ITUПубликации
Рекомендации

Международный союз электросвязи
Сектор стандартизации

Рекомендация

МСЭ-Т X.1352 (2022) Попр. 1 (03/2024)

СЕРИЯ X: Сети передачи данных, взаимосвязь открытых систем и безопасность

Безопасные приложения и услуги (II) – Безопасность интернета вещей (IoT)

Требования безопасности для устройств и шлюзов интернета вещей

Поправка 1: Добавления и исправления

РЕКОМЕНДАЦИИ МСЭ-Т СЕРИИ X

СЕТИ ПЕРЕДАЧИ ДАННЫХ, ВЗАИМОСВЯЗЬ ОТКРЫТЫХ СИСТЕМ И БЕЗОПАСНОСТЬ

СЕТИ ПЕРЕДАЧИ ДАННЫХ ОБЩЕГО ПОЛЬЗОВАНИЯ	X.1–X.199
ВЗАИМОСВЯЗЬ ОТКРЫТЫХ СИСТЕМ	X.200–X.299
ВЗАИМОДЕЙСТВИЕ МЕЖДУ СЕТЯМИ	X.300–X.399
СИСТЕМЫ ОБРАБОТКИ СООБЩЕНИЙ	X.400–X.499
СПРАВОЧНИК	X.500–X.599
ОРГАНИЗАЦИЯ СЕТИ ВОС И СИСТЕМНЫЕ АСПЕКТЫ	X.600–X.699
УПРАВЛЕНИЕ В ВОС	X.700–X.799
БЕЗОПАСНОСТЬ	X.800–X.849
ПРИЛОЖЕНИЯ ВОС	X.850–X.899
ОТКРЫТАЯ РАСПРЕДЕЛЕННАЯ ОБРАБОТКА	X.900–X.999
БЕЗОПАСНОСТЬ ИНФОРМАЦИИ И СЕТЕЙ	X.1000–X.1099
БЕЗОПАСНЫЕ ПРИЛОЖЕНИЯ И УСЛУГИ (I)	X.1100–X.1199
БЕЗОПАСНОСТЬ КИБЕРПРОСТРАНСТВА	X.1200–X.1299
БЕЗОПАСНЫЕ ПРИЛОЖЕНИЯ И УСЛУГИ (II)	X.1300–X.1499
Связь в чрезвычайных ситуациях	X.1300–X.1309
Безопасность повсеместных сенсорных сетей	X.1310–X.1319
Безопасность умных электросетей	X.1330–X.1339
Сертифицированная электронная почта	X.1340–X.1349
Безопасность интернета вещей (IoT)	**X.1350–X.1369**
Безопасность интеллектуальных транспортных систем (ИТС)	X.1370–X.1399
Безопасность технологии распределенного реестра (DLT)	X.1400–X.1429
Безопасность приложений (2)	X.1450–X.1459
Безопасность веб-среды (2)	X.1470–X.1489
ОБМЕН ИНФОРМАЦИЕЙ, КАСАЮЩЕЙСЯ КИБЕРБЕЗОПАСНОСТИ	X.1500–X.1599
БЕЗОПАСНОСТЬ ОБЛАЧНЫХ ВЫЧИСЛЕНИЙ	X.1600–X.1699
КВАНТОВАЯ СВЯЗЬ	X.1700–X.1729
БЕЗОПАСНОСТЬ ДАННЫХ	X.1750–X.1799
БЕЗОПАСНОСТЬ МЕЖДУНАРОДНОЙ ПОДВИЖНОЙ ЭЛЕКТРОСВЯЗИ (IMT)	X.1800–X.1839
БЕЗОПАСНОСТЬ МЕТАВСЕЛЕННОЙ И ЦИФРОВЫХ ДВОЙНИКОВ	X.2000–X.2199
БЕЗОПАСНОСТЬ ЦЕПОЧКИ ПОСТАВОК ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ	X.2150–X.2199
БЕЗОПАСНОСТЬ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА (ИИ)/МАШИННОГО ОБУЧЕНИЯ (МО)	X.2200–X.2249

Для получения более подробной информации просьба обращаться к перечню Рекомендаций МСЭ-Т.

Рекомендация МСЭ-Т X.1352

Требования безопасности для устройств и шлюзов интернета вещей

Поправка 1

Добавления и исправления

Резюме

В Рекомендации МСЭ-Т X.1352 определены детальные требования по пяти аспектам безопасности, применимым к устройствам и шлюзам интернета вещей (IoT): аутентификация, криптография, безопасность данных, безопасность платформы устройств и физическая безопасность. Эти требования основаны на эталонной модели IoT, которая определена в Рекомендации МСЭ-Т Y.4100, и структуре безопасности IoT, которая определена в Рекомендации МСЭ-Т X.1361.

Аспект аутентификации включает аутентификацию пользователя, безопасное использование учетных данных для аутентификации и аутентификацию устройств. Аспект криптографии включает использование безопасных криптографических алгоритмов, безопасное управление ключами и безопасное генерирование случайных чисел. Аспект безопасности данных охватывает безопасную передачу и хранение данных, управление информационными потоками, безопасное управление сеансами и управление информацией, позволяющей установить личность (PII). Аспект безопасности платформы устройств включает пять элементов: безопасное программное обеспечение, безопасное обновление, управление безопасностью, ведение журналов событий и проставление отметок времени. Аналогично аспект физической безопасности включает безопасный физический интерфейс и защиту от несанкционированного доступа.

Хронологическая справка[*]

Издание	Рекомендация	Утверждено	Исследовательская комиссия	Уникальный идентификатор
1.0	МСЭ-Т X.1352	02.09.2022 г.	17-я	11.1002/1000/14990
1.1	МСЭ-Т X.1352 (2022) Попр. 1	01.03.2024 г.	17-я	11.1002/1000/15665

Ключевые слова

Аутентификация, криптография, безопасность данных, безопасность платформы устройств, безопасность устройств и шлюзов IoT, шлюз IoT, оценка безопасности IoT, физическая безопасность.

[*] Для доступа к Рекомендации наберите в адресном поле вашего веб-навигатора URL https://handle.itu.int/, после которого укажите уникальный идентификатор Рекомендации.

ПРЕДИСЛОВИЕ

Международный союз электросвязи (МСЭ) является специализированным учреждением Организации Объединенных Наций в области электросвязи и информационно-коммуникационных технологий (ИКТ). Сектор стандартизации электросвязи МСЭ (МСЭ-Т) – постоянный орган МСЭ. МСЭ-Т отвечает за изучение технических, эксплуатационных и тарифных вопросов и за выпуск Рекомендаций по ним в целях стандартизации электросвязи на всемирной основе.

На Всемирной ассамблее по стандартизации электросвязи (ВАСЭ), которая проводится каждые четыре года, определяются темы для изучения исследовательскими комиссиями МСЭ-Т, которые, в свою очередь, вырабатывают Рекомендации по этим темам.

Утверждение Рекомендаций МСЭ-Т осуществляется в соответствии с процедурой, изложенной в Резолюции 1 ВАСЭ.

В некоторых областях информационных технологий, которые входят в компетенцию МСЭ-Т, необходимые стандарты разрабатываются на основе сотрудничества с ИСО и МЭК.

ПРИМЕЧАНИЕ

В настоящей Рекомендации термин "администрация" используется для краткости и обозначает как администрацию электросвязи, так и признанную эксплуатационную организацию.

Соблюдение положений данной Рекомендации осуществляется на добровольной основе. Однако данная Рекомендация может содержать некоторые обязательные положения (например, для обеспечения функциональной совместимости или возможности применения), и в таком случае соблюдение Рекомендации достигается при выполнении всех указанных положений. Для выражения требований используются слова "следует", "должен" (shall) или некоторые другие обязывающие выражения, такие как "обязан" (must), а также их отрицательные формы. Употребление таких слов не означает, что от какой-либо стороны требуется соблюдение положений данной Рекомендации.

ПРАВА ИНТЕЛЛЕКТУАЛЬНОЙ СОБСТВЕННОСТИ

МСЭ обращает внимание на вероятность того, что практическое применение или выполнение настоящей Рекомендации может включать использование заявленного права интеллектуальной собственности. МСЭ не занимает какую бы то ни было позицию относительно подтверждения, действительности или применимости заявленных прав интеллектуальной собственности независимо от того, доказываются ли такие права членами МСЭ или другими сторонами, не относящимися к процессу разработки Рекомендации.

На момент утверждения настоящей Рекомендации МСЭ не получил извещения об интеллектуальной собственности, защищенной патентами, которые могут потребоваться для выполнения настоящей Рекомендации. Однако те, кто будет применять Рекомендацию, должны иметь в виду, что вышесказанное может не отражать самую последнюю информацию, и поэтому им настоятельно рекомендуется обращаться к соответствующим базам МСЭ-Т, доступным на веб-сайте МСЭ-Т, по адресу http://www.itu.int/ITU-T/ipr/.

СОДЕРЖАНИЕ

Рекомендация МСЭ-Т X.1352

Требования безопасности для устройств и шлюзов интернета вещей

Поправка 1

Исправления и добавления

Примечание редактора. – Данная публикация содержит полный текст. Изменения, вносимые настоящей Поправкой, показаны в режиме отображения исправлений в тексте Рекомендации МСЭ-Т X.1352 (2022).

1 Сфера применения

В настоящей Рекомендации определены детальные требования по пяти аспектам безопасности, применимым к устройствам и шлюзам интернета вещей (IoT): аутентификация, криптография, безопасность данных, безопасность платформы устройств и физическая безопасность. Эти требования основаны на эталонной модели IoT, которая определена в [ITU-T Y.4100], и структуре безопасности IoT, которая определена в [ITU-T X.1361].

2 Справочные материалы

Указанные ниже Рекомендации МСЭ-Т и другие справочные документы содержат положения, которые путем ссылок на них в данном тексте составляют положения настоящей Рекомендации. На момент публикации указанные издания были действующими. Все Рекомендации и другие справочные документы могут подвергаться пересмотру; поэтому всем пользователям данной Рекомендации предлагается изучить возможность применения последнего издания Рекомендаций и других справочных документов, перечисленных ниже. Перечень действующих на настоящий момент Рекомендаций МСЭ-Т регулярно публикуется. Ссылка на документ, приведенный в настоящей Рекомендации, не придает ему как отдельному документу статус Рекомендации.

