость или любые другие показатели производительности, определенные предприятием.

2 Помимо производства, другие области деятельности предприятия могут включать в себя проектирование, логистику, маркетинг, закупки, продажи или любые другие области, указанные предприятием.

3.1.24 **базовые защитные меры** (baseline controls): Минимальный набор защитных мер, установленный для системы или организации.

3.1.25 **мера обеспечения информационной безопасности** (control): Мера, направленная на изменение риска.

Примечания

1 К мерам обеспечения информационной безопасности относятся процессы, политика, устройства, практические приемы или другие действия, используемые для изменения риска.

2 Меры обеспечения информационной безопасности не всегда могут приводить к запланированным или предполагаемым изменениям риска.

3.1.26 **воздействие** (impact): Результат нежелательного инцидента информационной безопасности.

3.1.27 **рекомендации** (guidelines): Описание, поясняющее действия и способы их выполнения, необходимые для достижения установленных целей.

3.1.28 **активы** (asset): Все, что имеет ценность для организации.

3.1.29 **инцидент информационной безопасности** (information security incident): Любое непредвиденное или нежелательное событие, которое может нарушить деятельность или информационную безопасность.

Примечание — Инцидентами информационной безопасности являются:

- утрата функций низковольтной аппаратуры;
- системные сбои или перегрузки;
- ошибки пользователей;
- несоблюдение политик или рекомендаций;
- нарушение физических мер защиты;
- неконтролируемые изменения систем;
- сбои программного обеспечения и отказы технических средств;
- нарушение правил доступа;
- утрата активов;
- несанкционированный доступ к информации.

3.1.30 **центровик (локальной вычислительной сети)** (hub): Устройство, используемое для взаимосвязи нескольких устройств оконечного оборудования данных и выполняющее функции восстановления амплитуды сигналов, синхронизации сигналов, обнаружения конфликтов в локальной вычислительной сети и оповещения о них, а также распространения сигналов по центровикам нижних уровней и оконечному оборудованию данных.

3.1.31 **системы промышленной автоматики и контроля** (industrial automation and control systems): Группа персонала, а также совокупность аппаратного и программного обеспечений, которые могут регулировать или воздействовать иным образом на безопасное, защищенное и надежное функционирование производственного процесса.

Примечание — Такие системы могут включать в себя, но не ограничиваются этим:

- промышленные системы управления, включающие в себя распределенные системы управления, ПЛК, пульты дистанционного управления, интеллектуальные электронные устройства, системы диспетчерского контро-

ля и сбора данных (SCADA), а также системы мониторинга и диагностики (в данном контексте системы управления процессами наделены базовыми функциями системы управления процессами и автоматизированной системы безопасности SIS, которые могут быть или физически разделены друг от друга, или объединены друг с другом);

- ассоциированные информационные системы, например системы упреждающего или многосвязного регулирования, а также сетевые оптимизаторы, специальные мониторы к оборудованию, графические интерфейсы, архиваторы, автоматизированные системы управления производственными процессами и информационно-управляющие системы предприятия;

- ассоциированные внутренние, пользовательские сетевые или машинные интерфейсы, используемые для обеспечения управления, защиты и функциональности производственных операций в ходе непрерывных, периодических, дискретных и прочих процессов.

3.1.32 **коммутационный аппарат** (switching device): Аппарат, предназначенный для включения или отключения тока в одной или нескольких электрических цепях.

3.1.33 **низковольтное устройство распределения и управления** (low-voltage switchgear and controlgear assembly): Низковольтные коммутационные аппараты и устройства управления, измерения, сигнализации, защиты, регулирования, собранные совместно, со всеми внутренними электрическими и механическими соединениями и конструктивными элементами.

3.1.34 **идентификация** (identification): Действия по присвоению субъектам и объектам доступа идентификаторов и/или сравнению предъявляемого идентификатора с перечнем присвоенных идентификаторов.

3.1.35 **процесс** (process): Перечень взаимосвязанных или взаимодействующих мероприятий, в результате которых исходные ресурсы преобразуются в конечный продукт.

3.1.36 **оценочный уровень доверия** (evaluation assurance level): Перечень требований доверия, представляющий некоторое положение на предопределенной шкале доверия и составляющий пакет доверия.

3.1.37 **система защиты информации от несанкционированного доступа** (system of protection from unauthorized access to information): Комплекс организационных мер и программно-технических (в том числе криптографических) средств защиты от несанкционированного доступа к информации в автоматизированных системах.

3.1.38 **строгая аутентификация** (strong authentication): Аутентификация с применением только метода многофакторной взаимной аутентификации и использованием криптографических протоколов аутентификации.

3.1.39 **идентификация пломбировочного устройства** (sealing device identification): Определение подлинности и целостности пломбировочного устройства по его характерным индивидуальным признакам, а также по отсутствию изменений в расположении пломбировочного устройства на объекте пломбирования путем визуального осмотра или с помощью технических средств общего применения, специализированных технических средств с использованием или без использования специальных методик.

3.1.40 **индикаторное пломбировочное устройство** (indicator sealing device): Устройство, обеспечивающее индикацию фактов несанкционированного доступа к объекту защиты путем идентификации его целостности, обеспечивающее механическую защиту с усилием растяжения в диапазоне от 0,05 до 1,0 кН.

3.2 Сокращения

В настоящем стандарте применены следующие сокращения:

ИТ — информационные технологии;
ЛВС — локальная вычислительная сеть;
ОВиК — отопление, вентиляция и кондиционирование воздуха;
ОТ — операционная технология;
ПК — персональный компьютер;
ПЛК — программируемый логический контроллер;
ПО — программное обеспечение;
ПЭ — пример эксплуатации;
СОТ — система охранная телевизионная;
ЧМИ — человеко-машинный интерфейс;
ЭМС — электромагнитная совместимость;

APN — имя точки доступа (Access Point Name);
BMS — система управления зданием (Building Management Systems);
BT — Bluetooth®[1];
DDoS — распределенная атака типа «отказ в обслуживании» (Distributed Denial of Service);
DMZ — демилитаризованная зона (Demilitarized Zone);
DNP — распределенный сетевой протокол (Distributed Network Protocol);
DoS — отказ в обслуживании (Denial of Service);
CRL — список аннулированных сертификатов (Certificate Revocation List);
CVSS — общая система оценки уязвимости (Common Vulnerability Scoring System);
ERP — планирование ресурсов предприятия (Enterprise Resource Planning);
IACS — система промышленной автоматизации и контроля (Industrial Automation and Control Systems);
ICS — промышленная система управления (Industrial Control System);
IDS — система обнаружения вторжений (Intrusion Detection System);
IoT — технология «Интернет вещей» (Internet of Things);
IPS — система предупреждения вторжений (Intrusion Prevention System);
IPsec — протокол по защите информации в сети;
JTAG — интерфейс отладки «Joint Test Action Group» [IEEE 1149];
MAC — уникальный идентификатор управления доступом к устройству (Media Access Control);
MLP — многопротокольная коммутация по меткам (Multiprotocol Label Switching);
NFC — связь малого радиуса действия (Near Field Communication);
P2P — пиринговое соединение (Peer to Peer Connection);
RBAC — управление доступом на основе ролей (Role Based Access Control);
RS485 — рекомендованный стандарт 485 (согласно TIA 485-A);
SCADA — диспетчерский контроль и сбор данных (Supervisory Control and Data Acquisition);
SD-карта — карта памяти типа «secure digital»;
SL — уровень безопасности (Safety Level);
SSL — протокол защиты информации уровень защищенных сокетов (Secure Socket Layer);
ULP — универсальный логический разъем (Universal Logic Plug);
USB — универсальная последовательная шина (Universal Serial Bus);
VPN — виртуальная частная сеть (Virtual Private Network);
WCI — беспроводной интерфейс связи (Wireless Communication Interface);
WLAN — беспроводная локальная вычислительная сеть (Wide Local Area Network).

4 Общие положения

Целостность или наличие основных функций низковольтной аппаратуры может зависеть от аспектов физической безопасности и ИБ. Существующие методы обеспечения ИБ в отношении физического доступа к низковольтной аппаратуре и НКУ должны рассматриваться как часть мер физической безопасности совместно с мерами обеспечения ИБ.

5 Задачи информационной безопасности

В части распределения электроэнергии с помощью низковольтной аппаратуры и НКУ (см. приложение Б) общие цели ИБ заключаются в обеспечении гарантии их работы в соответствии с проектом и конфигурацией, а также целенаправленном предотвращении непреднамеренного срабатывания и защиты их основных функций, связанных с ИБ.

Необходимо учитывать следующие основные аспекты ИБ: целостность, подлинность и доступность данных. В политике информационной безопасности следует подробно описать, что необходимо

[1] Товарный знак Bluetooth® является примером подходящего протокола связи, реализуемого платно. Данная информация дается для удобства пользования настоящим документом и не представляет собой рекомендацию к применению этого протокола связи.

защищать и каким образом этого можно достичь. Обзор соответствующих аспектов ИБ, которые необходимо учитывать, приведен в приложении В, а уровни ИБ определены в Б.3 приложения Б.

6 Управление жизненным циклом информационной безопасности

6.1 Общие положения

Защита от атак на ИБ должна быть определена на основе результатов оценки рисков угроз ИБ, чтобы идентифицировать потенциальные угрозы и уязвимости, а также определить перечень мер обеспечения ИБ. Перечень должен охватывать каждую стадию жизненного цикла низковольтной аппаратуры и НКУ, а также учитывать физический доступ к ним с учетом места установки (см. рисунок 1 в качестве примера).

Угрозы ИБ и связанные с ними меры обеспечения ИБ приведены в примерах эксплуатации (ПЭ), описанных в приложении А, которые перечислены ниже в таблице 1.

Таблица 1 — Примеры угроз ИБ при эксплуатации низковольтной аппаратуры и НКУ

Угроза	Номер ПЭ
Обновление вредоносной прошивкой	ПЭ 1, см. пункт А.2 ПЭ 5, см. пункт А.6
Атака типа распределенного отказа в обслуживании	ПЭ 3, см. пункт А.4
Несанкционированный доступ к производственной сети (ОТ)	ПЭ 2, см. пункт А.3
Несанкционированный доступ к НКУ	ПЭ 4, см. пункт А.5
Несанкционированный доступ к низковольтной аппаратуре	ПЭ 6, см. пункт А.7 ПЭ 7, см. пункт А.8 ПЭ 8, см. пункт А.9

Для некоторых отраслей усилия, направленные на снижение рисков угроз ИБ, могут значительно перевесить выгоду от использования программируемых цифровых продуктов и высокоинтегрированных систем. В таких случаях рекомендуется проводить анализ рисков угроз ИБ, подробно определяющий преимущества и недостатки использования низковольтной аппаратуры и НКУ.

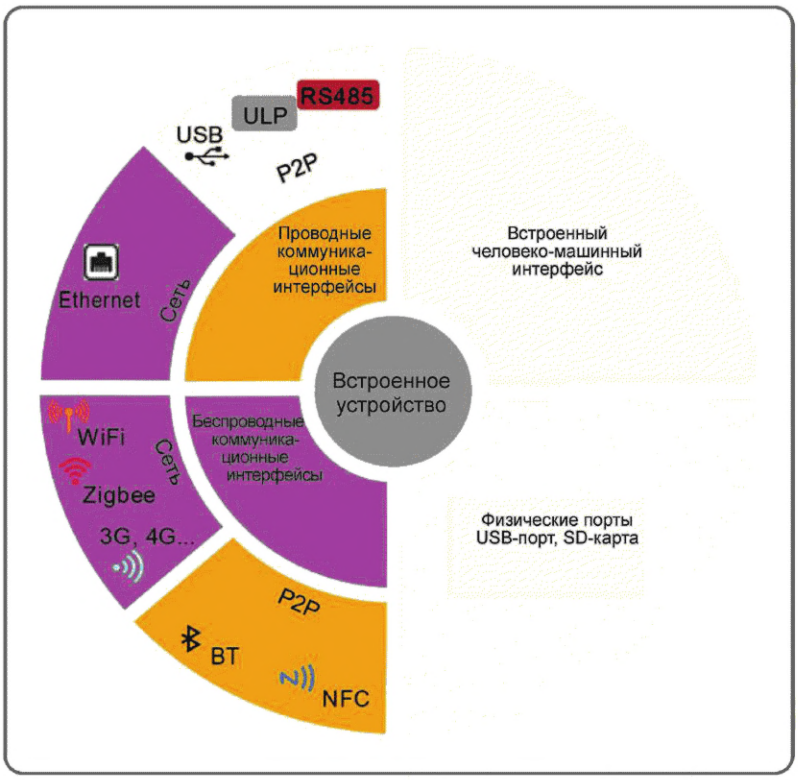


Рисунок 1 — Пример интерфейсов встроенного цифрового передающего устройства в низковольтную аппаратуру и НКУ, которые могут подвергаться атаке

6.2 Управление рисками угроз ИБ

Как правило, оценка рисков угроз ИБ основана на известных, выявленных уязвимостях и угрозах с учетом места установки. После проведения оценки определяют соответствующие меры обеспечения ИБ, необходимые для выполнения общих задач ИБ.

