ФЕДЕРАЛЬНОЕ АГЕНТСТВО

ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

ГОСТ Р ИСО/МЭК 27033-2— 2021

Информационные технологии

МЕТОДЫ И СРЕДСТВА ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ

Безопасность сетей

Часть 2

Рекомендации по проектированию и реализации безопасности сетей

(ISO/IEC 27033-2:2012, IDT)

Издание официальное

Москва
Стандартинформ
2021

Предисловие

1 ПОДГОТОВЛЕН Федеральным государственным учреждением «Федеральный исследовательский центр «Информатика и управление» Российской академии наук» (ФИЦ ИУ РАН); Акционерным обществом «Научно-технический и сертификационный центр по комплексной защите информации» (АО Центр «Атомзащитаинформ») ГК «Росатом» и Обществом с ограниченной ответственностью «Информационно-аналитический вычислительный центр» (ООО ИАВЦ) на основе собственного перевода на русский язык англоязычной версии стандарта, указанного в пункте 4

2 ВНЕСЕН Техническим комитетом по стандартизации ТК 22 «Информационные технологии»

3 УТВЕРЖДЕН И ВВЕДЕН В ДЕЙСТВИЕ Приказом Федерального агентства по техническому регулированию и метрологии от 18 мая 2021 г. № 368-ст

4 Настоящий стандарт идентичен международному стандарту ИСО/МЭК 27033-2:2012 «Информационные технологии. Методы и средства обеспечения безопасности. Безопасность сетей. Часть 2. Рекомендации по проектированию и реализации безопасности сетей» (ISO/IEC 27033-2:2012 «Information Technology—Security Techniques —Network Security — Part 2: Guidelines for the design and implementation of network security», IDT).

ИСО/МЭК 27033-2 разработан подкомитетом ПК 27 «Методы и средства обеспечения безопасности ИТ» Совместного технического комитета СТК 1 «Информационные технологии» Международной организации по стандартизации (ИСО) и Международной электротехнической комиссии (МЭК).

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

Дополнительные сноски в тексте стандарта, выделенные курсивом, приведены для пояснения текста оригинала

5 ВВЕДЕН ВПЕРВЫЕ

6 Некоторые положения международного стандарта, указанного в пункте 4, могут являться объектом патентных прав. Международная организация по стандартизации (ИСО) и Международная электротехническая комиссия (МЭК) не несут ответственности за идентификацию подобных патентных прав

Правила применения настоящего стандарта установлены в статье 26 Федерального закона от 29 июня 2015 г. № 162-ФЗ «О стандартизации в Российской Федерации». Информация об изменениях к настоящему стандарту публикуется в ежегодном (по состоянию на 1 января текущего года) информационном указателе «Национальные стандарты», а официальный текст изменений и поправок — в ежемесячном информационном указателе «Национальные стандарты». В случае пересмотра (замены) или отмены настоящего стандарта соответствующее уведомление будет опубликовано в ближайшем выпуске ежемесячного информационного указателя «Национальные стандарты». Соответствующая информация, уведомление и тексты размещаются также в информационной системе общего пользования — на официальном сайте Федерального агентства по техническому регулированию и метрологии в сети Интернет (www.gost.ru)

Содержание

Введение

Серия ИСО/МЭК 27033 состоит из следующих частей под одним общим заголовком: «Информационные технологии. Методы и средства обеспечения безопасности. Безопасность сетей»:

- часть 1. Обзор и понятия;
- часть 2. Рекомендации по проектированию и реализации безопасности сетей[1)];
- часть 3. Эталонные варианты реализации сетей. Угрозы, методы проектирования и вопросы управления;
- часть 4. Обеспечение безопасного межсетевого взаимодействия между сетями с помощью шлюзов безопасности;
- часть 5. Обеспечение безопасного межсетевого взаимодействия в сетях с помощью виртуальных частных сетей (VPN[2)]);
- часть 6. Обеспечение безопасности беспроводного доступа к IP-сетям.

Примечание — Следует отметить, что могут появиться и другие части, относящиеся к постоянно изменяющимся и возникающим технологиям в области безопасности сетей.

---

1) *Положения настоящего стандарта должны рассматриваться с учетом требований национальных нормативных правовых актов и стандартов Российской Федерации в области защиты информации.*

2) *Далее по тексту используется сокращение VPN.*

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

Информационные технологии

МЕТОДЫ И СРЕДСТВА ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ

Безопасность сетей

Часть 2

Рекомендации по проектированию и реализации безопасности сетей

Information technology. Security techniques. Network security.
Part 2. Guidelines for the design and implementation of network security

Дата введения — 2021—11—30

1 Область применения

Настоящий стандарт содержит рекомендации для организаций при проектировании и внедрении систем обеспечения безопасности сетей, а также документирования этих процессов.

2 Нормативные ссылки

В настоящем стандарте использованы следующие нормативные ссылки. Для датированных ссылок применяют только указанное издание, для недатированных — последнее издание (включая все изменения).