[ITU-T X.1361] Рекомендация МСЭ-Т X.1361 (2018 г.), *Структура безопасности интернета вещей на основе модели с использованием шлюза*.

[ITU-T Y.4100] Рекомендация МСЭ-Т Y.4100/Y.2066 (2014 г.), *Общие требования к интернету вещей*.

3 Определения

3.1 Термины, определенные в других документах

В настоящей Рекомендации используются следующие термины, определенные в других документах.

3.1.1 аутентификация (**authentication)** [ITU-T X.1254]: Обеспечение гарантии заявленной идентичности объекта.

3.1.2 функциональные возможности (capability) [b-ISO 16100-1]: Набор функций и услуг с набором критериев для оценки рабочих характеристик источника функциональных возможностей.

3.1.3 конфиденциальность (confidentiality) [b-ITU-T X.800]: Свойство, защищающее информацию от доступа к ней или ее раскрытия неуполномоченными лицами, устройствами или процессами.

3.1.4 полномочия (credential) [b-ITU-T X.1252]: Набор данных, представляемых как доказательство утверждаемой идентичности и/или прав.

3.1.5 случайное число криптографического качества (cryptographic-quality random number) [b-ITU-T X.667]: Случайное или псевдослучайное число, генерированное механизмом, обеспечивающим достаточный разброс многократно генерируемых значений, которое должно быть приемлемо для использования в криптографической работе (и используется в такой работе).

3.1.6 криптография (cryptography) [b-ITU-T X.800]: Дисциплина, включающая принципы, средства и методы для преобразования данных, необходимого для того, чтобы скрыть содержащуюся в них информацию, предотвратить их скрытое изменение и/или предотвратить их несанкционированное использование.

3.1.7 целостность данных (data integrity) [b-ITU-T X.800]: Показатель того, что данные не были изменены или разрушены несанкционированным способом.

3.1.8 устройство (device) [b-ITU-T Y.4000]: Применительно к интернету вещей означает элемент оборудования, который обладает обязательными возможностями связи и дополнительными возможностями измерения, срабатывания, а также ввода, хранения и обработки данных.

3.1.9 управление ключами (key management) [b-ITU-T X.800]: Генерирование, хранение, распределение, удаление, архивирование и применение ключей в соответствии со стратегией безопасности.

3.1.10 управление внесением исправлений (patch management) [ITU-T X.1361]: Процесс, включающий в себя получение, тестирование и установку множества исправлений в информационные системы.

ПРИМЕЧАНИЕ. – Можно рассмотреть возможность управления уязвимостями.

3.1.11 информация, позволяющая установить личность (personally identifiable information (PII)) [b-ISO/IEC 29100]: Любая информация, которая: a) может быть использована для идентификации субъекта PII, к которому относится такая информация; или b) прямо или косвенно связана с субъектом PII.

3.1.12 физическая безопасность (physical security) [b-ITU-T X.800]: Меры, принимаемые для обеспечения физической защиты ресурсов от умышленных и непреднамеренных угроз.

3.1.13 настройка безопасной конфигурации (secure configuration) [ITU-T X.1361]: Процесс настройки сетевых устройств, позволяющий снизить уровень присущих этим устройствам уязвимостей и обеспечить предоставление только тех услуг, которые необходимы для выполнения ими своей роли.

3.1.14 шлюз безопасности (security gateway) [ITU-T X.1361]: Точка соединения между сетями, или подгруппами внутри сетей, или программными приложениями различных доменов безопасности, которая предназначена для защиты сети в среде интернета вещей в соответствии с заданной политикой безопасности.

ПРИМЕЧАНИЕ. – Этот термин иногда заменяют термином "шлюз". Определение взято из [b-ISO/IEC 27033-1].

3.1.15 угроза (threat) [b-ISO/IEC 27000]: Потенциальная причина нежелательного инцидента, который может нанести ущерб системе или организации.

3.1.16 уязвимость (vulnerability) [b-ISO/IEC 27000]: Слабое место актива или мер контроля, которое может быть использовано одной или несколькими угрозами.

3.1.17 управление уязвимостями (vulnerability management) [ITU-T X.1361]: Процесс, включающий выявление, классификацию, устранение и смягчение последствий уязвимостей.

3.2 Термины, определенные в настоящей Рекомендации

В настоящей Рекомендации определены следующие термины.

3.2.1 атака методом полного перебора (brute-force attack): Попытки методом проб и ошибок скомпрометировать механизм аутентификации путем перебора возможных значений паролей или ключей.

3.2.~~1~~2 фактор безопасности (security dimension): Совокупность мер безопасности, разработанных для обеспечения определенного аспекта безопасности сетей.

3.2.~~2~~3 безопасность платформы устройств (device platform security): Набор мер обеспечения безопасности для микропрограммного обеспечения и его функциональных возможностей по обновлению стороннего программного обеспечения и управлению им для устройств и шлюзов интернета вещей наряду с функциональными возможностями по их проверке.

ПРИМЕЧАНИЕ. – В зависимости от функциональных возможностей аппаратного обеспечения микропрограммное обеспечение может заменяться программным обеспечением поверх операционной системы.

3.2.34 обфускация (obfuscation): Результат операции, выполняемой над программным кодом или данными прикладной программы, которая приводит к тому, что приложения прячутся или скрываются тем или иным образом, не нанося ущерба выводу кода.

4 Сокращения и акронимы

В настоящей Рекомендации используются следующие сокращения и акронимы.

API	Application Programming Interface		Интерфейс прикладного программирования
CAPTCHA	Completely Automated Public Turing test to tell Computers and Humans Apart		Полностью автоматизированный открытый тест Тьюринга, позволяющий отличить действия человека от операций компьютера
CoAP	Constrained Application Protocol		Протокол ограниченного применения
DDoS	Distributed Denial of Service		Распределенный отказ в обслуживании
DoS	Denial of Service		Отказ в обслуживании
F/W	Firmware		Микропрограммное обеспечение
FTP	File Transfer Protocol		Протокол передачи файлов
H/W	Hardware		Оборудование
ID	Identifier		Идентификатор
IDS	Intrusion Detection System		Система обнаружения вторжений
IMEI	International Mobile Equipment Identity		Международный идентификатор оборудования подвижной связи
IoT	Internet of Things		Интернет вещей
IPS	Intrusion Prevention System		Система предотвращения вторжений
LwM2M	Lightweight Machine to Machine		Облегченное межмашинное взаимодействие
MAC	Media Access Control		Управление доступом к среде передачи
MCU	Microcontroller Unit		Блок микроконтроллера
MQTT	Message Queuing Telemetry Transport		Протокол передачи телеметрических данных посредством очереди сообщений
OS	Operating System	ОС	Операционная система
PII	Personally Identifiable Information		Информация, позволяющая установить личность
PIN	Personal Identification Number		Персональный идентификационный номер
S/W	Software	ПО	Программное обеспечение
SD	Secure Digital		Защищенный цифровой носитель
SHA	Secure Hash Algorithm		Алгоритм безопасного хеширования
SNMP	Simple Network Management Protocol		Простой протокол управления сетью
SSA	Shoulder-Surfing Attack		Атака типа подсматривание через плечо
SSH	Secure Shell		Защищенный командный процессор

SWD	Serial Wire Debug	Проверка последовательного интерфейса
TLS	Transport Layer Security	Безопасность транспортного уровня
UART	Universal Asynchronous Receiver/Transmitter	Универсальный асинхронный приемопередатчик
UID	Unique Identifier	Уникальный идентификатор
UPnP	Universal Plug and Play	Универсальная автоматическая настройка устройств
USB	Universal Serial Bus	Универсальная последовательная шина

5 Соглашения

В настоящей Рекомендации используются следующие соглашения.

Вспомогательный глагол "следует" (should) означает требование, которое рекомендуется, но не является абсолютно необходимым.

Вспомогательный глагол "должен" или "требуется" (shall) означает требование, которому необходимо неукоснительно следовать и отклонение от которого не допускается, если будет сделано заявление о соответствии настоящей Рекомендации.

Вспомогательный глагол "может" (can), который иногда встречается в тексте настоящей Рекомендации, обозначает наличие возможности.

Использование слова "следует" в Дополнении I не носит нормативного характера.

6 Обзор

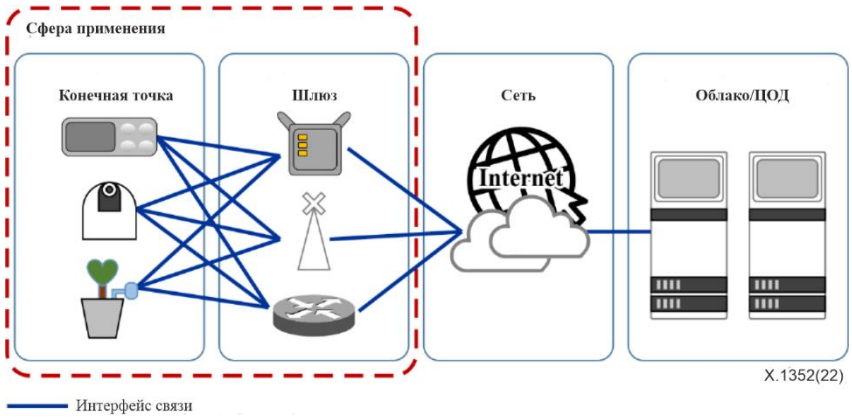

Рисунок 1 – Сфера применения требований безопасности

На основе средств безопасности, предлагаемых в [ITU-T X.1361] и [ITU-T Y.4100], и как описано в Дополнении II, требования безопасности для устранения проблем и угроз в устройствах и шлюзах IoT (за исключением сетевых систем и платформ) определены по пяти аспектам безопасности, а именно: аутентификация, криптография, безопасность данных, безопасность платформы устройств и физическая безопасность.