Все соответствующие угрозы и известные уязвимости низковольтной аппаратуры и НКУ, которые могут повлиять на основные функции низковольтной аппаратуры, должны быть рассмотрены и задокументированы в рамках оценки рисков угроз ИБ.

Следующие аспекты должны быть учтены в оценке рисков совместно с целевым уровнем ИБ:

- система защиты информации от несанкционированного доступа;
- оценочный уровень доверия;
- процессы;
- хранилища данных;
- внешние объекты взаимодействия;
- внутренние и внешние протоколы связи, реализованные в низковольтной аппаратуре и НКУ;
- внутренние физические порты доступа, включая порты отладки;
- соединения на печатной плате, такие как соединения JTAG или отладочные заголовки, которые могут использоваться для атаки на низковольтную аппаратуру;
- потенциальные векторы атак, в том числе атак на аппаратные средства, если применимо;
- потенциальные угрозы, их вероятность, степень тяжести и последствия согласно системе оценки уязвимостей (например, CVSS);
- снижение и/или нейтрализация каждой угрозы;
- выявленные проблемы, связанные с безопасностью;
- внешние зависимости в виде драйверов или сторонних приложений (код, не разработанный поставщиком), которые связаны с приложением.

В ходе оценки уязвимости низковольтной аппаратуры при ее целевом применении определяют уязвимости, которые представляют определенные угрозы, а также их потенциальное влияние на основные функции, связанные с безопасностью.

В результате оценки рисков угроз ИБ составляют описание:

- аппаратуры/системы, в отношении которых проводилась оценка рисков угроз ИБ (например, мобильная панель управления);
- каждой стадии, таких как проектирование, внедрение, ввод в эксплуатацию, эксплуатация и техническое обслуживание;
- выявленные уязвимости, которые могут быть использованы угрозами и привести к рискам угроз ИБ (включая преднамеренные атаки на низковольтную аппаратуру и НКУ, прикладные программы и соответствующее ПО, а также непредвиденные события в результате человеческой ошибки);
- потенциальные последствия рисков угроз ИБ посредством анализа условий, в которых они могут возникать;
- для каждой из стадий требования к дополнительным мерам обеспечения ИБ;
- информация о мерах обеспечения ИБ, принятых для снижения или нейтрализации угроз.

6.3 Реагирование на риски угроз ИБ

Меры обеспечения ИБ с учетом рисков угроз:

а) снижение рисков угроз ИБ до приемлемого уровня посредством:

1) исключения рисков угроз ИБ на стадии проектирования;
2) ограничения рисков угроз ИБ;
3) переноса или разделения рисков угроз ИБ (на другой объект или с ним);

б) принятие рисков угроз ИБ, если они допустимы.

6.4 Перечень требований к ИБ

На основе результатов оценки рисков угроз ИБ, в том числе уязвимостей низковольтной аппаратуры, составляют перечень требований к безопасности, содержащий следующее:

- описание основной функции низковольтной аппаратуры, связанной с ИБ;
- уязвимости, которые могут повлиять на эту функцию, и предполагаемые угрозы, если применимо;
- последствия потери основной функции, связанной с ИБ;
- описание предложенных мер обеспечения ИБ.

6.5 Критические данные

Особое внимание следует уделить защите критических данных. Критические данные для целостности и доступности основных функций низковольтной аппаратуры включают следующее:

а) данные о состоянии или срабатывании низковольтной аппаратуры, связанные с безопасностью эксплуатации (электрическая блокировка, пуск двигателя, повторное включение и т. д.);

б) данные о конфигурации низковольтной аппаратуры, в том числе:

1) параметры автоматических выключателей, расцепителей защиты от перегрузки и сверхтока (номинальные характеристики низковольтной аппаратуры, число полюсов и т. д.);

2) параметры бесконтактных реле (диапазон измерений, нормально разомкнутое или нормально замкнутое выходное положение и т. д.).

Также могут быть определены другие данные, относящиеся к основным функциям низковольтной аппаратуры, связанным с безопасностью.

Функция измерения параметров электроэнергии на некоторых предприятиях может требовать защиты. В таком случае следует принимать дополнительные меры по обеспечению конфиденциальности.

6.6 Системная архитектура

6.6.1 Система управления

Как правило, низковольтную аппаратуру, предназначенную для коммутации и управления, устанавливают в виде узлов. При необходимости внедряют интерфейсы связи (например, шлюз) для предоставления удаленного доступа с целью наблюдения и управления. Такие системы рассматривают как системы управления.

Поверхность атаки на систему управления во многом зависит от ее архитектуры. Для оценки рисков, связанных с архитектурой, следует оценить уровень ее функциональных возможностей и связь с внешней средой.

6.6.2 Уровни коммуникационной системы

Ниже рассмотрен пример классификации уровней безопасности коммуникационной системы низковольтной аппаратуры для технологической или производственной системы.

6.6.2.1 Уровень 0. Процесс

Уровень 0 соответствует фактическому физическому процессу. Такие процессы относятся к разного рода производственному оборудованию во всех секторах, которые включают в себя, но не ограничиваются этим, производство, нефтехимическую промышленность, фармацевтику, целлюлозно-бумажную промышленность и электроэнергетику.

Уровень 0 распространяется на системы низшего уровня без возможностей цифровой связи:

- защитно-коммутационную аппаратуру без цифровых модулей связи (автоматические выключатели, электромеханические реле, контакторы);
- датчики на основе коммутационных элементов (концевые выключатели).

6.6.2.2 Уровень 1. Локальное управление и контроль

Уровень 1 включает в себя функции, задействованные в контроле и управлении физическими процессами.

Низковольтная аппаратура локального управления и контроля:

- защитно-коммутационные аппараты с передачей данных о своем состоянии, контроле качества электроэнергии, протекающей через низковольтную аппаратуру;
- ПЛК;
- панели ЧМИ, установленные непосредственно на НКУ.

Каналы связи между низковольтной аппаратурой на 1-м уровне могут рассматриваться как каналы с ограниченной функциональностью и ограниченной зоной.

Уровень 1 распространяется также на системы безопасности и защиты, которые отслеживают процесс и автоматически возвращают его в безопасное состояние, если он вышел за рамки безопасности. Такой уровень включает в себя также системы, которые отслеживают процесс и оповещают оператора об угрозе возникновения небезопасных условий.

6.6.2.3 Уровень 2. Диспетчерское управление

Уровень 2 системы сложного уровня с SCADA или BMS системами, включающими в себя базы данных, за исключением консолей программирования и рабочих станций инженеров.

Уровень 2 включает в себя следующие функции:

а) ЧМИ для операторов;

б) средства аварийно-предупредительной сигнализации для операторов;

в) функции диспетчерского контроля;

г) сбор данных о динамике процесса.

6.6.2.4 Уровень 3. Управление деятельностью

Уровень 3 — система с постоянно подключенными консолями программирования или инженерными рабочими станциями и другими корпоративными системами с системами дистанционного управления.

Уровень 3 включает в себя следующие функции:

а) предоставление отчетов о ходе производства на участках, в т. ч. о текущих производственных издержках;

б) сбор и хранение данных о ходе производства, имеющемся оборудовании, рабочей силе, сырье, запчастях и энергопотреблении для разных участков;

в) сбор данных и их автономный анализ в соответствии с требованиями инженерных функций. Это может включать в себя статистический анализ качества и соответствующие функции управления;

г) осуществление необходимых функций, относящихся к персоналу, таких как: статистика рабочего времени (например, время, задание), график отпусков, баланс рабочей силы, сводная диаграмма продвижений по службе, а также внутренние инструктажи и повышение квалификации персонала;

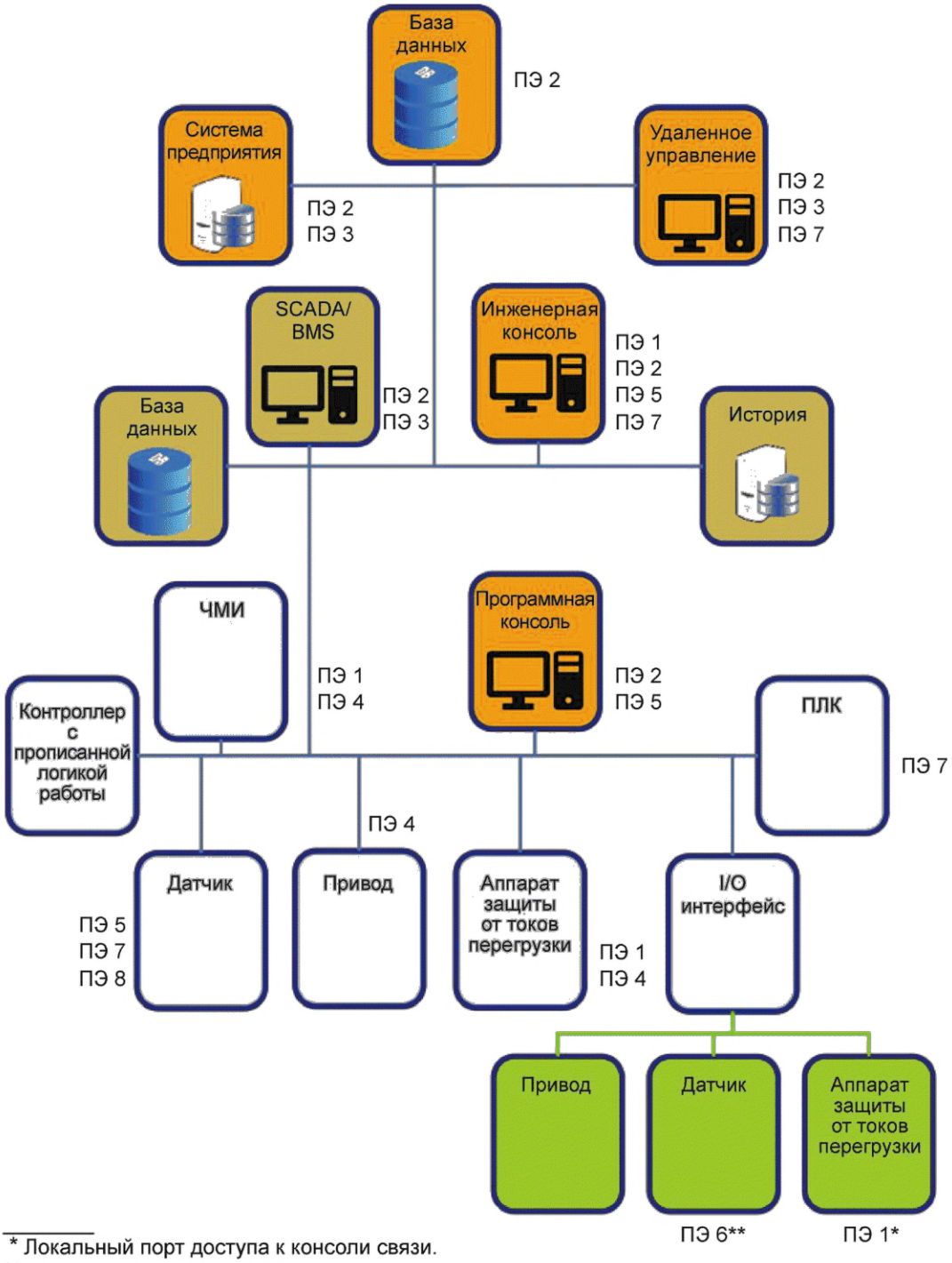
д) установление оперативного детального графика производства для отдельно взятых участков, который охватывает техническое обслуживание, транспортирование и другие производственные нужды;

е) оптимизацию издержек на отдельно взятых производственных участках при одновременном соблюдении графика производства, установленного функциями уровня 4;

ж) корректировку графиков производства для компенсации сбоев заводского производства, которые могут произойти на соответствующих участках ответственности.

Примечание — Особое внимание уделяется консолям программирования и инженерным рабочим станциям, которые содержат значительный перечень дополнительных инструментов для инициаторов атак. Их постоянное присутствие в системе управления является достаточным аргументом, чтобы отнести их к максимальному уровню риска.

На рисунке 2 представлены данные уровни функциональных возможностей в архитектуре систем управления.



* Локальный порт доступа к консоли связи.
** Локальный доступ к ЧМИ.

ПЭ — номер примера эксплуатации согласно приложению А;

— каналы связи (проводные или беспроводные); — провода цепи управления;

— система уровня 0 (аппаратура без возможностей связи); — система уровня 1;

— система уровня 2; — система уровня 3

Рисунок 2 — Архитектура системы управления

6.6.3 Виды структур подключения

Виды подключения систем управления (Cx) можно разделить на следующие структуры:

- C1 — изолированная, когда сеть системы управления полностью закрыта;
- C2 — предприятия подключены к информационной системе, но без возможности выполнения операций извне этой информационной системы. Данная информационная система может быть подключена к общественной сети, например сети Интернет, или даже распределена по нескольким объектам;
- C3 — подключение уровня C2 с помощью беспроводной связи, как показано на рисунке 3. Беспроводной доступ очень уязвим для атак;



Рисунок 3 — Структура подключения систем управления C3

- C4 — распределенная система управления с возможностью выполнения операций извне согласно рисунку 4. Разные объекты взаимодействуют между собой в пределах закрытой инфраструктуры. Эта инфраструктура может быть полностью частной или арендованной у оператора услуг связи. Данная структура также относится к системам управления, в которых возможны операции извне или из сети управления (например, удаленное обслуживание, удаленное управление);



Рисунок 4 — Структура подключения систем управления C4

- C5 — распределенная система управления с открытой инфраструктурой (сеть Интернет) согласно рисунку 5. Инициатор атаки может с легкостью получать доступ к разным точкам доступа в системе управления. Это обуславливает необходимость дополнительных мер обеспечения ИБ. Дополнитель-

ные ресурсы не выделяются системе управления, которая может стать «сопутствующей жертвой» аномально высокой загрузки сети.



Рисунок 5 — Структура подключения систем управления С5

К этой структуре относятся такие виды инфраструктуры, как APN или VPN типа MLP.

В этой структуре дополнительные потенциальные уязвимости связаны с обеспечением ИБ на уровнях контроля физического доступа и удаленного обслуживания.

6.6.4 Уровни потенциального воздействия на систему управления

Уровень потенциального воздействия на систему управления — это сочетание уровней функциональных возможностей средств связи и подключения. В таблице 2 приведены уровни потенциального воздействия на систему от Е1 (минимальный) до Е5 (максимальный). Он определяет объем рисков угроз ИБ, с которыми может сталкиваться система управления. При более высоких рисках угроз ИБ потребуется более обширная оценка рисков.

Таблица 2 — Уровень потенциального воздействия на систему управления

Уровни коммуникационной системы низковольтной аппаратуры	Уровни подключения систем управления (Cx)				
	C1	C2	C3	C4	C5
Система уровня 3	E3	E3	E4	E4	E5
Система уровня 2	E2	E2	E3	E4	E5
Система уровня 1	E1	E2	E3	E4	E5
Примечание – E1 – минимальный уровень потенциального воздействия; E5 – максимальный уровень потенциального воздействия.					

Уровни коммуникационной системы НКУ и подключения систем управления не имеют прямой зависимости друг от друга. По этой причине некоторые ячейки могут не соответствовать какой-либо реальной системе управления. На уровни могут влиять и другие факторы, включая количество задействованных аппаратов, и при оценке рисков угроз ИБ следует учитывать неоднородность используемой низковольтной аппаратуры.

Примеры оценки рисков угроз ИБ, связанных с их уровнем потенциального воздействия, находятся в стадии рассмотрения.

Не поддерживающая связь низковольтная аппаратура, показанная зеленым цветом на рисунке 2, не рассматривается в уровне потенциального воздействия, но должна быть включена в оценку рисков, если они содержат встроенное ПО.

Уровень потенциального воздействия применяют для оценки степени тяжести потенциального воздействия атак на низковольтную аппаратуру, чтобы выбрать соответствующие меры обеспечения ИБ (см. приложение А).

7 Требования к информационной безопасности

7.1 Общие положения

Следующие требования основаны на примерах эксплуатации, приведенных в приложении А.

Согласно требованиям раздела 6 изготовитель должен реализовать соответствующие меры по обеспечению ИБ, приведенные в 7.2—7.4.

Предполагается, что компоненты связи, связанные с низковольтной аппаратурой, должны поддерживать свой уровень функциональной целостности в пределах предполагаемой промышленной среды (физической и электромагнитной).

Примечание — Готовые потребительские устройства связи с расширенными возможностями, как правило, не соответствуют требованиям для применения в промышленной среде и имеют высокий уровень уязвимости ИБ.

7.2 Аспекты по обеспечению ИБ

Конфиденциальность данных, ограничение потока данных и своевременное реагирование на события не рассматриваются в настоящем стандарте.

Минимальный требуемый профиль безопасности представлен в таблице 3.

В приложении В приведена информация о каждом аспекте безопасности информации.

Таблица 3 — Минимальный профиль безопасности низковольтной аппаратуры и НКУ

Аспекты безопасности	Уровни безопасности SL1—SL4
Контроль идентификации и аутентификации	SL1
Контроль пользования	SL1
Целостность системы	SL1
Конфиденциальность данных	—
Ограничение потока данных	—
Своевременный отклик на события	—
Работоспособность и доступность ресурсов	SL1

Соответствующие векторы уровней безопасности рекомендуется выбирать согласно результатам оценки рисков угроз ИБ в соответствии с разделом 6.

7.3 Физический доступ с учетом места установки

Физический доступ к низковольтной аппаратуре должен исключать посторонних лиц. При этом двери, предусмотренные для зон ограниченного доступа, должны обеспечивать возможность беспрепятственной эвакуации на улицу путем открывания без использования ключа, инструмента или любого другого устройства, не являющегося частью механизма открывания.

При необходимости на основе результатов оценки рисков угроз ИБ должна быть разработана, задокументирована и внедрена стратегия обеспечения физической безопасности.

Электрические цепи и аппаратура для критических энергосистем должны быть доступны только для квалифицированного персонала.

Основными мерами управления физическим доступом к низковольтной аппаратуре являются запертые двери отдельных НКУ, опломбирование панелей НКУ, применение систем сигнализации и видеонаблюдение.

К помещениям, в которых устанавливаются НКУ, предъявляется перечень требований (см. [1], пункт А.11):

а) для охраняемых зон с целью предупреждения несанкционированного физического доступа, повреждения и вмешательства в основные функции аппаратуры, связанные с безопасностью:

1) должны быть определены периметры физической безопасности, используемые для защиты зон, содержащих чувствительную или критическую информацию и средства ее обработки;

2) физический контроль доступа: контроль доступа должен быть определен и реализован для авторизованных лиц для входа в помещения, где установлены НКУ, такие как электротехнические зоны с ограниченным доступом;

3) мониторинг физической безопасности с функциями наблюдения и упреждения: следует использовать средства безопасности для мониторинга безопасности помещений. Например, СОТ следует использовать для наблюдения и записи доступа к зонам повышенной безопасности в помещениях организации; следует развернуть пункты охраны для обнаружения доступа злоумышленников к помещениям организации или использовать охранную сигнализацию и другие устройства для обнаружения присутствия злоумышленников в помещениях организации;

4) защита от внешних атак и агрессивного воздействия окружающей среды: следует рассмотреть вопрос о физической защите от стихийных бедствий, физических атак или несчастных случаев и, если необходимо, разработать и реализовать их;

б) с целью предотвращения потери, повреждения или кражи аппаратуры и нарушения деятельности организации:

1) разделение аппаратуры по объектам и защита: хранилища необходимо защищать во избежание несанкционированного доступа. Меры контроля должны быть реализованы для минимизации рисков потенциальных физических и внешних угроз со стороны места установки, например кража, пожар, взрывы, задымление, вода (или перебои водоснабжения), пыль, вибрации, химические воздействия, уровни электромагнитных помех, превышающих общие уровни ЭМС, определенные для конкретной среды, и вандализм;

2) безопасность кабелей: силовые и телекоммуникационные кабели, по которым передаются данные или вспомогательные информационные услуги, должны быть защищены от перехвата, вмешательства или повреждения;

3) обслуживание низковольтной аппаратуры необходимо обслуживать в соответствии с требованиями, указанными изготовителем, чтобы гарантировать его постоянную доступность и целостность. Например, прошивку необходимо обновлять в соответствии с рекомендациями изготовителя;

в) постороннее вмешательство в низковольтную аппаратуру: если вышеупомянутые меры обеспечения ИБ не реализованы, аппаратуру необходимо защитить во избежание внутреннего доступа, например: отключение/удаление портов JTAG, опломбирование съемных крышек, отключение неиспользуемых периферийных портов процессора, конструктивные особенности корпусов аппаратуры, обеспечивающие их защиту от несанкционированного доступа, использование аппаратуры, защищающего от несанкционированного доступа, для соединения секций корпуса компонентов, если поставляются элементы местного управления настройками (при помощи дисплея или переключателей), обеспечение средств блокировки или пломбировки их от несанкционированного доступа.

7.4 Требования к программному обеспечению, встроенному в низковольтную аппаратуру

7.4.1 Общие положения

Изготовитель низковольтной аппаратуры должен учитывать требования, приведенные в 7.4.2—7.4.8.

7.4.2 Защита учетных данных

В низковольтной аппаратуре должно быть установлено только ПО, которое необходимо для поддержки его основных функций. Например, службы отладки, используемые во время разработки, должны быть удалены перед выпуском в обращение.

Чтобы ограничить учетные записи от вредоносных программ типа «бэкдор» и избежать жестко заданных учетных данных, в ПО, установленном в низковольтной аппаратуре, не должно быть учетных

записей, паролей или закрытых ключей, которые не могут быть изменены, отключены или удалены авторизованным конечным потребителем (пользователем).

7.4.3 Криптографическая защита информации

Для криптографической защиты информации применяют отраслевые рекомендации и руководящие принципы, разработанные на основе алгоритмов, приведенных в национальных нормативно-правовых документах в области ИБ. Изготовители низковольтной аппаратуры не должны изобретать собственные алгоритмы или использовать алгоритмы из неизвестных источников. Предоставляющий источник должен гарантировать обновления и исправления в случае уязвимостей и сбоев.

Изготовитель должен определить методику мониторинга уязвимостей для используемых функций безопасности.

Пример — Интеграция открытого SSL (протокол защиты информации).

7.4.4 Надежность и целостность ПО, встроенного в низковольтную аппаратуру

7.4.4.1 Проверка ИБ

Проверка ИБ должна выполняться, например, с помощью тестирования устойчивости, сканирования уязвимостей, статического анализа кода или анализа двоичного кода. Как правило, проверку проводят с использованием доступных инструментов.

Примечание — Руководство по разработке встроенного ПО для низковольтной аппаратуры, включая безопасное кодирование, см. в [2][1)].

Следует ограничить перечень доступного для запуска ПО. К запуску следует допускать только прикладное ПО и сервисы, необходимые для работы оборудования. Все остальное ПО должно быть запрещено к запуску и контролироваться на уровне операционной системы или средства защиты информации.

7.4.4.2 Целостность и подлинность ПО

Программные продукты должны иметь цифровую подпись, для обеспечения проведения проверки ПО пользователем на целостность и подлинность перед его использованием.

Потребителю (пользователю) рекомендуется проверять цифровую подпись перед установкой ПО в низковольтную аппаратуру.

Цифровая подпись должна быть окончательно проверена аппаратурой перед принятием установки. Необходимо обеспечить безопасную загрузку и безопасное обновление. Проверку необходимо выполнять в случае обновления ПО при помощи удаленной или беспроводной связи.

Асимметричные алгоритмы, используемые в цифровой подписи, должны быть выполнены на основе ГОСТ 34.10 и других национальных нормативно-правовых документов в области ИБ.

Цифровая подпись должна иметь формат в соответствии с использованием стандартных технологий.

Изготовители должны разработать процесс защиты закрытого ключа, используемого для подписи, от несанкционированного доступа (примеры управления ключами ИБ для низковольтной аппаратуры энергосистем см. в [3]). В случае компрометации закрытого ключа, например раскрытия или неправомерного использования, изготовители должны принять адекватные меры для восстановления целостности встроенного ПО и отозвать все сертификаты, связанные с ключом. CRL должен быть доступен и должен периодически обновляться изготовителем.