Аспект аутентификации включает аутентификацию пользователя, безопасное применение учетных данных для аутентификации и аутентификацию устройств.

Аспект криптографии включает использование безопасных криптографических алгоритмов, безопасное управление ключами и безопасное генерирование случайных чисел.

Аспект безопасности данных включает безопасную передачу и безопасное хранение данных, управление информационными потоками, безопасное управление сеансом и защиту PII.

Аспект безопасности платформы устройств включает в себя пять элементов: безопасное программное обеспечение (ПО), безопасное обновление, управление безопасностью, ведение журналов событий и проставление отметок времени.

Аналогично к аспекту физической безопасности относятся безопасный физический интерфейс и защита от несанкционированного доступа.

На рисунке 2 показаны целевые показатели аспектов безопасности устройства и шлюза IoT. Устройство и шлюз IoT обычно состоят из блока микроконтроллера (MCU), модуля связи, оперативного запоминающего устройства (ОЗУ) и портов ввода/вывода. Элементы защиты могут быть элементами аппаратного или программного обеспечения. В MCU входят микропрограммное обеспечение, физические интерфейсы и ОЗУ. В данном случае ПО с операционной системой (ОС) может быть заменено микропрограммным обеспечением. Модуль связи требует применения шифрования для защиты данных при передаче. Флеш-ОЗУ обеспечивает надежное хранение данных аутентификации и криптографии, а также конфиденциальность/целостность данных. Для доступа через физические интерфейсы, такие как универсальный асинхронный приемопередатчик (UART), также требуется аутентификация пользователя. Неиспользуемые аппаратные интерфейсы должны быть удалены или отключены.

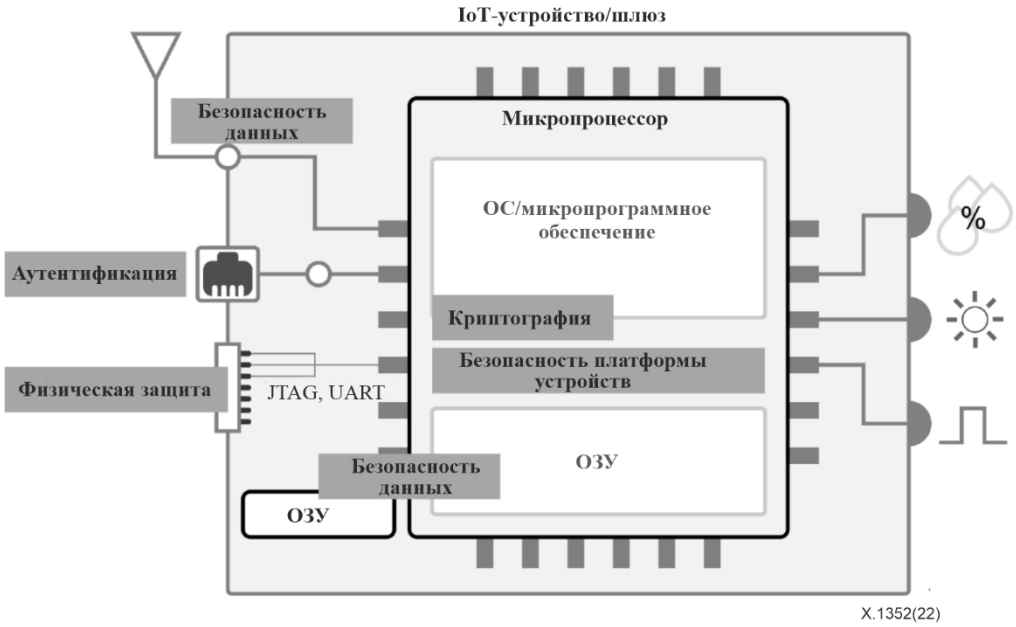

Рисунок 2 – Пример применения средств безопасности в устройствах и шлюзах IoT

7 Угрозы/уязвимости безопасности устройств и шлюзов IoT

Угрозы/уязвимости безопасности устройств и шлюзов IoT, которые могут сделать их возможными целями кибератак, описаны в пунктах 7.1 и 7.2. Угрозы безопасности шлюзов включают угрозы для устройств IoT.

7.1 Угрозы/уязвимости безопасности для устройств IoT

Устройства могут подвергаться следующим угрозам/уязвимостям.

– ST-D-1 – обход процедуры аутентификации. Неавторизованный пользователь получает доступ к устройству, а также может получить доступ к важным данным, включая пользовательские данные и файлы конфигурации, хранящиеся в устройстве.

– ST-D-2 – несанкционированное подключение устройства. Устройство подвергается воздействию любого неавторизованного устройства или же его данные, такие как пользовательские данные, могут быть переданы на любое неавторизованное устройство.

– ST-D-3 – превышение прав. Предоставление чрезмерных или излишних прав позволяет злоумышленнику получить доступ ко всем допустимым операциям и контролируемым данным, включая пользовательские данные устройства.

– ST-D-4 – неограниченные повторные попытки аутентификации. Неавторизованный пользователь, повторяющий попытки аутентификации, может получить доступ к подлинной учетной записи пользователя.

– ST-D-5 – ошибка из-за одновременного доступа. Одновременный доступ с нескольких учетных записей администратора может привести к несогласованным изменениям в конфигурации критически важных функций.

– ST-D-6 – раскрытие и угадывание аутентификационной информации. Когда аутентификационная информация, такая как пароль, ненадежна, жестко запрограммирована или хранится в виде обычного текста или когда пароль аутентификации или персональный идентификационный номер (PIN-код) отображаются в виде открытого текста, (так называемое подсматривание через плечо (SSA)), или когда аутентификационная информация скомпрометирована каким-либо иным способом (например, при помощи социальной инженерии), или сгенерирована при помощи метода с недостаточной случайностью, злоумышленник может увидеть аутентификационную информацию ~~(так называемое подсматривание через плечо (SSA))~~ или угадать ее.

– ST-D-7 – слабый пароль. Злоумышленник может определить незащищенную комбинацию, например пароль по умолчанию или слабый пароль, что может позволить ему выдать себя за легального пользователя.

– ST-D-8 – слабый ключ шифрования/случайное число. Недостаточно длинный криптографический ключ или предсказуемое случайное число могут оказаться неспособными защитить важные данные.

– ST-D-9 – слабый криптографический алгоритм. Проанализировав трафик, в котором используется слабый криптографический алгоритм, злоумышленник может предсказать данные ключей или распознать текст зашифрованного сообщения (шифротекст).

– ST-D-10 – отсутствие проверки вводимых значений. Отсутствие проверки вводимых значений может привести к неисправности устройства.

– ST-D-11 – раскрытие данных и манипулирование данными. Злоумышленник может раскрыть, использовать или изменить важнейшие данные, такие как пользовательские данные, конфигурация устройства и криптографические ключи, которые передаются через устройство или хранятся в нем.

– ST-D-12 – перехват сеанса пользователя. Злоумышленник может получить несанкционированный доступ к подлинной учетной записи пользователя, чей сеанс был закрыт неправильно, или использовать действующие сеансы нескольких устройств, в которых используется один и тот же криптографический ключ.

– ST-D-13 – небезопасное обновление. Предполагаемый файл обновления не может быть загружен или загружен файл обновления из неавторизованного/неаутентифицированного источника.

– ST-D-14 – ошибка обновления. Ошибка, возникшая во время обновления, может привести к неправильной работе устройства.

– ST-D-15 – ошибка целостности. Непредусмотренное изменение исполняемых кодов или параметров конфигурации может привести к неисправности устройства.

– ST-D-16 – вредоносное ПО. Код, который обладает непредусмотренными функциями, может быть использован в злонамеренных целях.

– ST-D-17 – использование оставшейся в памяти информации. Криптографический ключ, пароль и конфиденциальные данные, используемые для операций шифрования, аутентификации и передачи данных, остаются в памяти и могут использоваться злоумышленниками.

– ST-D-18 – непредусмотренное изменение критически важных конфигураций. Отсутствие средств управления защитой устройства может привести к непредусмотренным изменениям критически важных конфигураций и небезопасному предоставлению услуг.

– ST-D-19 – реакция на небезопасную ошибку. Отсутствие надлежащей системы обнаружения и реагирования на ошибки и вредоносное поведение устройства могут привести к небезопасному предоставлению услуг.

– ST-D-20 – небезопасная разработка. Потенциальные уязвимости в системе безопасности могут возникать в процессе разработки и реализации устройства, а оценка и реагирование на них в процессе тестирования могут отсутствовать или быть неподходящими.

– ST-D-21 – уязвимая ОС. В уязвимой среде ОС злоумышленники могут взломать или обойти функции устройства.

– ST-D-22 – уязвимые модули или библиотеки сторонних производителей. Злоумышленник может вызывать такие модули или библиотеки для своих целей.

– ST-D-23 – незащищенная конфиденциальная информация в системном журнале. Злоумышленник может раскрыть и использовать конфиденциальную информацию из системного журнала.

– ST-D-24 – выявление критически важной информации в процессе исправления ошибок. Злоумышленник может раскрыть и использовать критически важную информацию в процессе создания журнала регистрации событий и исправления ошибок при выпуске и распространении устройства.

– ST-D-25 – несанкционированный физический доступ. Устройство подвергается несанкционированному физическому доступу и внесению непредусмотренных изменений в его конфигурацию.

– ST-D-26 – незащищенные соединения с сетями. IoT-устройства, подключенные к незащищенным сетям, могут быть уязвимы для атак, особенно если в сети отсутствуют надлежащие меры шифрования и аутентификации.

7.2 Угрозы/уязвимости безопасности для шлюзов IoT

Шлюзы могут подвергаться следующим угрозам/уязвимостям.

– ST-G-1 – ненадежная передача данных. Ненадежная передача данных может привести к сбоям в работе устройства или распространению вредоносного кода.

– ST-G-2 – атака, вызывающая отказ в обслуживании (DoS), или распределенная DoS-атака. DoS-атака может привести к потере работоспособности устройства.

– ST-G-3 – несанкционированный доступ к подключенным устройствам. В случаях, когда шлюз имеет какие-либо возможности контроля над подключенными устройствами, несанкционированный доступ к шлюзу может привести к нарушению безопасности всех подключенных устройств.

– ST-G-4 – слабое шифрование. Отсутствие шифрования данных, передаваемых между шлюзами IoT, что приводит к потенциальному подслушиванию или перехвату данных.

– ST-G-5 – физическое вмешательство. Незапертые помещения или слабые меры физической защиты могут позволить злоумышленникам вмешаться в работу оборудования шлюза, что может привести к получению конфиденциальных данных или манипулированию функциональностью шлюза.

8 Требования безопасности

В настоящей Рекомендации представлены требования безопасности для устройств и шлюзов IoT на основе пяти аспектов безопасности, определенных в разделе 6, и сформирован набор требований безопасности, основанных на положениях модели угроз и конкретных функциональных свойствах IoT. Возможности обеспечения безопасности основаны на [ITU-T X.1361], как описано в Дополнении II.

8.1 Аутентификация

Аспект аутентификации охватывает аутентификацию пользователя, безопасное использование учетных данных для аутентификации и аутентификацию устройств.

8.1.1 Аутентификация пользователя

Должна быть предусмотрена функция смены Ззаводскойго пароль я по умолчанию ~~должен быть изменен~~ (AU-1-1).

– ~~Пароль должен устанавливаться в процессе первоначальной аутентификации или когда требуется изменение пароля после первоначальной аутентификации~~Устройство должно обеспечивать функцию, например, веб-интерфейс, с тем чтобы пользователи могли изменить пароль аутентификации после первоначальной аутентификации или каждый раз, когда требуется изменение.

– Если на устройстве включено дистанционное управление, пароль по умолчанию для учетной записи управления должен быть изменен до соединения с сетью.

– ~~Пароль должен отличаться от первоначального или предыдущего пароля.~~Функция должна обеспечить выполнение правила, согласно которому новый пароль должен отличаться от начального и предыдущих шести значений.

При доступе к функциям управления безопасностью или конфиденциальным данным пользователь должен предварительно пройти идентификацию и аутентификацию (AU-1-2).

– При доступе к функциям управления безопасностью, например к функциям настройки устройства IoT, учетной записи пользователя или прав доступа, пользователь должен пройти идентификацию и аутентификацию.

– Право доступа к функциям управления безопасностью или конфиденциальным данным для пользователей с привилегиями должно осуществляться отдельно от управления правами доступа обычных пользователей.

– Для предотвращения несанкционированного доступа к восстановлению учетной записи следует реализовать безопасный механизм восстановления пароля, включающий процедуру аутентификации.

– В дополнение к паролям для повышения уровня безопасности следует добавить многофакторную аутентификацию. Для аутентификации пользователей может использоваться комбинация таких факторов, как пароли, биометрические данные, смарт-карты или одноразовые пароли.

Количество попыток аутентификации должно быть ограничено (AU-1-3).

– Если разрешены повторные попытки аутентификации, устройство IoT может быть уязвимо для атак методом прямого подбора. Таким образом в устройстве должна быть предусмотрена функция надлежащего реагирования на повторяющиеся попытки аутентификации.

– Эта функция может быть реализована одним из следующих способов:

  a) ограничение количества попыток аутентификации путем блокировки учетной записи или отключения функции аутентификации на определенный период времени (рекомендуется ограничить количество попыток аутентификации пятью или менее попытками и отключать функции аутентификации не менее чем на 5 минут);

  b) превышение указанного количества попыток аутентификации расценивается как несанкционированный сетевой трафик, и пользователь вносится в список автоблокировки (рекомендуется ограничить количество попыток аутентификации 10 или менее попытками);

  c) применение полностью автоматизированного открытого теста Тьюринга, позволяющего отличить действия человека от операций компьютера (CAPTCHA).

Предустановленный или заводской пароль устройства должен быть уникальным, сгенерированным случайным образом и достаточно надежным (AU-1-4).

Следует предусмотреть функцию управления учетными записями и правами доступа пользователей (AU-1-5).

– Следует предусмотреть возможность управления всеми учетными записями пользователей (включая учетную запись администратора), используемыми на устройстве IoT, например для их добавления и удаления, а также для назначения прав доступа.

– Если используется модель управления доступом на основе ролей, следует четко определить права доступа ко всем функциям устройства IoT и назначить эти права соответствующим образом.

Ко всем учетным записям пользователей следует применять принцип наименьшей привилегии (AU-1-6).

– Всем учетным записям пользователей следует назначить права доступа в соответствии с привилегиями на основе ролей.

Одновременный доступ к учетной записи администратора следует ограничить (AU-1-7).

– Следует ограничить возможность одновременного доступа к услугам управления одной учетной записью администратора и предусмотреть функцию прерывания предыдущего сеанса доступа или ограничения новых попыток доступа.

Пароль должен быть безопасным с точки зрения длины, повторяемости и сложности (AU-1-8).

– В устройствах IoT следует предусмотреть функцию назначения пользователем безопасного пароля с точки зрения длины, повторяемости и сложности.

Если аутентификация пользователя производится через SSH, то при аутентификации следует обеспечить использование ключей SSH. Аутентификацию с помощью пароля следует отключить (AU-1-9).

8.1.2 Безопасное использование учетных данных

Не следует использовать жестко запрограммированные учетные данные (AU-2-1).

– Не следует делать пароль (PIN-код, секретный ключ и т. д.) жестко запрограммированным и хранить его в виде открытого текста.

При выполнении аутентификации по паролю пароль следует маскировать (AU-2-2).

– Если пароль отображается в виде открытого текста, он может быть уязвим для SSA. Таким образом, чтобы предотвратить такое отображение при вводе пароля, составляющие пароль символы следует замаскировать, например, звездочками ("*").

Не следует предоставлять никаких конкретных сообщений о сбое сеанса аутентификации (AU-2-3).

8.1.3 Аутентификация устройства

Уникальный идентификатор (UID) каждого аппаратного устройства должен быть сохранен (AU-3-1). См. таблицу 1.

– Устройство IoT должно иметь уникальный и фиксированный идентификатор (ID).

Таблица 1 – UID устройств IoT

Идентификатор	Описание
Адрес управления доступом к среде (MAC)	Уникальный идентификатор, присвоенный сетевому интерфейсу для связи на канальном уровне сегмента сети (48 битов)
Международный идентификатор оборудования подвижной связи (IMEI), международный идентификационный номер терминала подвижной связи	Уникальный номер для смартфонов Назначается производителем при выпуске сотового телефона Состоит из 15 цифр: сертификационный код (восемь цифр); серийный номер модели (шесть цифр); и проверочное число (одна цифра)

Перед передачей конфиденциальных данных или соединением в целях управления следует выполнять процесс взаимной аутентификации устройств (AU-3-2).

– Примеры взаимной аутентификации:

a) использование секретного ключа на основе метода шифрования с открытым ключом;

b) использование атрибутов безопасности (UID, ключ и т. д.) и микрочипов безопасности;

c) применение протокола безопасности транспортного уровня (TLS) (или дейтаграммы TLS) к облегченному протоколу связи, то есть протоколу ограниченного применения (CoAP), протоколу облегченного межмашинного взаимодействия (LwM2M) или протоколу передачи телеметрических данных посредством очереди сообщений (MQTT).

8.2 Криптография

– Если использование общих криптографических алгоритмов затруднено из-за ограниченной емкости ОЗУ и ПЗУ, необходимо использовать облегченные криптографические алгоритмы.

– Следует использовать криптографические алгоритмы для противодействия атакам по побочным каналам.

Необходимо осуществлять надежное управление криптографическими ключами на протяжении всего их жизненного цикла (CR-1-2).

– Генерирование, обновление, распространение, использование, хранение и уничтожение ключей следует осуществлять безопасным образом.

– Для проверки целостности и хэширования следует использовать безопасные хэш-функции (например, SHA-256).

Генерирование случайных чисел следует осуществлять с помощью алгоритма с установленной степенью случайности (CR-1-3).

8.3 Безопасность данных

К аспекту безопасности данных относятся безопасная передача и безопасное хранение данных, управление информационными потоками, безопасное управление сеансом и защита PII.

8.3.1 Безопасная передача и безопасное хранение данных

Передаваемые данные должны быть зашифрованы (DS-1-1).

– Передаваемые данные должны быть зашифрованы с использованием безопасного криптографического алгоритма (см. CR-1-1).

При создании канала передачи данных или управления следует применять безопасный режим (DS-1-2).

– При передаче данных следует использовать протокол безопасности, обеспечивающий конфиденциальность и целостность передаваемых данных, а также аутентификацию сторон источника и назначения.

– По возможности следует проводить анонимизацию данных, с тем чтобы снизить риск, связанный с их раскрытием.

Данные, хранящиеся в устройствах, должны быть зашифрованы (DS-1-3).

– Содержимое устройств хранения данных должно быть зашифровано с использованием безопасного криптографического алгоритма (см. CR-1-1).

Удаленные данные не должны восстанавливаться (DS-1-4).

– При необходимости утилизации, обновления или замены устройств должна быть предусмотрена возможность удаления (например, инициализация заводских параметров настройки), так чтобы данные не могли быть восстановлены.

8.3.2 Управление информационным потоком

Не следует допускать несанкционированный сетевой трафик (DS-2-1).

Мониторинг доступа к данным и моделей потоков может помочь обнаружить аномалии и потенциальные инциденты в области безопасности, что обеспечит возможность своевременного вмешательства и реагирования. (DS-2-2).

Реагирование на атаки DoS или атаки распределенного отказа в обслуживании (DDoS) с помощью шлюза IoT (DS-2-3).

8.3.3 Безопасное управление сеансом связи

По истечении заданного времени бездействия сеанс связи следует завершить (DS-3-1).

– При повторном обращении после завершения сеанса следует проводить повторную аутентификацию.

Значение идентификатора сеанса должно быть непредсказуемым (DS-3-2).