7.4.5 Отказ в обслуживании

Атаки типа DoS и DDoS, как правило, вызваны следующим:

- лавинной рассылкой (переполнение) пакетов в сети связи. В этом случае низковольтная аппаратура становится недоступной и неспособной отправлять данные и аварийные сигналы или выполнять команды системы SCADA или контроллера;
- перегрузкой ресурсов низковольтной аппаратуры, которая ведет к потере или некорректной работе основной функции;
- перезагрузкой встроенного в низковольтную аппаратуру ПО, которая ведет к временной потере основных функций.

ПО, встроенное в низковольтную аппаратуру, должно быть спроектировано таким образом, чтобы предотвратить влияние атак типа DoS и DDoS на его основные функции. Для снижения уровня воздей-

[1)] В Российской Федерации действует ГОСТ Р 56939—2016 «Защита информации. Разработка безопасного программного обеспечения. Общие требования».

ствия атак необходимо задействовать только требуемые для этого службы и порты. Функцию ограничения скорости передачи данных допускается реализовать при помощи сбрасывания пакетов данных при достижении порогового значения скорости.

Системная архитектура должна быть спроектирована таким образом, чтобы снизить вероятность и влияние DoS или DDoS. Например, сеть ОТ должна быть отделена от сети ИТ, а низковольтная аппаратура не должна иметь прямого доступа к сети Интернет без соответствующих мер обеспечения ИБ.

Для защиты от DoS-атак в рамках разрешенных сетевых соединений сетевые средства защиты информации должны предотвращать эксплуатацию уязвимостей, которые могут быть эксплуатированы по сети. Для этого межсетевые экраны необходимо настроить в режим белого списка, на них должен быть активирован модуль системы предотвращения вторжений и активированы правила для выявления эксплуатации известных уязвимостей и защиты от лавинной рассылки.

7.4.6 Проверка подлинности пользователей

Если интерфейсы низковольтной аппаратуры предназначены для доступа пользователя через периферийное оборудование или удаленно, они должны обеспечивать средства для выполнения идентификации и аутентификации законных пользователей — сотрудников, взаимодействующих с ними.

Для реализации функции аутентификации и авторизации следует использовать техники RBAC. Проверка подлинности пользователей может быть реализована, например, на основе паролей, смарт-карт, биометрических данных и т. д. Пример управления доступом для управления работой энергосистемы в зависимости от выполняемой функции см. в [4].

Авторизация пользователей должна быть основана на ролях и разрешениях для соответствующих пользователей. При определении ролей и разрешений следует руководствоваться принципом минимального перечня привилегий.

При первом использовании ПО, встроенного в низковольтную аппаратуру, необходимо предоставить как минимум один стандартный элемент учетных данных, который рекомендуется изменить.

Процесс проверки подлинности необходимо пересматривать и корректировать с учетом совершенствования требований политики безопасности. ПО, встроенное в низковольтную аппаратуру, должно поддерживать реализацию такой политики.

Проверка подлинности может быть проведена на самом ПО, встроенном в низковольтную аппаратуру, или быть компонентом системы в сети ОТ/ИТ.

События, связанные с ИБ, такие как попытки входа в систему, должны регистрироваться на уровне ПО, встроенного в низковольтную аппаратуру, или на уровне системы для мониторинга и последующего анализа. Кроме того, это хранилище событий (контрольный журнал) должно быть защищено от несанкционированного доступа (защита целостности).

Следует рассмотреть необходимость проверки подлинности и авторизацию пользователей ПО, чтобы гарантировать, что команды и данные поступают от доверенного оборудования.

7.4.7 Системы связи

Незащищенные системы связи следует изолировать от внешнего периметра с помощью меры физического доступа либо с применением межсетевого экрана на системном уровне или других эквивалентных мер обеспечения ИБ, таких как VPN или IPsec.

При необходимости авторизации с возможностью применения строгой аутентификации следует учитывать защищенные протоколы связи, например: защищенный протокол Modbus, «защищенный» ProfiNet[1)] (см. [5]), в качестве защищенного расширения протокола связи DNP3, а также протоколов связи (с учетом [6]).

7.4.8 Беспроводные системы связи

Для защиты беспроводной связи следует руководствоваться актуальными рекомендациями (см., например, [7]) в отношении Bluetooth или другого признанного стандарта.

7.5 Требования к защите аппаратной части низковольтной аппаратуры

7.5.1 Общие положения

Контроль фактической электрической схемы и перечня компонентов на соответствие указанным в документации — наиболее простой, производительный и минимально необходимый способ защиты от

[1)] Товарный знак ProfiNet® является примером подходящего протокола связи, реализуемого на платной основе. Данная информация приводится для удобства пользования настоящим стандартом и не представляет собой рекомендацию к применению этого протокола связи со стороны МЭК.

недопустимой неумышленной замены (брака) или умышленной подмены (закладки, аппаратного бэкдора).

7.5.2 Комплектность сопроводительных документов

Комплект документации с поставляемым оборудованием должен включать:

- принципиальную электрическую схему (Э3 по ГОСТ 2.702);
- электрическую схему соединений (Э4 по ГОСТ 2.702);
- перечень элементов электрической схемы (ГОСТ 2.701).

Примечание — Указанный перечень документов является минимально необходимыми для контроля электронной части оборудования.

7.5.3 Контроль несанкционированного вскрытия низковольтной аппаратуры

При испытаниях, входном контроле и эксплуатации необходимо осуществлять контроль несанкционированного вскрытия низковольтной аппаратуры:

а) провести идентификацию пломбировочного устройства, при его наличии;

б) в случае нарушения пломбировочного устройства или его отсутствия — проверить состав компонентов и электрической схемы оборудования на соответствие документации. По результатам проверки корпус в местах креплений пломбируется для предотвращения и/или индикации его вскрытия в процессе эксплуатации.

Типы пломбировочных устройств приведены в ГОСТ 31282. Рекомендуется применять пломбировочные устройства индикаторного типа.

7.5.4 Контроль электронных компонентов

На этапе производства низковольтной аппаратуры необходимо проверять соответствие электронных компонентов сопроводительной документации (в т. ч. их подлинность — отсутствие признаков контрафактного происхождения) перед монтажом (в случае собственного или контролируемого производства) или непосредственно на собранной печатной плате (в случае неконтролируемого производства).

Контрафактные электронные компоненты, как правило, не соответствуют заявленным техническим характеристикам либо имеют существенно сниженный срок эксплуатации или дополнительные уязвимости (не учтенные на этапе разработки и испытаний), которые повышают уровень угрозы безопасности и надежности работы системы в целом.

8 Инструкции по установке, эксплуатации и техническому обслуживанию

В дополнение к требованиям ГОСТ IEC 60947-1—2017, подраздел 6.3, изготовитель должен предоставить всю информацию для установки низковольтной аппаратуры и настройки, мер обеспечения ИБ, необходимых для поддержания заданного уровня ИБ.

Изготовитель должен указать меры обеспечения ИБ к потенциальным угрозам в отношении основных функций низковольтной аппаратуры.

В документацию на низковольтную аппаратуру должна быть включена следующая информация:

- требования к физической безопасности, при необходимости.

Пример — Низковольтную аппаратуру необходимо размещать в запираемом НКУ с уникальным ключом в целях ограничения доступа к его внешним незащищенным портам связи;

- описания портов связи и сервисов;
- перечень зависимостей от других компонентов системы для обеспечения безопасного развертывания.

Пример — Датчик IO-Link зависит от главного устройства IO-Link, чтобы гарантировать ограничения в поведении в защищенном режиме, а также аутентификацию конфигурации;

- описание всех учетных записей пользователей и системы с рекомендацией к изменению заданных по умолчанию паролей;
- рекомендации по установке;
- развернутая инструкция по настройке средств безопасности, предусмотренных в низковольтной аппаратуре или поставляемых в дополнение к ней (например, межсетевой экран, антивирус); руководство по настройке журнала регистрации событий и предупреждений (см. приложение Г).

Для соответствующих потенциальных требований и рекомендаций по ИБ изготовитель должен предоставить знаки безопасности, графические символы или примечания по безопасности, уязвимости. Символ, приведенный на рисунке 6, рекомендуется применять в документах и инструкциях по ИБ.



Рисунок 6 — Пример символа для инструкций по ИБ

Эффективность мер обеспечения ИБ низковольтной аппаратуры и НКУ зависит от анализа рисков угроз ИБ и выбранной стратегии ИБ всей системы; система ИБ требует внедрения с последующим управлением. В зависимости от ситуации (см. [8][1)] или [1]) возможно приведение в документации на низковольтную аппаратуру в качестве общих требований с учетом передовой практики.

При обнаружении уязвимостей системы ИБ при эксплуатации сведения об обнаруженной уязвимости в установленном порядке следует направить в национальный орган, регулирующий ИБ.

Рекомендации по стратегии ИБ приведены в приложении Г.

9 Разработка и испытания

9.1 Общий метод разработки

Для учета требований ИБ на низковольтную аппаратуру при проведении разработки и испытаний необходимо подготовить план разработки, включающий следующие рекомендации:

а) перечень реализации функций ИБ в отношении требований безопасности (см. раздел 6 [9]) применяют к низковольтной аппаратуре при необходимости;

б) проверку функциональных возможностей безопасности (см. [10], раздел 7, и [1], раздел 10) следует учитывать для обеспечения возможности поддержания проверки предполагаемой работы функций ИБ;

в) меры по разработке безопасного ПО (см. раздел 2 [2][2)]) применяют с учетом/совместно с мерами обеспечения ИБ, рассматриваемыми в качестве основных функций. При определении мер по разработке безопасного ПО должны учитываться требования, установленные действующими нормативными правовыми документами, документами по стандартизации и иными документами, принятыми уполномоченными органами власти (регуляторами). Дополнительные рекомендации к управлению ИБ см. в разделе 5 [9]:

- безопасность среды разработки, безопасные репозитории и ИБ в системе контроля версий;
- контрольные точки безопасности в рамках основных стадий проекта;
- способность разработчиков избегать, обнаруживать и исправлять уязвимости.

Дополнительные испытания низковольтной аппаратуры, предназначенной для работы в энергосистеме, см. в [11] и [12].

9.2 Испытания

Проверка безопасности и валидационное испытание должны проводиться в течение жизненного цикла проекта. Рекомендации см. в разделе 9 [9].

[1)] В Российской Федерации действует ГОСТ Р МЭК 62443-2-1—2015 «Сети коммуникационные промышленные. Защищенность (кибербезопасность) сети и системы. Часть 2-1. Составление программы обеспечения защищенности (кибербезопасности) системы управления и промышленной автоматики».

[2)] В Российской Федерации действует ГОСТ Р 56939—2016 «Защита информации. Разработка безопасного программного обеспечения. Общие требования».

Приложение А
(справочное)

Примеры эксплуатации

А.1 Общие положения

В настоящем приложении описаны ПЭ для обоснования соответствующих требований, применимых к НКУ и низковольтной аппаратуре.