– Для генерации идентификатора сеанса следует применять безопасный алгоритм на основе случайных чисел.

– Во время аутентификации при каждом сеансе следует изменять идентификатор сеанса, а использованные идентификаторы сеанса – уничтожать.

Реализация механизма прерывания сеанса должна аннулировать сеансы в режиме реального времени при обнаружении подозрительной активности или при отправке пользователем запроса на выход из системы (DS-3-3).

– Обеспечивает возможность незамедлительного реагирования на инциденты в области безопасности или завершение сеанса по инициативе пользователя, что совершенствует контроль над сверхактивными сеансами.

8.3.4 Управление данными PII

В течение жизненного цикла ключа следует осуществлять надежное управление данными PII (DS-4-1).

– Сбор, использование, хранение и уничтожение данных PII следует осуществлять безопасным способом.

8.4 Безопасность платформы устройств

В аспект безопасности платформы устройств включено пять элементов: безопасное ПО, безопасное обновление, управление безопасностью, ведение журналов событий и проставление отметок времени.

8.4.1 Безопасное программное обеспечение

Следует применять безопасные методы кодирования (PL-1-1).

– Программное обеспечение следует разрабатывать и реализовывать с учетом требований безопасности.

– Можно проводить регулярные аудиты безопасности и обзоры кода для выявления и устранения уязвимостей в ПО.

Известные уязвимости программного обеспечения должны быть обнаружены и удалены (PL-1-2).

– Если ПО разработано с использованием протоколов, библиотек, интерфейсов прикладного программирования (API), пакетов или источников с открытым кодом, содержащих известные уязвимости, эти уязвимости также могут содержаться в ПО и в ОС.

– Для проверки уязвимостей устройства и их удаления необходимо использовать общедоступные сведения об известных уязвимостях (например, [b-CVE]).

Следует применять обфускацию (PL-1-3).

– Эти требования могут применяться главным образом к разрабатываемым приложениям, облегчающим восстановление исходного кода.

– Поскольку для извлечения важной информации о логике или ключах могут быть использованы известные средства обратного инжиниринга, необходимо обеспечить соответствующий уровень защиты.

Следует обеспечить функцию проверки целостности параметров конфигурации и исполняемых кодов (PL-1-4).

– Чтобы гарантировать работоспособность устройств IoT, следует периодически в автоматическом режиме или вручную проверять целостность параметров конфигурации и исполняемых кодов во время загрузки.

В случае ошибки нарушения целостности принимаются соответствующие меры.

8.4.2 Безопасное обновление

Обновление должно производиться авторизованными пользователями (PL-2-1).

В случае сбоя процесса обновления следует задействовать функцию отката (PL-2-2).

Перед обновлением следует выполнить проверку целостности и аутентификации (PL-2-3).

– В отношении выполняющего обновление пользователя следует проводить аутентификацию, проверку целостности следует производить в отношении адреса сервера обновлений, в отношении файла обновления следует проводить проверку как аутентификации, так и целостности.

– Подлинность пользователя может быть подтверждена повторной аутентификацией пользователя непосредственно перед процедурой обновления.

– Авторизованный пользователь может проверить целостность адреса сервера обновлений путем визуального контроля.

– Проверка целостности и подлинности файлов обновлений может быть выполнена путем верификации криптографической цифровой подписи.

8.4.3 Управление безопасностью

Необязательные услуги следует отключить (PL-3-1).

– Следует отключить необязательные услуги (Telnet, протокол передачи файлов (FTP), протокол универсальной автоматической настройки устройств (UPnP), простой протокол управления сетью (SNMP) и т. д.) и указать необходимые услуги, предоставляемые устройством.

– Когда такие услуги необходимы, должна использоваться их безопасная альтернатива, например, SSH вместо Telnet, SFTP вместо FTP, SNMPv3 вместо SNMP.

Функции дистанционного управления следует выполнять в надежной среде (PL-3-2).

Следует применять безопасную стороннюю библиотеку (PL-3-3).

– Для разработки следует использовать последние версии сторонней библиотеки и модулей без каких бы то ни было известных уязвимостей или дефектов безопасности.

Следует предусмотреть самопроверку (PL-3-4).

– Для обнаружения ошибок основного аппаратного и программного обеспечения следует предусмотреть функцию самопроверки при запуске (включении питания) устройства IoT или после его запуска.

8.4.4 Регистрация событий

Следует производить регистрацию событий, связанных с безопасностью (PL-4-1).

– Следует выполнять регистрацию событий и предусмотреть возможность обнаружения и отслеживания ~~любого~~любых попыток доступа к журналу, успешных и неуспешных аутентификаций, изменений в правах пользователей и аномального поведения устройства.

Следует обеспечить механизм безопасной регистрации событий (PL-4-2).

– Следует предусмотреть механизм защиты журнала событий для предотвращения его потери и несанкционированного изменения (в том числе удаления).

– Следует надежно хранить журналы и защищать их от несанкционированного доступа, несанкционированного вмешательства и удаления.

8.4.5 Отметки времени

Следует обеспечить надежное проставление отметок времени (PL-5-1).

8.5 Физическая безопасность

Аспект физической безопасности включает безопасность физических интерфейсов и защиту устройств IoT от несанкционированного вмешательства.

8.5.1 Безопасный физический интерфейс

Следует отключить все излишние внешние интерфейсы (PH-1-1).

– Следует указать параметры и функции всех внешних интерфейсов (локальной сети, универсальной последовательной шины (USB), порта защищенных цифровых (SD) карт и т. д.), доступных снаружи.

– При необходимости следует осуществлять контроль для предотвращения несанкционированного доступа.

Должен предотвращаться несанкционированный доступ к внутреннему интерфейсу (PH-1-2).

– Должны быть указаны параметры и функции всех внутренних интерфейсов Объединенной группы по вопросам тестирования (JTAG), проверки пользовательского интерфейса (SWD), UART и т. д.), доступных снаружи.

– При необходимости должен производиться контроль для предотвращения несанкционированного доступа.

Следует обеспечить контроль среды (PH-1-3).

– Следует обеспечить защиту устройств от воздействия внешних факторов, таких как температура, влажность и пыль.

8.5.2 Защита от несанкционированного вмешательства

Следует обеспечить функцию обнаружения несанкционированного физического вмешательства и реагирования на него (пломбы, замки, защитная сигнализация, обнуляющие датчики, сигналы тревоги и т. п.) (PH-2-1).

Приложение A

Связь между требованиями безопасности интернета вещей и угрозами/уязвимостями безопасности

(Данное Приложение является неотъемлемой частью настоящей Рекомендации.)

Требования безопасности IoT перечислены и описаны в разделе 8, а угрозы/уязвимости безопасности – в разделе 7. В таблице A.1 показана связь между требованиями безопасности IoT и угрозами/уязвимостями безопасности.

Таблица A.1 – Связь между требованиями безопасности IoT и угрозами/уязвимостями безопасности

Номер требования	Аспект требования	Описание требования	Угрозы/уязвимости безопасности
AU-1-1	Аутентификация	Должна быть обеспечена функция смены ~~З~~заводско~~й~~го парол~~ь~~я по умолчанию ~~должен быть изменен~~	ST-D-6
AU-1-2	Аутентификация	При доступе к функциям управления безопасностью или конфиденциальным данным пользователь должен предварительно пройти идентификацию и аутентификацию	ST-D-1
AU-1-3	Аутентификация	Количество попыток аутентификации должно быть ограничено	ST-D-4 ST-D-5
AU-1-4	Аутентификация	Предустановленный пароль устройства должен быть уникальным, сгенерированным случайным образом и надежным	ST-D-1
AU-1-5	Аутентификация	Следует предусмотреть функцию управления учетными записями и правами доступа пользователей	ST-D-3
AU-1-6	Аутентификация	Ко всем учетным записям пользователей следует применять принцип наименьшей привилегии	ST-D-3
AU-1-7	Аутентификация	Одновременный доступ к учетной записи администратора следует ограничить	ST-D-1
AU-1-8	Аутентификация	Пароль следует сделать безопасным с точки зрения длины, повторяемости и сложности	ST-D-7
AU-1-9	Аутентификация	Если поддерживается SSH, при аутентификации следует обеспечить использование ключей SSH	ST-D-4 ST-D-6 ST-D-7
AU-2-1	Аутентификация	Не следует использовать жестко запрограммированные учетные данные	ST-D-6
AU-2-2	Аутентификация	При выполнении аутентификации по паролю пароль следует маскировать	ST-D-6
AU-2-3	Аутентификация	Не следует предоставлять никаких конкретных сообщений о сбое сеанса аутентификации	ST-D-6
AU-3-1	Аутентификация	Следует сохранять уникальный идентификатор каждого аппаратного устройства	ST-D-2

Таблица A.1 – Связь между требованиями безопасности IoT и угрозами/уязвимостями безопасности

Номер требования	Аспект требования	Описание требования	Угрозы/уязвимости безопасности
AU-3-2	Аутентификация	Перед передачей конфиденциальных данных или соединением в целях управления следует выполнять процесс взаимной аутентификации устройств	ST-D-2
CR-1-1	Криптография	При передаче или хранении данных должны использоваться безопасные криптографические алгоритмы	ST-D-8 ST-D-9
CR-1-2	Криптография	Необходимо осуществлять надежное управление криптографическими ключами на протяжении всего их жизненного цикла	ST-D-8
CR-1-3	Криптография	Генерирование случайных чисел следует осуществлять с помощью алгоритма с установленной степенью случайности	ST-D-8
DS-1-1	Безопасность данных	Передаваемые данные должны быть зашифрованы	ST-D-11
DS-1-2	Безопасность данных	При создании канала передачи данных или управления следует применять безопасный режим	ST-D-11
DS-1-3	Безопасность данных	Данные, хранящиеся в устройстве, должны быть зашифрованы	ST-D-11
DS-1-4	Безопасность данных	Удаленные данные не должны восстанавливаться	ST-D-17
DS-2-1	Безопасность данных	Не следует допускать несанкционированный сетевой трафик	ST-G-1
DS-2-2	Безопасность данных	Мониторинг доступа к данным и моделей потоков может помочь обнаружить аномалии и потенциальные инциденты в области безопасности, что обеспечит возможность своевременного вмешательства и реагирования	ST-G-1
DS-2-3	Безопасность данных	Реагирование на атаки DoS или DDoS с помощью шлюза IoT	ST-G-2
DS-3-1	Безопасность данных	По истечении заданного времени бездействия сеанс связи следует завершить	ST-D-12
DS-3-2	Безопасность данных	Значение идентификатора сеанса должно быть непредсказуемым	ST-D-12
DS-3-3	Безопасность данных	Сеансы следует аннулировать в режиме реального времени при обнаружении подозрительной активности или при отправке пользователем запроса на выход из системы	ST-D-12
DS-4-1	Безопасность данных	В течение жизненного цикла ключа следует осуществлять надежное управление данными PII	ST-D-11
PL-1-1	Безопасность платформы устройств	Следует применять безопасные методы кодирования	ST-D-10 ST-D-20 ST-D-23 ST-D-24