А.2 Защита от вредоносных обновлений прошивки низковольтного коммутационного аппарата

Таблица А.1 — Пример защиты от вредоносных обновлений прошивки низковольтного коммутационного аппарата (ПЭ 1)

Название примера	Защита от обновления низковольтного коммутационного аппарата вредоносной прошивкой	
Обслуживание в течение эксплуатации	Техническое обслуживание на промышленном/коммерческом объекте с минимальным уровнем потенциального воздействия E3 (уровень коммуникационной системы 3, структура подключения системы управления C2) согласно таблице 2	
Стадия	Ввод в эксплуатацию и техническое обслуживание	
Задача и лица, получающие пользу	Обеспечение бесперебойного энергоснабжения конечных потребителей. Защита соответствующих критических данных (см. 6.5)	
Участники процесса	Злоумышленник	Инициатор атаки управляет несанкционированным воздействием
	Руководитель участка	Контролирует доступ к сети и гарантирует принятие надлежащих мер обеспечения ИБ
Общее описание: действия соответствующих участников процесса	Злоумышленник в своей лаборатории создает поврежденную прошивку (содержащую «логическую бомбу» (нежелательный код, вставленный в программное обеспечение, которое срабатывает только после того, как происходит конкретное событие). Злоумышленник отправляет фальшивое электронное письмо (спам) от изготовителя руководителям участков с прикрепленной вредоносной прошивкой с просьбой выполнить обновление из-за серьезной ошибки в низковольтном коммутационном аппарате. Руководитель участка верит электронному сообщению и приступает к обновлению. Поврежденная прошивка работает, как и оригинальная. В предварительно установленную дату низковольтный коммутационный аппарат отключается («логическая бомба» активируется). Все зараженные коммутационные аппараты отключаются одновременно. Руководитель объекта не видит первопричины такого события. После каждого включения коммутационного аппарата руководителем он снова отключается, непосредственно влияя на работу отдельного НКУ или электроснабжение всего объекта. Руководитель объекта обращается к изготовителю за диагностикой и исправлением проблемы. Все представленные в поддержку данные соответствуют ожидаемому поведению (оригинальная прошивка). Вариант: злоумышленник может потребовать выкуп	
Контрмеры	Изготовитель	Для гарантии целостности и подлинности прошивки низковольтного коммутационного аппарата все версии прошивки должны иметь цифровую подпись изготовителя. Эта цифровая подпись должна быть проверена перед началом выполнения прошивки
	Руководитель объекта	Руководители объектов должны определить строгую политику обновления прошивки. Например: - определение списка сотрудников, ответственных за критическое обслуживание, такое как обновление прошивки; - определение необходимых тренингов по обеспечению ИБ; - определение для этих сотрудников соответствующих прав доступа с утвержденными инструментами обновления (компьютер, ПО и т. д.); - проверка веб-сайта изготовителя для получения последних актуальных мер обеспечения ИБ

А.3 Защита от несанкционированного доступа к информационной сети предприятия

Таблица А.2 — Пример защиты от несанкционированного доступа к информационной сети предприятия (ПЭ 2)

Название примера	Защита от несанкционированного доступа к информационной сети предприятия. В случае несанкционированного доступа к информационной сети предприятия злоумышленники могут выключить и/или отправить ложные команды на низковольтную аппаратуру (например, выключатели)	
Обслуживание в течение эксплуатации	В течение эксплуатации или ввода в эксплуатацию на производственном объекте с минимальным уровнем потенциального воздействия Е2 (уровень коммуникационной системы 1, структура подключения системы управления С2) в соответствии с таблицей 2	
Стадия	Производственный процесс на предприятии	
Задача и лица, получающие пользу	Обеспечить неприкосновенность к информационной сети предприятия во избежание ложных команд и изменения состояния установленного низковольтного оборудования. Избежать критических аварий и ненадлежащего использования низковольтной аппаратуры с последующим нарушением функций, связанных с безопасностью	
Участники процесса	Злоумышленник	Инициирует атаку, входящую в производственную сеть
	Руководитель участка	Контролирует доступ к сети и гарантирует принятие надлежащих мер обеспечения ИБ
	Инженер по ИБ отдела ИТ	Отвечает за осведомленность о возможных фишинговых сообщениях электронной почты, а также за эффективность межсетевого экрана и безопасность сети
	Сотрудники	Сотрудники не распознают фишинговую атаку и переходят по ссылке на вредоносный сайт, предоставляя злоумышленнику доступ к сети компании
Общее описание: действия соответствующих участников процесса	Злоумышленнику необходим доступ к производственной сети. Используя соединение между корпоративной сетью (ИТ) и производственной сетью (ОТ), он начинает рассылать фишинговые электронные письма (с указанием конкретных целей и достоверным содержанием) сотрудникам, чтобы получить логин и пароль для доступа к сети. Высокотехнологичные инструменты злоумышленника не только в ИТ, но и в промышленной системе управления (ICS). Некоторые сотрудники верят фишинговым сообщениям электронной почты, и злоумышленник может получить доступ к корпоративной сети и, следовательно, к производственной сети с прямым доступом к низковольтной аппаратуре. Чем выше уровень автоматизации завода, тем выше риски критических повреждений. Руководитель объекта обнаруживает некорректное поведение низковольтной аппаратуры, отключает автоматическое управление низковольтной аппаратурой и решает начать ручные операции. Отдел ИБ начинает расследование, чтобы понять, как злоумышленнику удалось проникнуть в производственную сеть и управлять низковольтной аппаратурой	

А.4 Защита от распределенных атак типа DDoS (отказ в обслуживании) через незащищенную аппаратуру с IoT

Таблица А.3 — Пример защиты от распределенных атак типа DDoS (отказ в обслуживании) через незащищенную аппаратуру с IoT (ПЭ 3)

Название примера	Защита от атаки типа DDoS посредством незащищенных аппаратов IoT. DDoS-атака приводит к перегрузке производственной сети интернет-трафиком из разных мест, что приводит к сбою системы управления
Обслуживание в течение эксплуатации	Электромонтаж с минимальным уровнем потенциального воздействия Е4 (уровень коммуникационной системы 2, структура подключения системы управления С4) согласно таблице 2
Стадия	Электромонтажные работы в здании, на промышленном/коммерческом объекте

Окончание таблицы А.3

Задача и лица, получающие пользу	Обеспечить непрерывную работу системы управления при несанкционированном воздействии DDoS. Избежать отключения системы управления и злоумышленного использования каналов связи в производственной сети	
Участники процесса	Злоумышленник	Инициирует DDoS-атаку в отношении уязвимых аппаратов
	Управляющая компания	Отвечает за управление эксплуатацией и обслуживание зданий
	Техник по обслуживанию объектов	Проводит работы с объектами, включая обслуживание, ремонт и поддержку клиентов
Общее описание: действия соответствующих участников процесса	Злоумышленник устанавливает вредоносное ПО на один незащищенный IoT-аппарат, подключенный к сети Интернет. Примеры незащищенных аппаратов — это аппараты бытового и аналогичного назначения с непроверенным уровнем безопасности. Многие аппараты используют пароль по умолчанию и не имеют функции обновления ПО. Вредоносная программа сканирует сеть Интернет на предмет заражения других незащищенных аппаратов IoT и пытается войти на обнаруженные аппараты, используя наиболее распространенные имена пользователей и пароли по умолчанию. Вредоносная программа устанавливается на аппараты, где авторизация прошла успешно. Когда запускается вредоносное ПО, сотни или даже тысячи незащищенных аппаратов IoT превращаются в удаленно управляемых «ботов», готовых участвовать в DDoS-атаках. Злоумышленник сканирует сеть Интернет на предмет устройств для атаки и запускает DDoS-атаку на выбранные устройства, используя ботов. Одно из устройств, которое является целью атаки, — это система управления отоплением, которая контролирует отопление и вентиляцию в здании. Система управления отоплением перегружена трафиком и пытается ответить на атаку перезагрузкой основной цепи управления. Это повторяется, и, наконец, система управления отключается, что вызывает незапланированные простои отопления и вентиляции в здании. Управляющая компания, которая отслеживает и настраивает систему управления удаленно, обнаруживает, что удаленное соединение потеряно. Невозможно восстановить соединение, поэтому управляющая компания направляет в здание специалиста по обслуживанию для изучения проблемы на месте. Проблема решается в два этапа: 1) первый шаг предпринимает техник, который отключает поврежденное оборудование от сети Интернет и переключает систему отопления в ручной режим; 2) управляющая компания проверяет причины и пытается найти решение. Атака DDoS устраняется путем установки межсетевого экрана между системой управления и сетью Интернет перед повторным подключением системы. Межсетевой экран предотвращает попадание DDoS-атаки в систему управления, поскольку вредоносный трафик фильтруется	
Контрмеры	Применяют несколько уровней защиты в соответствии с архитектурой эшелонированной (многоуровневой) защиты: - системный уровень: обеспечить ИБ на протяжении всего жизненного цикла системы управления, от проектирования до монтажа и от ввода в эксплуатацию до обслуживания; - сетевой уровень: логическое разделение между ЛВС системы управления (локальной сетью) и другой сетью с помощью межсетевого экрана, управляемых коммутаторов, однонаправленных шлюзов и т. д. В ЛВС системы управления должен быть разрешен только законный трафик; не подключать потребительскую или незащищенную низковольтную аппаратуру (аппараты со слабой защитой) к локальной сети системы управления; - уровень аппаратуры: повысить уровень безопасности аппаратуры системы управления путем принятия следующих мер: отключить неиспользуемые порты и службы; обновить прошивку аппаратуры, чтобы гарантировать установку последних исправлений ИБ; проверить надежность аппаратуры, включая лавинные сообщения «флудинг» и тестирование защиты (например, методом «фаззинг»); заменить пароль по умолчанию надежным паролем, уникальным для конкретного аппарата	

А.5 Защита от несанкционированного доступа к информационной сети с помощью легитимного аппарата

Таблица А.4 — Пример защиты от несанкционированного доступа к информационной сети с помощью легитимного аппарата (ПЭ 4)

Название примера	Защита от неавторизованной аппаратуры, подключенной к сети связи. Сбор информации, дистанционное управление низковольтной аппаратурой	
Обслуживание в течение эксплуатации	Электромонтаж с начальным уровнем потенциального воздействия E2 (уровень коммуникационной системы 1, структура подключения системы управления C2) согласно таблице 2. Этот уровень меняется на E4 (уровень коммуникационной системы 1, структура подключения системы управления C4) после взлома с помощью дополнительного устройства связи	
Стадия	Техническое обслуживание на промышленном/коммерческом объекте	
Задача и лица, получающие пользу	Обеспечение защиты и безопасности сети от потенциального воздействия при помощи неавторизованных аппаратов, интегрированных в эту сеть. Избежание выключения и плохой связи внутри сети	
Участники процесса	Злоумышленник	Инициирует атаку пытается заполучить удаленный контроль над сетью
	Администратор сети	Обслуживает и обеспечивает безопасность сети, отслеживает подключение низковольтной аппаратуры IoT
	Инженер по безопасности отдела ИТ	Отвечает за работоспособность межсетевого экрана и безопасность сети
	Оператор на периферии	Проверяет и обслуживает установленную низковольтную аппаратуру
	Злоумышленник	Проникает в электротехническое помещение и подключает к сети неавторизованный аппарат 3G/4G
	Инженер по безопасности объекта	Отвечает за безопасность помещений
Общее описание: действия соответствующих участников процесса	Из-за недостаточной физической безопасности в электротехнических помещениях и НКУ злоумышленник может проникнуть в электротехническое помещение, открыть секцию НКУ и подключить устройство связи 3G/4G к сети. Дистанционно злоумышленник может подключиться к внутренней сети с помощью средств связи 3G/4G и обойти все меры обеспечения ИБ, предусмотренные для сети Интернет и внутренних сетей (межсетевые экраны и т. д.). Он сможет: - отправлять команды отключения низковольтной аппаратуры; - изменять данные и параметры низковольтной аппаратуры; - отправлять ложные данные слежения за системой (при наличии); - создавать помехи для работы сети. Это может немедленно повлиять на корректную работу системы из-за отключения части низковольтной аппаратуры	
Подробное описание: триггер, этапы, относящиеся к тому, как участники процесса взаимодействуют и т. д.	Физический доступ и использование нелегальных устройств связи	
	Доступ	Из-за отсутствия политики физической безопасности и мер обеспечения ИБ посторонний может получить доступ к содержимому электротехнических помещений и НКУ. Это нарушение безопасности
	Соединение	Злоумышленник может подключить незаконное устройство с возможностью автономной связи на большие расстояния (3G/4G или даже Wi-Fi)
	Атака	Использование удаленного подключения для внедрения вредоносных данных и/или поведения
	Обнаружение	Местный оператор на периферии или сетевой администратор обнаруживает аномальное поведение и пытается найти первопричину. Дальнейший физический осмотр оператором на периферии позволяет обнаружить и демонтировать незаконное устройство

Окончание таблицы А.4

Контрмеры	Определение и реализация политики физической безопасности и реализация процессов обнаружения незаконных устройств	Применение принципа эшелонированной (многоуровневой) защиты с добавлением физической безопасности: - должна быть реализована физическая безопасность для предупреждения доступа посторонних лиц в электротехнические помещения; - должна быть реализована физическая безопасность для предотвращения доступа посторонних лиц к НКУ; - для обнаружения подозрительных компонентов или устройств следует провести физический осмотр. Для обнаружения новых/подозрительных устройств связи необходимо реализовать мониторинг сети: - подходящей будет регистрация в системе: только аппаратура, имеющая сертификат, подписанный уполномоченным органом, может связываться с системой

А.6 Защита от вредоносного обновления прошивки аппарата (например, бесконтактное реле), установленного в НКУ, подключенного проводным способом к интерфейсу IO-Link

Таблица А.5 — Пример защиты от вредоносного обновления прошивки аппарата (например, бесконтактное реле), установленного в НКУ, подключенного проводным способом к интерфейсу IO-Link (ПЭ 5)