Таблица A.1 – Связь между требованиями безопасности IoT и угрозами/уязвимостями безопасности

Номер требования	Аспект требования	Описание требования	Угрозы/уязвимости безопасности
PL-1-2	Безопасность платформы устройств	Известные уязвимости программного обеспечения должны быть обнаружены и удалены	ST-D-16 ST-D-21
PL-1-3	Безопасность платформы устройств	Следует применять обфускацию	ST-D-16
PL-1-4	Безопасность платформы устройств	Следует поддерживать функцию проверки целостности параметров конфигурации и исполняемых кодов	ST-D-15
PL-2-1	Безопасность платформы устройств	Обновление должно проводиться авторизованными пользователями	ST-D-13
PL-2-2	Безопасность платформы устройств	Следует обеспечить функцию отката в случае сбоя процесса обновления	ST-D-14
PL-2-3	Безопасность платформы устройств	Перед обновлением следует выполнить проверку целостности и аутентификации	ST-D-15
PL-3-1	Безопасность платформы устройств	Излишние услуги следует отключить	ST-D-16
PL-3-2	Безопасность платформы устройств	Функции дистанционного управления следует выполнять в надежной среде	ST-D-18
PL-3-3	Безопасность платформы устройств	Следует применять безопасную стороннюю библиотеку	ST-D-22
PL-3-4	Безопасность платформы устройств	Следует предусмотреть самопроверку	ST-D-19
PL-4-1	Безопасность платформы устройств	Следует производить регистрацию событий, связанных с безопасностью	ST-D-23
PL-4-2	Безопасность платформы устройств	Следует обеспечить механизм безопасной регистрации событий	ST-D-23
PL-5-1	Безопасность платформы устройств	Следует обеспечить надежное проставление отметок времени	ST-D-18
PH-1-1	Физическая безопасность	Следует отключить все излишние внешние интерфейсы	ST-D-24 ST-D-25
PH-1-2	Физическая безопасность	Должен предотвращаться несанкционированный доступ к внутреннему интерфейсу	ST-D-24 ST-D-25
PH-1-3	Физическая безопасность	Следует обеспечить контроль среды	ST-D-24 ST-D-25
PH-2-1	Физическая безопасность	Следует обеспечить функцию обнаружения несанкционированного физического вмешательства и реагирования на него (пломбы, замки, защитная сигнализация, обнуляющие датчики, сигналы тревоги и т. п.)	ST-D-24 ST-D-25

Дополнение I

Возможности безопасности для интернета вещей

(Данное Дополнение не является неотъемлемой частью настоящей Рекомендации.)

I.1 Обзор

В настоящей Рекомендации рассматриваются только требования безопасности с учетом надежности и качества обслуживания. Возможности безопасности для IoT расширены по сравнению с описанными в [b-ITU-T X.1361]. В архитектуру IoT следует включить общие возможности, перечисленные в таблице I.1.

Таблица I.1 – Связь между требованиями безопасности IoT и возможностями безопасности

Возможности	Соответствующие требования
Безопасная связь для поддержки доверенной связи с обеспечением безопасности и защиты конфиденциальности данных	DP-1-1, DS-1-2
Безопасное управление ключами для поддержки безопасной связи	CR-2-1
Безопасное управление данными для доверенного управления данными с обеспечением безопасности и защиты их конфиденциальности	DS-2-1, DS-1-4
Аутентификация для проверки подлинности устройств	AU-1-1, AU-1-2, AU-1-3, AU-1-4, AU-1-8, AU-1-9
Авторизация (контроль доступа) для авторизации устройств	AU-3-1, AU-3-2
Аудит для обеспечения полностью прозрачного, прослеживаемого и воспроизводимого мониторинга доступа к данным и попыток доступа к приложениям IoT на основе соответствующих нормативно-правовых актов	PL-4-1, PL-4-2
Безопасное предоставление услуг для доверенного предоставления услуг с обеспечением безопасности и защиты конфиденциальности	DS-4-1, DS-3-2
Интеграция безопасности для интеграции различных стратегий и методов обеспечения безопасности, относящихся к разным функциональным компонентам IoT	–
Реализация безопасных протоколов с использованием общедоступных и стандартизированных алгоритмов шифрования	CR-1-1
Реализация безопасных протоколов на основе облегченного шифрования	CR-1-1
Безопасное и устойчивое обновление программного обеспечения, в частности модулей или приложений	PL-2-1, PL-2-2, PL-2-3
Управление определением идентичности для устройств/датчиков, шлюзов, платформ/служб IoT	AU-2-1, AU-2-2, AU-2-3, DS-3-2, DS-4-1
Сканирование на предмет выявления уязвимостей	–
Мониторинг доступа к данным и попыток доступа к приложениям IoT на основе полной прозрачности, прослеживаемости и воспроизводимости	PL-4-1, PL-4-2
Аппаратная защита (например, на базе модуля доверенной платформы) для предотвращения рисков, связанных с физическим доступом, которые возникают в результате виртуализации сетей и шлюзов	PH-1-1, PH-1-2, PH-2-1
Многотрактовая маршрутизация для предотвращения атак с избирательной переадресацией	–
Защита PII от утечек на протяжении всего жизненного цикла PII	DS-4-1
Настройка безопасной конфигурации	–
Использование облегченного шифрования	CR-1-1
Простое шифрование с присоединенными данными для маскирования (EAMD) [b-ITU-T X.1362] для связи с другими объектами, включая шлюз	–

В архитектуру IoT следует включить возможности, связанные с криптографическими алгоритмами, перечисленные в таблице I.2.

Таблица I.2 – Связь между требованиями безопасности и возможностями, связанными с криптографическими алгоритмами

Возможности	Соответствующие требования
Генерация случайных чисел криптографического качества для поддержки управления ключами [b-IETF RFC 4086]	CR-3-1
Периодическое обновление ключей шифрования, необходимых для потокового вещания	–
Использование стандартизированных алгоритмов шифрования	CR-1-1

В архитектуру IoT следует включить связанные с контекстом возможности, перечисленные в таблице I.3.

Таблица I.3 – Связь между требованиями безопасности и возможностями, связанными с контекстом

Возможности	Соответствующие требования
Устойчивость к атакам по сторонним каналам	–
Поддержка безопасной практики программирования, обеспечивающей тщательную проверку вводимых данных в системах, службах, приложениях баз данных и веб-услугах	PL-1-1, PL-1-3, PL-1-4
Плановая оценка рисков для определения рисков, возникающих в различных эксплуатационных контекстах	PL-1-4

I.2 Возможности безопасности для датчиков/устройств

В датчиках/устройствах IoT следует предусмотреть функции безопасности, перечисленные в таблице I.4.

Таблица I.4 – Связь между требованиями безопасности и возможностями безопасности для датчиков/устройств IoT

Возможности	Соответствующие требования
Управление ключами	CR-2-1
Согласование алгоритмов шифрования	CR-1-1
Шифрование данных, включая в некоторых случаях данные плоскости сигнализации, контроля и управления, для уменьшения проблем безопасности, связанных с конфиденциальностью данных, передаваемых по беспроводной сети	CR-1-1, DS-1-1, DS-1-2
Обеспечение целостности данных, передаваемых по беспроводной сети, с использованием соответствующей схемы защиты целостности, которая гарантирует, что пользовательские данные или данные плоскости сигнализации, контроля и управления не были искажены или изменены	CR-1-1, DS-1-1, DS-1-2, PL-2-3
Аутентификация источника данных или проверка подлинности датчиков/устройств IoT, а также администратора и обслуживающего персонала сенсорной сети	AU-1-2, AU-1-6, PL-2-1
Управление внесением исправлений, включая обновление защищенного программного модуля	PL-2-1, PL-2-2, PL-2-3
Реализация безопасного протокола на основе облегченного шифрования	CR-1-1

Таблица I.4 – Связь между требованиями безопасности и возможностями безопасности для датчиков/устройств IoT

Возможности	Соответствующие требования
Контроль доступа, гарантирующий, что доступ к элементам сети, хранимой информации, информационным потокам, услугам и приложениям имеют только авторизованные пользователи или устройства	AU-1-2, AU-3-1, AU-3-2
Обнаружение или предотвращение несанкционированного изменения	PH-2-1
Генерация случайных чисел криптографического качества для поддержки управления ключами	CR-3-1
Устойчивость к атакам по сторонним каналам	–
Обнаружение вредоносного программного обеспечения и защита от него	–
Защита от утечки PII	DS-4-1

В устройствах IoT следует предусмотреть функции безопасности, перечисленные в таблице I.5.

Таблица I.5 – Связь между требованиями безопасности и возможностями безопасности для устройств IoT

Возможности	Соответствующие требования
Проверка подлинности и целостности программного обеспечения на устройстве с использованием криптографически созданных цифровых подписей [b-ISO/IEC 9796-3]	PL-1-4
Брандмауэр, обнаружение вторжений, защита от вторжений или углубленная проверка пакетов для управления трафиком, завершающимся в устройстве	DS-2-1
Настройка безопасной конфигурации	PL-1-4

I.3 Возможности безопасности для шлюзов

Следует поддерживать возможности безопасности платформ/услуг, перечисленные в таблице I.6.

Таблица I.6 – Связь между требованиями безопасности и возможностями безопасности для шлюзов

Возможности	Соответствующие требования
Система обнаружения вторжений (IDS)/система предотвращения вторжений (IPS)	DS-2-1
Управление ключами	CR-2-1
Настройка безопасной конфигурации	PL-1-4
Согласование алгоритмов шифрования	CR-1-1
Шифрование данных, включая в некоторых случаях данные плоскости сигнализации, контроля и управления, передаваемые между шлюзом и устройствами или компонентами IoT в центре обработки данных, для уменьшения проблемы безопасности, связанной с конфиденциальностью данных, передаваемых по беспроводной сети	CR-1-1, DS-1-1, DS-1-2
Обеспечение целостности данных, передаваемых по беспроводной сети, с использованием соответствующей схемы защиты целостности, которая гарантирует, что пользовательские данные или данные плоскости сигнализации, контроля или управления не были искажены или изменены	CR-1-1, DS-1-1, DS-1-2, PL-2-3

Таблица I.6 – Связь между требованиями безопасности и возможностями безопасности для шлюзов

Возможности	Соответствующие требования
Поддержание готовности к противодействию DoS-атакам различными методами – от безопасной разработки исходных программ, анализа исходного кода и тестирования на уязвимости до использования системы обнаружения или предотвращения вторжений в сети или на хосте	PL-1-1, DS-2-2
Аутентификация источника данных или проверка подлинности датчиков/устройств IoT, а также администратора и обслуживающего персонала сенсорной сети	AU-1-2, AU-1-6, PL-2-1
Контроль доступа, гарантирующий, что доступ к элементам сети, хранимой информации, информационным потокам, услугам и приложениям имеют только авторизованные пользователи или устройства	AU-1-2, AU-3-1, AU-3-2
Подотчетность устройств IoT для обеспечения того, чтобы любое нарушение политики можно было проследить до конкретного устройства	PL-4-1
Возможность обновления защищенных программных модулей	PL-2-1, PL-2-2, PL-2-3

I.4 Возможности безопасности для сетей

Согласно [b-ITU-T X.805] для сети следует обеспечить возможности безопасности, перечисленные в таблице I.7.

Таблица I.7 – Связь между требованиями безопасности и возможностями безопасности для сети

Элементы	Возможности	Соответствующие требования
C_NT.1 [b-ITU-T X.805]	Аспект безопасности связи гарантирует, что информация передается только между уполномоченными оконечными точками (информация не изменяет направления и не перехватывается при передаче между этими оконечными точками)	PL-3-1

I.5 Возможности безопасности для платформ/служб

Платформы/службы должны поддерживать возможности безопасности, перечисленные в таблице I.8.

Таблица I.8 – Связь между требованиями безопасности и возможностями безопасности для платформ/служб

Возможности	Соответствующие требования
Защита регистрационных данных для криптографических операций – набора данных, удостоверяющих заявленную идентичность и/или полномочия	DS-2-1
Смена заданных по умолчанию имен пользователей и паролей в ходе первоначальной настройки	AU-1-1, AU-1-2
Реализация надежных паролей и детализированной политики контроля доступа	AU-1-4, AU-1-6
Блокирование излишних портов	PL-3-1, PH-1-1, PH-1-2
Поддержка настройки безопасной конфигурации, например, для удаления излишних служб и программного обеспечения	AU-1-5, PL-3-1
Защита от заражения вредоносными программами путем использования антивирусного программного обеспечения	PL-3-4
Реализация политики управления внесением исправлений	PL-2-1, PL-2-2, PL-2-3

Таблица I.8 – Связь между требованиями безопасности и возможностями безопасности для платформ/служб

Возможности	Соответствующие требования
Управление уязвимостями	PL-1-1, PL-1-2
Обновление защищенных программных модулей и приложений	PL-2-1, PL-2-3
Управление ключами для безопасного обмена сообщениями между шлюзом и платформой/службой	CR-1-2
Согласование алгоритмов шифрования для организации безопасного туннеля между шлюзом и платформой/службой в том случае, если необходим безопасный обмен сообщениями между шлюзом и платформой/службой; поддержание готовности к противодействию DoS-атакам	AU-1-5, DS-1-1, DS-1-2
Сетевой мониторинг	–
Защита PII при хранении	DS-4-1
Обеспечение безопасности на прикладном уровне для предотвращения угроз и атак на прикладном уровне, описанных в пункте 8.4 [ITU-T X.1361]	–
Обеспечение поддержки для снижения последствий атак на основе логических выводов	–

Дополнение II

Примеры применения требований безопасности для устройств и шлюзов интернета вещей

(Данное Дополнение не является неотъемлемой частью настоящей Рекомендации.)

Многие устройства IoT имеют уязвимости и недостатки защиты, связанные с аутентификацией, криптографией и защитой данных. Кроме того, большинство из них уязвимы в отношении физических интерфейсов и платформ разработки устройств. В этом Дополнении описаны примеры разработки функций безопасности в соответствии с предлагаемыми требованиями.

II.1 Пример применения аутентификации – уязвимость к атакам через посредника

Известна уязвимость процедуры аутентификации между сервером и сетевой видеокамерой. При квитировании TLS сетевая видеокамера не отклоняет недействительные сертификаты. Злоумышленник похищает важный ключ. См. рисунок II.1.

Меры противодействия:

– отказ от приема недействительного сертификата протокола защищенных сокетов;

– использование привязки открытого ключа протокола передачи гипертекста.

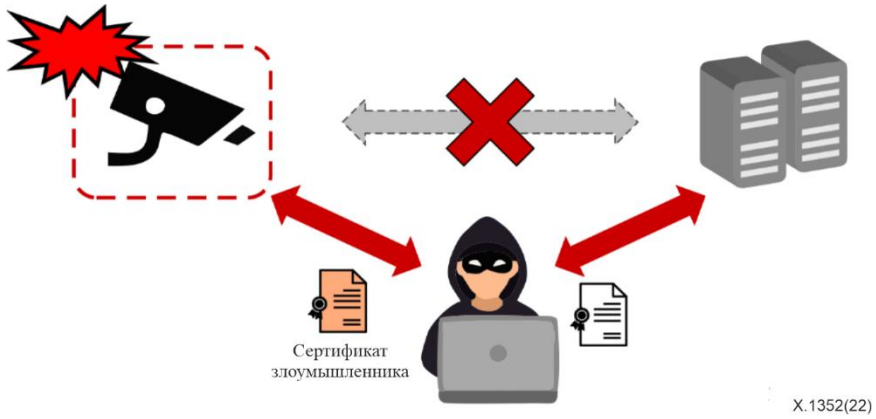

Рисунок II.1 – Пример аутентификации

II.2 Пример применения криптографии – слабый криптографический алгоритм

См. рисунок II.2.

Возможные уязвимости:

– слабый алгоритм шифрования – Base64;

– метод проверки данных – защищенный алгоритм хеширования 1 (SHA1).

Меры противодействия:

– уровень безопасности выше, чем у 128-битового алгоритма шифрования (см. [b-ISO/IEC 19790]);

– метод проверки данных – SHA 256 [b-ISO/IEC 10118-3].

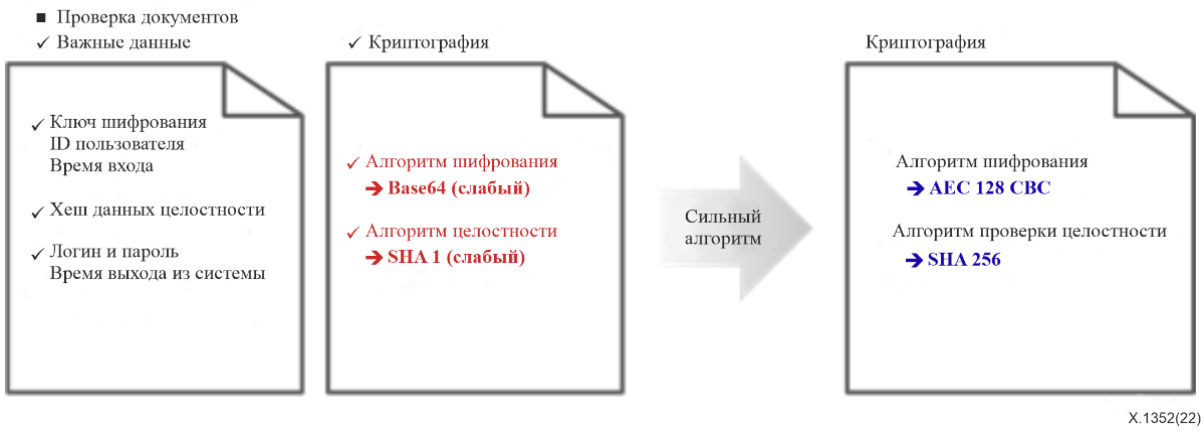

Рисунок II.2 – Пример применения криптографии

II.3 Пример применения функций защиты данных и криптографии – слабая проверка целостности передаваемых данных

См. рисунок II.3.

Уязвимость:

– слабая проверка целостности передаваемых данных (метод проверки целостности данных – циклическая проверка по избыточности).

Меры противодействия:

– метод проверки данных – хеш-данные SHA 256 [b-ISO/IEC 10118-3];

– полное разделение данных и пересборка кадров.