Название примера	Защита от вредоносного обновления прошивки аппарата (например, бесконтактное реле), установленного в НКУ, подключенного проводным способом к интерфейсу IO-Link	
Обслуживание в течение эксплуатации	Монтаж, эксплуатация, обслуживание при минимальном уровне потенциального воздействия E2 (уровень коммуникационной системы 1, структура подключения системы управления C2) согласно таблице 2	
Стадия	Стадия эксплуатации техники, регулярное техническое обслуживание	
Задача и лица, получающие пользу	Обеспечить актуальную конфигурацию, целостность файлов (конфигурация, функции, параметры и т. д.), полученных от изготовителя. Выгода для компании-оператора, оператора и изготовителя аппаратуры: надежная работа НКУ, отсутствие жалоб клиентов	
Участники процесса	Злоумышленник	Инициирует атаку с целью изменения или организации атаки на установленную прошивку
	Инженер по автоматизации производства	Определяет полномочия и роли, а также контролирует и обслуживает систему автоматизации
	Оператор по обслуживанию	Инициатор обновления (действие)
	Оператор на периферии	Никаких действий в этом процессе

Окончание таблицы А.5

<table>
<tr><td>Общее описание: действия соответствующих участников процесса</td><td colspan="2">Злоумышленник в своей лаборатории создает поврежденную прошивку (включая «логическую бомбу»).
Злоумышленник представляет поврежденную прошивку для загрузки по электронной почте или в сети Интернет/на поддельной домашней странице.
Инженер по автоматизации производства доверяет поддельной электронной почте, сети Интернет/поддельной домашней странице (поврежденная прошивка).
Инженер по автоматизации производства загружает и сохраняет поврежденную микропрограмму в инструменте обслуживания.
Оператор по обслуживанию отсоединяет соединительный кабель или вилку аппарата и подключает аппарат к инструменту для обслуживания.
Оператор по обслуживанию инициирует загрузку поврежденной прошивки из инструмента обслуживания в аппарат в соответствии с определенным процессом.
Оператор по обслуживанию отсоединяет инструмент для обслуживания и снова подключает соединительный кабель или вилку к аппарату.
НКУ работает, поврежденная прошивка остается незамеченной, пока испорченная прошивка не вызовет неисправность (поддельные данные/информация) и т. д.
Инженер по автоматизации производства или оператор замечает неисправность и отправляет изготовителю жалобу клиента (обнаружение скимминга маловероятно).
Инженер по обслуживанию или изготовитель заменяет аппарат в НКУ.
Отдел качества изготовителя проводит расследование, чтобы выяснить причину неисправности. Подходящая проверка достоверности или оригинальности установленной прошивки позволяет определить поврежденную прошивку</td></tr>
<tr><td rowspan="4">Подробное описание: триггер, этапы, относящиеся к тому, как участники процесса взаимодействуют и т. д.</td><td>Инженер по автоматизации производства</td><td>Инженер по автоматизации производства доверяет поддельной электронной почте, сети Интернет/поддельной домашней странице. Он думает, что это легитимный источник данных</td></tr>
<tr><td>Оператор по обслуживанию</td><td>Оператор по обслуживанию доверяет поврежденной прошивке. Инструмент обслуживания и аппарат не имеют встроенной проверки достоверности или оригинальности для идентификации поврежденной прошивки</td></tr>
<tr><td>Инженер по автоматизации производства</td><td>Инженер по автоматизации производства или отдел качества инициирует работы с жалобой потребителя</td></tr>
<tr><td>Изготовитель</td><td>Изготовитель проводит анализ, чтобы выяснить причину рекламации. Сравнивая исходный код и контрольную сумму, можно найти испорченную прошивку</td></tr>
<tr><td rowspan="2">Контрмеры</td><td>Технологические</td><td>Для обеспечения гарантии целостности и подлинности прошивки аппаратуры все их версии должны иметь цифровую подпись изготовителя. Эту цифровую подпись необходимо проверить перед выполнением. Цифровая подпись должна быть определена с учетом уровня безопасности (SL1—SL4 настоящего стандарта) и потенциальных рисков неисправности. Необходим анализ рисков угроз ИБ</td></tr>
<tr><td>Организационные</td><td>Отдел автоматизации производства должен определить строгую политику обновления прошивки. Например:
- определить список сотрудников, ответственных за критическое обслуживание, такое как обновление прошивки;
- определить необходимые тренинги по ИБ;
- определить для этих сотрудников соответствующие права доступа с утвержденными инструментами обновления, например ПК, ПО, инструмент обслуживания (от изготовителя);
- проверить на веб-сайте изготовителя наличие актуальных контрмер по безопасности информации;
- определить разрешенный источник (домашняя страница/ссылки изготовителя) для загрузок</td></tr>
</table>

А.7 ЧМИ. Защита от несанкционированного доступа к аппарату (установленному в НКУ) — некорректная параметризация

Таблица А.6 — Пример защиты от несанкционированного доступа к аппарату (установленному в НКУ) — некорректная параметризация (ПЭ 6)

Название примера	ЧМИ. Защита от несанкционированного доступа к аппарату (установленному в НКУ) — некорректная параметризация	
Обслуживание в течение эксплуатации	Работа с минимальным уровнем потенциального воздействия E1 согласно таблице 2 имеет низший уровень, без наличия функциональных возможностей связи	
Стадия	Стадия активации техники	
Задача и лица, получающие пользу	Обеспечивает непрерывность, достоверность информации/данных и функций. Выгода для компании-оператора, оператора и изготовителя аппарата: надежная работа НКУ, отсутствие жалоб клиентов. Этот вариант использования описывает аппарат, снабженный только кнопками и светодиодом для программирования параметризации	
Участники процесса	Инициатор атаки	Инициирует атаки, изменяет заданные и настроенные параметры аппарата в текущем состоянии
	Инженер по автоматизации производства	Никаких действий
	Оператор по обслуживанию	Никаких действий
	Администратор сети ИТ	Никаких действий
	Оператор на периферии	Никаких действий
Общее описание: действия соответствующих участников процесса	Аппарат установлен в НКУ. Аппарат функционирует по установленным параметрам. Аппарат и НКУ работают должным образом. Инициатор атаки имеет физический доступ к аппарату (кнопкам), установленному в НКУ. Аппарат не защищен от изменения настроек параметров. Злоумышленник может изменить значения параметров аппарата на ложные с помощью кнопок. Несанкционированное изменение конфигурации параметров может оставаться незамеченным в течение длительного времени в зависимости от приложения. Несанкционированное изменение конфигурации аппарата будет обнаружено, когда будет достигнуто критическое состояние в процессе; например будет достигнут максимальный уровень в резервуаре, и аппарат не сгенерирует сигнал обнаружения	
Подробное описание: триггер, этапы, относящиеся к тому, как участники процесса взаимодействуют и т. д.	Инициатор атаки	Злоумышленник имеет доступ к ручному управлению настройками эксплуатации, например домашняя страница изготовителя (не обязательно). Злоумышленник получает доступ к аппарату, установленному в НКУ. Злоумышленник активирует режим программирования (сознательно или методом проб и ошибок). Злоумышленник манипулирует параметрами. Злоумышленник или аппарат автоматически активирует измененные параметры. Злоумышленник уходит от аппарата незамеченным

Окончание таблицы А.6

Контрмеры	Изготовитель	Подходящие меры обеспечения ИБ отсутствуют. Обязанность предоставлять информацию: изготовитель должен указать в документации на аппарат (например, в руководстве по эксплуатации): - в аппарат не встроены средства защиты; - подходящий метод интеграции, например с дополнительным аксессуаром для ограничения доступа к кнопке аппарата
	Интегратор/ пользователь	Интегратор и оператор обязаны принимать соответствующие меры по обеспечению ИБ в соответствии с требованиями законодательства

А.8 ЧМИ. Защита от несанкционированного доступа к аппарату (установленному в НКУ) — некорректная параметризация

Таблица А.7 — Пример защиты от несанкционированного доступа к аппарату (установленному в НКУ) — некорректная параметризация (ПЭ 7)

Название примера	ЧМИ. Защита от несанкционированного доступа к аппарату (установленному в НКУ) — некорректная параметризация	
Обслуживание в течение эксплуатации	Эксплуатация при минимальном уровне потенциального воздействия E2 (уровень коммуникационной системы 1, структура подключения системы управления C2) согласно таблице 2	
Стадия	Стадия активации техники	
Задача и лица, получающие пользу	Обеспечить непрерывность и достоверность информации/данных и функций. Выгода для компании-оператора, оператора и изготовителя аппарата: надежная работа НКУ, отсутствие жалоб клиентов. Пример использования описывает аппарат, оснащенный кнопками и дисплеем, доступный через интерфейс данных для программирования параметров и блокировки кнопок	
Участники процесса	Злоумышленник	Инициирует атаки, изменяет заданные и настроенные параметры аппарата в текущем состоянии
	Инженер по автоматизации производства	Никаких действий
	Оператор по обслуживанию	Никаких действий
	Администратор сети ИТ	Никаких действий
	Оператор на периферии	Никаких действий
Общее описание: действия соответствующих участников процесса	Аппарат установлен в НКУ. Аппарат работает по установленным параметрам. Аппарат и НКУ работают должным образом. Злоумышленник имеет физический доступ к аппарату. Аппарат не защищен от перепрограммирования. Злоумышленник может модифицировать аппарат с помощью поддельных параметров. Несанкционированное перепрограммирование может оставаться незамеченным в течение длительного времени, в зависимости от приложения. Несанкционированное перепрограммирование аппарата будет обнаружено, когда будет достигнуто критическое состояние в процессе; например, достигается максимальный уровень в резервуаре, и аппарат не генерирует сигнал обнаружения	

Окончание таблицы А.7

Подробное описание: триггер, этапы, относящиеся к тому, как участники процесса взаимодействуют и т. д.	Злоумышленник	Получает доступ к инструкции по эксплуатации, например домашняя страница изготовителя (не обязательно). Получает доступ к аппарату, нарушая меры безопасности инфраструктуры. Узнает о вариантах доступа к аппарату. Входит в программный интерфейс, используя пароль по умолчанию или раскрытый пароль и идентификатор. Активирует режим настройки параметров и манипулирует ими. Злоумышленник или аппарат автоматически активирует измененные параметры
Контрмеры	Изготовитель	Устанавливает средство контроля доступа пользователей, например имена пользователей и пароли. Примеры реализации контроля доступа: - задержка в случае ввода неверного пароля; - задержка в случае перезапуска; - шифрование удаленного доступа; - отключение локальных кнопок аппарата; - регистрация числа неудачных попыток входа; - запрет доступа после регистрации *x* неудачных попыток входа в систему; - управление учетными записями пользователей (права/роли); - возможность смены пароля; - минимальная сложность пароля; - обязательная смена исходных паролей; - аппарат не должен работать без предварительной смены пароля; - подтверждение ввода; - использование протоколов, ориентированных на подключение; - предварительно определенные состояния выводов; - реализация базовой функции безопасности согласно настоящему стандарту
	Интегратор/ пользователь	Интегратор/пользователь должен создать и задокументировать определением авторизации. Интегратор/пользователь должен реализовать указанные выше аспекты, насколько ему известно, в соответствии с определением авторизации. Интегратор/пользователь обязан принимать соответствующие меры безопасности в соответствии с требованиями оператора и требованиями законодательства

А.9 Защита от несанкционированного доступа к аппарату (например, бесконтактное реле), установленному в НКУ, подключенному через беспроводной интерфейс связи (WCI)

Таблица А.8 — Пример защиты от несанкционированного доступа к аппарату (например, бесконтактное реле), установленному в НКУ, подключенному через беспроводной интерфейс связи (WCI) (ПЭ 8)

Название примера	Защита от несанкционированного доступа к аппарату (например, бесконтактное реле), установленному в НКУ, подключенному через беспроводной интерфейс связи (WCI)
Обслуживание в течение эксплуатации	Эксплуатация, обслуживание при минимальном уровне потенциального воздействия Е3 (уровень коммуникационной системы 1, структура подключения системы управления С3) согласно таблице 2
Стадия	Стадия активации техники
Задача и лица, получающие пользу	Обеспечить непрерывность и достоверность информации/данных и функций. Выгода для компании-оператора, оператора и изготовителя аппарата: надежная работа НКУ, отсутствие жалоб клиентов. Этот вариант использования также применим в системе интеллектуального производства