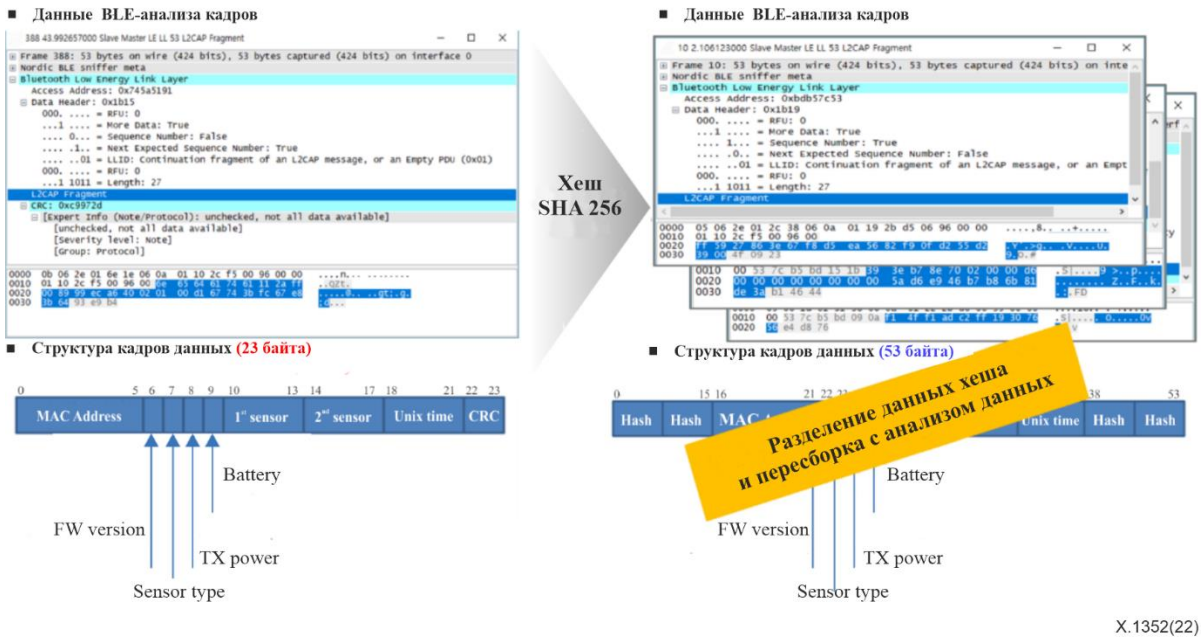

Рисунок II.3 – Пример применения функций защиты данных и криптографии

II.4 Пример применения защиты платформы устройств – слабое кодирование против эксплуатации уязвимостей

См. рисунок II.4.

Уязвимость:

– переполнение буфера и слабый API.

Средство защиты:

– проверка безопасного кодирования и предложение по устранению слабых кодов средствами статического анализа.

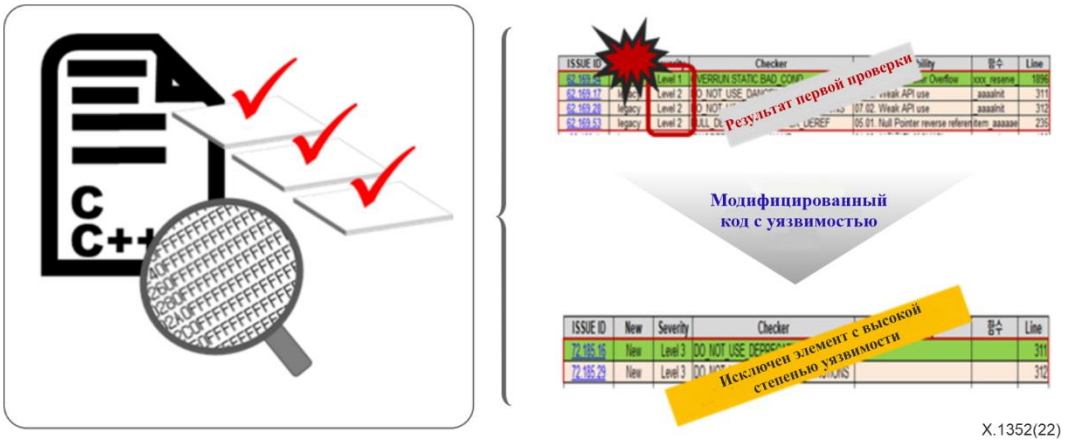

Рисунок II.4 – Пример применения функций защиты платформы устройств

II.5 Пример применения физической защиты – уязвимость внутреннего интерфейса на печатной плате

См. рисунок II.5.

Уязвимость:

– на массовом изделии доступен порт JTAG.

Средство защиты:

– обеспечение защиты доступа к памяти в MCU.

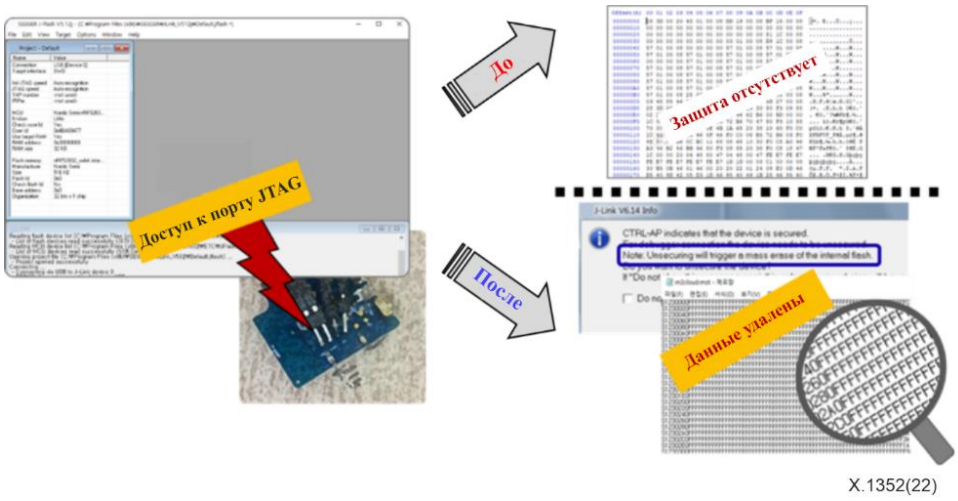

Рисунок II.5 – Пример применения физической защиты

Библиография

[b-ITU-T X.667] Recommendation ITU-T X.667 (2012), *Information technology – Procedures for the operation of object identifier registration authorities: Generation of universally unique identifiers and their use in object identifier*.

[b-ITU-T X.800] Рекомендация МСЭ-Т X.800 (1991 г.), *Архитектура безопасности для взаимосвязи открытых систем для приложений МККТТ*.

[b-ITU-T X.805] Рекомендация МСЭ-Т X.805 (2003 г.), *Архитектура безопасности для систем, обеспечивающих связь между оконечными устройствами*.

[b-ITU-T X.1252] Рекомендация МСЭ-Т X.1252 (2021 г.), *Базовые термины и определения в области управления определением идентичности*.

b-ITU-T X.1254] Рекомендация МСЭ-Т X.1254 (2020 г.), *Структура гарантии аутентификации объекта*.

[b-ITU-T X.1362] Рекомендация МСЭ-Т X.1362 (2017 г.), *Простая процедура шифрования для среды интернета вещей (IoT)*.

[b-ITU-T Y.4000] Рекомендация МСЭ-Т Y.4000/Y.2060 (2012 г.), *Обзор интернета вещей*.

[b-ISO 16100-1] ISO 16100-1:2009, *Industrial automation systems and integration – Manufacturing software capability profiling for interoperability – Part 1: Framework.*

[b-ISO/IEC 9796-3] ISO/IEC 9796-3:2006, *Information technology – Security techniques – Digital signature schemes giving message recovery – Part 3: Discrete logarithm based mechanisms.*

[b-ISO/IEC 10118-3] ISO/IEC 10118-3 (2018), IT *Security techniques – Hash-functions – Part 3: Dedicated hash-functions.*

[b-ISO/IEC 19790] ISO/IEC 19790 (2012), *Information technology – Security techniques – Security requirements for cryptographic modules.*

[b-ISO/IEC 27000] ISO/IEC 27000:2018, *Information technology – Security techniques – Information security management systems – Overview and vocabulary.*

[b-ISO/IEC 27033-1] ISO/IEC 27033-1:2015, *Information technology – Security techniques – Network security – Part 1: Overview and concepts.*

[b-ISO/IEC 29100] ISO/IEC 29100:2011, *Information technology – Security techniques – Privacy framework.*

[b-IETF RFC 4086] IETF RFC 4086 (2005), *Randomness requirements for security.*

[b-CVE] Mitre Corporation (Internet). *Common vulnerabilities and exposures*. Bedford, MA: Mitre Corporation. Available [viewed 2022-10-29] at: https://cve.mitre.org/

СЕРИИ РЕКОМЕНДАЦИЙ МСЭ-Т

Серия A	Организация работы МСЭ-Т
Серия D	Принципы тарификации и учета и экономические и стратегические вопросы международной электросвязи/ИКТ
Серия E	Общая эксплуатация сети, телефонная служба, функционирование служб и человеческие факторы
Серия F	Нетелефонные службы электросвязи
Серия G	Системы и среда передачи, цифровые системы и сети
Серия H	Аудиовизуальные и мультимедийные системы
Серия I	Цифровая сеть с интеграцией служб
Серия J	Кабельные сети и передача сигналов телевизионных и звуковых программ и других мультимедийных сигналов
Серия K	Защита от помех
Серия L	Окружающая среда и ИКТ, изменение климата, электронные отходы, энергоэффективность; конструкция, прокладка и защита кабелей и других элементов линейно-кабельных сооружений
Серия M	Управление электросвязью, включая СУЭ и техническое обслуживание сетей
Серия N	Техническое обслуживание: международные каналы передачи звуковых и телевизионных программ
Серия O	Требования к измерительной аппаратуре
Серия P	Качество телефонной передачи, телефонные установки, сети местных линий
Серия Q	Коммутация и сигнализация, а также соответствующие измерения и испытания
Серия R	Телеграфная передача
Серия S	Оконечное оборудование для телеграфных служб
Серия T	Оконечное оборудование для телематических служб
Серия U	Телеграфная коммутация
Серия V	Передача данных по телефонной сети
Серия X	**Сети передачи данных, взаимосвязь открытых систем и безопасность**
Серия Y	Глобальная информационная инфраструктура, аспекты протокола Интернет, сети последующих поколений, интернет вещей и "умные" города
Серия Z	Языки и общие аспекты программного обеспечения для систем электросвязи

Отпечатано в Швейцарии
Женева, 2024 г.