Окончание таблицы А.8

Участники процесса	Злоумышленник	Злоумышленник пытается получить доступ к переданным данным/информации аппарата через WCI (чтение и изменение данных/информации)
	Инженер по автоматизации производства	Никаких действий
	Оператор по обслуживанию	Никаких действий
	Администратор сети ИТ	Он отвечает за то, чтобы только авторизованная аппаратура имела доступ к WCI
	Оператор на периферии	Никаких действий
Общее описание: действия соответствующих участников процесса	У злоумышленника есть необходимое техническое оснащение. У него есть необходимые ноу-хау. Злоумышленник находится в диапазоне действия сети. Получает доступ к беспроводной сети: - читает данные/информацию; - изменяет данные/информацию и передает их получателю; - на аппарат воздействует таким образом, что он выходит из строя	
Подробное описание: триггер, этапы, относящиеся к тому, как участники процесса взаимодействуют и т. д.	Злоумышленник	Злоумышленник преодолевает существующие методы аутентификации. Реализация на радиочипе имеет недостаток безопасности, беспроводной протокол допускает вторжения. Или получает доступ к паролю: - считывает данные/информацию: это не обнаруживается; - меняет данные/информацию и передает их получателю, это не обнаруживается; - при воздействии злоумышленника аппарат выходит из строя. В результате канал связи переходит на аппарат более высокой производительности
Контрмеры	Изготовитель	Внедрение аутентификации и подтверждения; дополнительно обеспечение шифрования данных/информации; подписание данных/информации (целостность данных); изменение частоты канала передачи. Изготовитель должен предоставить защищенные обновления прошивки, при необходимости. Настройка двух разных радиоканалов для критических приложений (разнесение)
	Интегратор/ пользователь	Проведение анализа рисков угроз ИБ для конкретного приложения и определение соответствующих мер обеспечения ИБ. Мониторинг радиочастот. Электромагнитное экранирование производственных помещений. Мероприятия умного производства: - применение передовых технологий для аутентификации; - регулярное обновление прошивки; - контроль подключенных/неподключенных аппаратов в сети (например, MAC-адреса); - применение разных радиоканалов для критических приложений (разнесение); - инициирование процесса автоматического уведомления обо всех аномальных процессах; - сканирование на наличие несанкционированных точек доступа для обнаружения неавторизованных точек доступа

Приложение Б
(справочное)

Информационная безопасность и архитектура электрических систем

Б.1 Общие положения

Эффективный способ снижения риска угроз ИБ — распределить меры обеспечения ИБ на разных уровнях архитектуры рассматриваемой системы. НКУ распределения и управления также используются на первичном и вторичном уровнях распределения и управления электроэнергией.

Следует применять нисходящий подход для определения соответствующих мер обеспечения ИБ на каждом уровне архитектуры электрической системы.

Б.2 Пример архитектуры с применением низковольтной аппаратуры

Б.2.1 Здание

Уровни ИБ здания можно определить следующим образом:

1) сеть объекта (кампуса): межсетевой экран, антивирус, VPN;
2) ИТ-службы (ERP, сервер электронной почты, офис ИТ и т. д.);
3) сети здания: обнаружение вторжения, сетевые интерфейсы (ОВиК, ИТ, BMS и т. д.);
4) техническое помещение: ограждения, замки, контроль доступа;
5) сеть или система связи НКУ: межсетевой экран панели, проверка подлинности, проверка безопасности;
6) программируемый контроллер панели: защита приложений, управление исправлениями;
7) связь коммутационного аппарата: контроль, конфигурация.

На рисунке Б.1 представлен пример электрической архитектуры здания.



ГРЩ — главный распределительный щит; РЩ 1 — РЩ *n* — распределительный щит (*n* — порядковый номер щита)

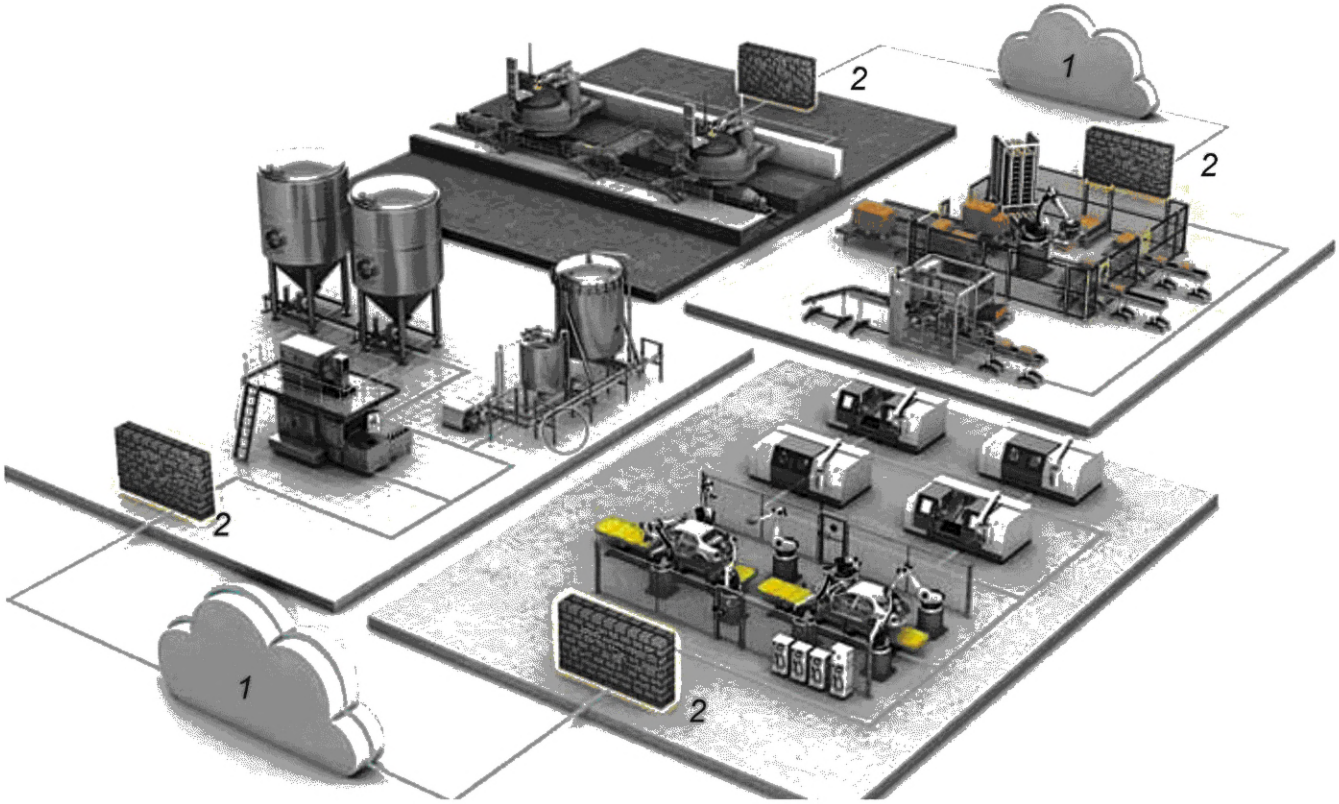
Рисунок Б.1 — Электрическая архитектура здания

Б.2.2 Производство

Уровни ИБ производственного объекта можно определить следующим образом:

1) ИТ-сеть: межсетевой экран, VPN, DMZ;
2) производственная сеть: межсетевой экран, VPN;
3) сеть цеха: определение вторжения;
4) физический: замки, контроль доступа;
5) сеть или система машинной связи: межсетевой экран оборудования, аутентификация, антивирус, проверка безопасности;
6) программируемый контроллер, установленный в НКУ: защита приложений, управление исправлениями;
7) система управления безопасностью: целостность безопасности;
8) связь НКУ управления: контроль, конфигурация, целостность безопасности.

На рисунке Б.2 представлено четыре примера производственных площадок (автомобилестроение и станкостроение, конвейерное производство и упаковка, химическая и пищевая промышленность).



1 — сеть Интернет; *2* — межсетевой экран

Рисунок Б.2 — Промышленные объекты

Б.3 Уровни системной безопасности низковольтной аппаратуры

При разработке требований к низковольтной аппаратуре необходимо рассматривать риски угроз ИБ в интерфейсах, например fieldbus, USB, ЛВС. Для дистанционного управления и обеспечения связи рекомендуется классифицировать его по одному из следующих уровней безопасности (см. [10]):

а) SL1: предотвращение неавторизованного раскрытия информации посредством ее несанкционированного извлечения или случайного обнародования (защита от случайного нарушения);

б) SL2: предотвращение неавторизованного раскрытия информации субъекту, активно ее ищущему с использованием простых средств, при незначительных ресурсах, посредственных навыках и низкой мотивации;

в) SL3: предотвращение неавторизованного раскрытия информации субъекту, активно ее ищущему, с использованием изощренных средств при умеренных ресурсах, наличии специальных познаний в IACS и умеренной мотивации;

г) SL4: предотвращение неавторизованного раскрытия информации субъекту, активно ее ищущему, с использованием изощренных средств при обширных ресурсах, наличии специальных познаний в IACS и высокой мотивации.

Требования к низковольтной аппаратуре должны определять требования ИБ, которые необходимы для достижения уровней безопасности, упомянутых в перечислениях а) — г), с учетом следующих аспектов:

1) меры для защиты от данного типа угроз путем настройки на стадии проектирования и установки;

2) оценка рисков угроз ИБ, необходимость защиты конкретной зоны от соответствующего уровня угрозы [см. перечисления а) — г)];

3) сотрудник, выполняющий либо сочетающий несколько функций: владельца актива, системного интегратора, поставщика низковольтной аппаратуры, — должен настроить зону, систему или компонент для удовлетворения конкретных требований безопасности, описанных в перечислениях а) — г).

Приложение В
(справочное)

Базовые аспекты информационной безопасности

В.1 Общие положения

В настоящем приложении приведен перечень аспектов ИБ, которые применимы к низковольтной аппаратуре (см. [10]).

Примечание — Профили ИБ в соответствии с [13][1)] и соответствие требований этого документа [1] и [10] находятся на рассмотрении.

В.2 Идентификация и аутентификация

Если интерфейсы низковольтной аппаратуры обеспечивают доступ пользователю к основной функции, связанной с безопасностью, следует учитывать возможность идентификации и аутентификации всех пользователей.

Примеры предотвращения несанкционированного доступа и внесения изменений включают:

- идентификацию и аутентификацию пользователей;
- аутентификацию сетей;
- управление учетными записями программ;
- управление беспроводным доступом;
- защиту с помощью аутентификации на основе пароля;
- ограничения по генерированию и сроку действия паролей для пользователей.

В.3 Контроль использования

После идентификации и аутентификации пользователя рекомендуется оставлять ограничение использования основной функции, связанной с ИБ (присвоенные привилегии прошедшего аутентификацию пользователя).

В.4 Целостность системы

Пользователь оборудования (владелец актива) несет ответственность за поддержание целостности системы в отношении основной функции, связанной с ИБ, реализуемой изготовителем оборудования.

Для обеспечения целостности системы критическими могут быть следующие аспекты:

- целостность/повреждение каналов связи (ЛВС, WLAN и т. д.), например использование криптографической защиты целостности (например, VPN);
- защита от вредоносного кода (от манипуляций, например вирусы, черви, трояны и шпионское ПО), например учет затрагиваемых интерфейсов (например, USB, интерфейсы программирования ПЛК, JTAG);
- обновление встроенного ПО;
- целостность ПО и информации (несанкционированные изменения);
- подтверждение ввода (правила проверки вводимых данных, выходящие за пределы допусков данные);
- определенное безопасное состояние в результате действий угрозы.

В.5 Конфиденциальность данных

Как правило, часть информации, генерируемая системой управления, в состоянии покоя или в работе носит конфиденциальный или секретный характер. Каналы передачи и хранилища конфиденциальных данных требуют защиты от подслушивания и несанкционированного доступа.

В области низковольтной аппаратуры и НКУ этот аспект может иметь значение, но не рассматривается в данном стандарте.

В.6 Ограничение потока данных

Пользователь оборудования (владелец актива) должен определить необходимые ограничения информационного потока и конфигурацию каналов, используемых для передачи этой информации.

Этот аспект следует учитывать при общей оценке рисков угроз ИБ, и он имеет значение в части низковольтной аппаратуры.

Рекомендуется применение сетевой сегментации для обеспечения времени реагирования системы управления, связанной с безопасностью, или функции, обеспечивающей коммутацию, защиту и управление.

[1)] В Российской Федерации действует ГОСТ Р ИСО/МЭК 15408-1—2012 «Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 1. Введение и общая модель».

В.7 Своевременное реагирование на события

Пользователь оборудования (владелец актива) должен установить политику и меры обеспечения ИБ, а также надлежащие линии связи и контроля, необходимые для реагирования на нарушения ИБ.

Этот аспект следует учитывать при общей оценке рисков угроз ИБ, а не только для низковольтной аппаратуры.

В.8 Доступность информационных ресурсов

Целью является обеспечение доступности низковольтной аппаратуры. Необходимо применять меры, касающиеся подлинности, целостности и защиты от угроз отказа в обслуживании.

Этот аспект следует учитывать при общей оценке рисков угроз ИБ, в том числе в низковольтной аппаратуре и НКУ.

Для обеспечения доступности ресурсов необходимо также учитывать следующие аспекты:

- управление ресурсами (например, сетевая сегментация или схемы приоритетов);
- параметры настройки сети и безопасности.

Доступность — свойство, определяющее возможность за заданное время получить требуемую информационную услугу авторизованному пользователю. С доступностью часто связывают такую характеристику системы, как готовность — способность к выполнению заявленных функций в установленных технических условиях.

Атаки, имеющие цель нарушить степень доступности, получили название атак на отказ в обслуживании (DOS-атаки).

Повышение и обеспечение заданных уровней конфиденциальности, целостности и доступности ресурсов осуществляются путем применения методов ИБ — различных организационно-технических мер обеспечения ИБ.

Приложение Г
(справочное)

Рекомендации для потребителей (пользователей)

Г.1 Общие положения

В настоящем приложении приведены примеры мер обеспечения ИБ в виде рекомендаций, которые изготовитель должен предоставить пользователю в целях создания и поддержания заданных уровней ИБ.

Г.2 Оценка рисков угроз ИБ

Г.2.1 Оценка рисков

Оценка рисков угроз ИБ — это процесс анализа и документирования рисков ИБ в системах распределения электроэнергии и системах управления низковольтной аппаратурой для выявления, определения приоритетов и снижения уровня потенциальных угроз.

На стадии оценки рисков выполняют следующее:

- документирование всех потенциальных угроз;
- расстановку приоритетов таких угроз по степени тяжести, влиянию на деятельность и критериям ИБ;
- порядок распределения ресурсов и проведения работ с угрозами.

В ходе оценки рисков изучаются возможные угрозы из внутренних источников, таких как недовольство сотрудников и подрядчиков, и из внешних источников, таких как хакеры и вандалы. При оценке рисков исследуются потенциальные угрозы для непрерывности работы и оценивается ценность и уязвимость активов, таких как запатентованные технологические разработки и другая интеллектуальная собственность, процессы и финансовые данные.

Результаты этой оценки следует использовать для определения приоритетов инвестиций в ресурсы обеспечения ИБ. Следует рассмотреть процессы, низковольтную аппаратуру и сети с наибольшим риском угроз ИБ и наибольшими последствиями для бизнеса и ИБ, а также определить наилучшую реализацию всесторонней защиты.

Г.2.2 Программа ИБ

Программа ИБ определяет политики, на которых основывается реализация эшелонированной (многоуровневой) защиты, а также меры для выполнения этих политик в зависимости от должности и роли пользователя. Политики и меры обеспечения ИБ определяют:

- роли и должностные обязанности для лиц, которых касаются политики и меры обеспечения ИБ;
- разрешение и запрещение на определенные виды деятельности и процессы;
- последствия несоблюдения требуемых мер;
- политики и методы реагирования на инциденты ИБ. В этих документах определяется последовательность действий, предпринимаемых в случае возникновения атаки или происшествия. Рекомендуется в состав документов включать:
  - план реагирования на инцидент ИБ с указанием порядка выполнения необходимых действий и информирования должностных лиц, ответственных за ИБ, для нейтрализации последствий инцидента ИБ;
  - план восстановления после инцидента ИБ с указанием порядка выполнения необходимых действий в зависимости от роли и должностных обязанностей сотрудников для восстановления низковольтной аппаратуры и процессов до рабочего состояния.

Г.3 Рекомендации по проектированию и установке систем с низковольтной аппаратурой, устанавливаемой в НКУ

Г.3.1 Общий контроль доступа

Основная часть обеспечения ИБ состоит в разработке эффективной политики контроля доступа. Контроль доступа заключается в идентификации групп пользователей или отдельных сотрудников в рамках организации и определении типа доступа, который необходим им для эффективного выполнения своей работы.

Управление паролями — это один из фундаментальных инструментов для защиты низковольтной аппаратуры. Паролями часто пренебрегают в промышленных системах управления. Политики и методы управления паролями зачастую не проработаны или полностью отсутствуют.

Пароли необходимо периодически менять, в том числе после первой установки низковольтной аппаратуры. Надежный пароль включает прописные и строчные буквы, цифры и специальные символы, если они доступны. Для пароля должно быть определено минимальное количество символов.

Рекомендуется применять контрольные вопросы.

Пример — Пароль «Москва» может служить для контрольного вопроса «город, в который Вы первый раз совершили поездку на поезде».

Все пользователи должны знать о рекомендациях по созданию и использованию паролей. В рекомендации следует включать:

- использование индивидуальных паролей для каждого пользователя;
- скрытие символов во время ввода пароля;
- запрет на передачу паролей по электронной почте или другим каналам связи.

Г.3.2 Рекомендации по локальному доступу

Локальный доступ к низковольтной аппаратуре и НКУ предоставляет различные возможности для доступа к информации о системе и управления ею. Необходимо ограничить локальный доступ к низковольтной аппаратуре и НКУ, установив его в закрытом помещении, например, чтобы избежать несанкционированного изменения настроек.

Необходимо создать правила управления доступом к закрытой зоне. В частности, необходимо гарантировать следующее:

- зона постоянно заперта;
- зона оборудована системой аутентификации и авторизации;
- ключ или код доступа должен быть только у авторизованного персонала;
- кабели коммуникационной сети, входящие в помещение, и порты подключения на коммуникационной аппаратуре за пределами помещения защищены;
- все устройства, такие как ПК, смартфоны и планшеты, которые имеют доступ к блоку управления, защищены в соответствии с последними рекомендациями изготовителя.

Для защиты доступа к оборудованию ПК, подключенному локально к его локальному интерфейсу (USB или подобному), рекомендуется:

- обеспечить надежную блокировку ПК, когда они не используются;
- убедиться, что ПК, на которых запущено ПО для настройки, требуют логина и пароля пользователя;
- обеспечить использование надежных паролей;
- убедиться, что пароли пользователей меняются регулярно;
- запретить использование старых паролей;
- установить таймер для блокировки экрана ПК по прошествии определенного времени неактивности;
- повысить защиту ПК в соответствии с последними рекомендациями изготовителей операционной системы, под управлением которой они работают;
- ограничить число пользователей, которым разрешено производить настройки;
- поддерживать список таких пользователей в актуальном состоянии.

Г.3.3 Рекомендации по удаленному доступу

При проектировании и построении промышленной сети управления необходимо применять методы разделения для отделения промышленной сети от сети ИТ. Перечисленные действия обеспечивают защиту от несанкционированного доступа к оборудованию. Дополнительно рекомендуется применение следующих действий:

- использование межсетевых экранов;
- создание демилитаризованных зон, если применимо;
- использование систем обнаружения вторжения (IDS) и/или устройств систем предупреждения вторжений (IPS);
- внедрение политики ИБ и программ обучения;
- определение методов реагирования на инциденты ИБ.

Г.3.4 Рекомендации по обновлениям прошивки

Чтобы снизить уязвимость к атакам, системы должны быть обновлены до последних версий программного обеспечения и прошивки, рекомендованных изготовителем.

При установке обновлений прошивки низковольтной аппаратуры или их компонентов рекомендуется:

- устанавливать обновления в соответствии с принятыми методами эксплуатации (ОТ), такими как испытание в непроизводственной системе для проверки перед их установкой и развертыванием в производственной среде;
- для загрузки и установки обновлений прошивки использовать только надежное ПО поставщика;
- перед загрузкой и установкой обновлений прошивки убедиться, что ПО поставщика использует действующий сертификат цифровой подписи;
- повысить защиту ПК, на котором установлено ПО поставщика, в соответствии с последними рекомендациями поставщика для операционной системы.

С регулярными интервалами времени, но не реже одного раза в три месяца, следует проводить проверку перечня аннулированных сертификатов (CRL), публикуемых поставщиками. Проведение проверки обеспечивает отсутствие скомпрометированных сертификатов в используемом оборудовании.

Библиография

[1] ISO/IEC 27001:2013 — Information technology — Security techniques — Information security management systems — Requirements (Информационные технологии. Методы обеспечения защиты. Системы обеспечения информационной безопасности. Требования)

[2] IEC TR 63201:2019 — Low-voltage switchgear and controlgear — Guidance for the development of embedded software (Аппаратура распределения и управления низковольтная. Руководство по разработке встроенного программного обеспечения)

[3] IEC 62351-9:2017 — Power systems management and associated information exchange — Data and communications security — Part 9: Cyber security key management for power system equipment (Управление энергосистемами и связанный с ним обмен информацией. Безопасность данных и коммуникаций. Часть 9. Управление ключами кибербезопасности для оборудования энергосистем)

[4] IEC 62351-8:2020 — Power systems management and associated information exchange — Data and communications security — Part 8: Role-based access control for power system management (Управление энергосистемами и связанный с ним обмен информацией. Безопасность данных и коммуникаций. Часть 8. Ролевое управление доступом для управления работой энергосистемы)

[5] IEC/TS 62351-5:2013 — Power systems management and associated information exchange — Data and communications security — Part 5: Security for IEC 60870-5 and derivatives (Управление энергосистемами и связанный с ним обмен информацией. Безопасность данных и коммуникаций. Часть 5. Безопасность для МЭК 60870-5 и производных)

[6] IEC 62351-6:2020 — Power systems management and associated information exchange — Data and communications security — Part 6: Security for IEC 61850 (Управление энергетическими системами и связанный с ним обмен информацией. Безопасность данных и коммуникаций. Часть 6. Безопасность для МЭК 61850)

[7] NIST 800-121 — Guide to Bluetooth Security (Руководство по безопасности для Bluetooth)

[8] IEC 62443-2-1:2010 — Industrial communication networks — Network and system security — Part 2-1: Establishing an industrial automation and control system security program (Сети коммуникационные производственные. Безопасность сети и систем. Часть 2-1. Установление программы безопасности производственных систем автоматизации и управления)

[9] IEC 62443-4-1:2018 — Security for industrial automation and control systems — Part 4-1: Secure product development lifecycle requirements [Безопасность систем промышленной автоматизации и контроля. Часть 4-1. Требования к жизненному циклу безопасной разработки (SDL) продуктов]

[10] IEC 62443-4-2:2019 — Security for industrial automation and control systems — Part 4-2: Technical security requirements for IACS components (Безопасность систем промышленной автоматизации и контроля. Часть 4-2. Требования к технической безопасности компонентов IACS)

[11] IEC TS 62351-100-1:2018 — Power systems management and associated information exchange — Data and communications security — Part 100-1: Conformance test cases for IEC TS 62351-5 and IEC TS 60870-5-7 (Управление энергосистемами и связанный с ним обмен информацией. Безопасность данных и коммуникаций. Часть 100-1. Варианты проверки соответствия требованиям IEC TS 62351-5 и IEC TS 60870-5-7)

[12] IEC TS 62351-100-3:2020 — Power systems management and associated information exchange — Data and communications security — Part 100-3: Conformance test cases for the IEC 62351-3, the secure communication extension for profiles including TCP/IP (Управление энергосистемами и связанный с ним обмен информацией. Безопасность данных и коммуникаций. Часть 100-3. Варианты проверки соответствия требованиям IEC 62351-3, расширение защищенной связи для профилей, включая TCP/IP)

[13] ISO/IEC 15408-1:2009 — Information technology — Security techniques — Evaluation criteria for IT security — Part 1: Introduction and general model (Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 1. Введение и общая модель)

УДК 621.317.799:006.354 МКС 29.130.20 NEQ

Ключевые слова: безопасность, аспекты безопасности, аппаратура распределения и управления, низковольтная аппаратура

Редактор *Н.В. Таланова*
Технический редактор *И.Е. Черепкова*
Корректор *Р.А. Ментова*
Компьютерная верстка *М.В. Малеевой*

Сдано в набор 13.12.2024. Подписано в печать 27.12.2024. Формат 60×84⅛. Гарнитура Ариал.
Усл. печ. л. 4,65. Уч.-изд. л. 3,95.

Подготовлено на основе электронной версии, предоставленной разработчиком стандарта

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

Поправка к ГОСТ 35090—2024 Аппаратура распределения и управления низковольтная. Аспекты безопасности

В каком месте	Напечатано	Должно быть		
Предисловие. Таблица согласования	—	Таджикистан	TJ	Таджикстандарт

(ИУС № 3 2026 г.)

gost.e-ecolog.ru