ISO/IEC 7498 (all parts), Information technology — Open systems interconnection — Basic reference model (Информационные технологии. Взаимосвязь открытых систем. Базовая эталонная модель)

ISO/IEC 27000:2009, Information technology — Security techniques — Information security management systems — Overview and vocabulary (Информационные технологии. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Общий обзор и терминология)

ISO/IEC 27001:2005, Information technology — Security techniques — Information security management systems — Requirements (Информационные технологии. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования)

ISO/IEC 27002:2005, Information technology — Security techniques — Code of practice for information security management (Информационные технологии. Методы и средства обеспечения безопасности. Свод норм и правил менеджмента информационной безопасности)

ISO/IEC 27005:2011, Information technology — Security techniques — Information security risk management (Информационные технологии. Методы и средства обеспечения безопасности. Менеджмент риска информационной безопасности)

ISO/IEC 27033-1, Information technology — Security techniques — Network security — Part 1: Overview and concepts (Информационные технологии. Методы и средства обеспечения безопасности. Безопасность сетей. Часть 1. Обзор и понятия)

Издание официальное

3 Термины и определения

В настоящем стандарте применены термины по ИСО/МЭК 7498 (все части), ИСО/МЭК 27000, ИСО/МЭК 27001, ИСО/МЭК 27002, ИСО /МЭК 27005 и ИСО/МЭК 27033-1.

4 Сокращения

POC — доказательство концепции (proof of concept);

RADIUS — служба удаленной аутентификации пользователей при коммутируемом подключении (remote authentication dial-in user service);

RAS — служба удаленного доступа (remote access service);

SMS — служба рассылки коротких сообщений (simple message service);

SMTP — простой протокол передачи почты (simple mail transfer protocol);

TACACS — сеансовый протокол управления терминальным доступом посредством системы (сервера) управления доступом (terminal access controller access-control system);

TFTP — простой протокол передачи файлов (trivial file transfer protocol);

TLS — протокол защиты транспортного уровня (transport layer security);

СПВ — система предотвращения вторжения.

5 Структура документа

Настоящий стандарт содержит следующие разделы и подразделы:

- подготовка к проектированию безопасности сетей:
  - введение;
  - идентификация активов;
  - сбор требований;
  - анализ требований;
  - анализ существующих проектов и реализаций;
- проектирование безопасности сетей:
  - введение;
  - принципы проектирования;
  - утверждение проекта;
- реализация:
  - введение;
  - критерии выбора сетевых компонентов;
  - критерии выбора продукта или поставщика;
  - управление сетью;
  - регистрация, мониторинг и реагирование на инциденты;
  - документация;
  - планы испытаний и проведение испытаний;
- утверждение реализации.

6 Подготовка к проектированию безопасности сетей

6.1 Введение

Цели создания безопасных сетей заключаются в обеспечении функционирования таких потоков информации, которые улучшают бизнес-процессы организации, и предотвращении потоков информации, которые их ухудшают. Подготовительные работы по проектированию и реализации безопасности сетей включают в себя следующие этапы:

- идентификация активов;
- сбор требований;
- анализ требований;

- оценка технических возможностей и ограничений;
- оценка существующих проектов и реализаций.

Данные этапы должны привести к подготовке начальной документации, содержащей все исходные данные для последующих этапов проектирования и реализации.

6.2 Идентификация активов

Идентификация активов является важным первым шагом в определении рисков информационной безопасности (ИБ[1)]) всех сетей. Защищаемые активы — это активы, которые могут ухудшить бизнес-процессы организации, если будут нарушены их целостность, доступность и конфиденциальность. Они включают в себя физические активы (серверы, коммутаторы, маршрутизаторы и т. д.) и логические активы (конфигурационные настройки, исполняемый код, данные и т. д.). Этот перечень активов должен быть создан как часть планирования непрерывности бизнес-процессов и анализа риска невозможности восстановления после аварий. Вопросы, на которые необходимо ответить:

- Какие отдельные типы сетевого оборудования и группы объектов должны быть защищены?
- Какие отдельные сегменты сетевой инфраструктуры должны быть защищены?
- Какие информационные активы и средства обработки информации должны быть защищены?
- Где в архитектуре информационных систем находятся информационные активы?

Идентифицируемые активы включают активы, необходимые для безопасной поддержки процессов управления и контроля трафика пользователей, а также функции, необходимые для функционирования сетевой инфраструктуры, услуг и приложений. К ним относятся такие устройства, как хосты, маршрутизаторы, межсетевые экраны и т. д., интерфейсы (внутренние и внешние), хранимая/обрабатываемая информация и используемые протоколы. Защита активов инфраструктуры является лишь частью цели проектирования безопасности сетей. Основной целью является защита активов организации таких, как информация и бизнес-процессы.

6.3 Сбор требований

6.3.1 Нормативные правовые требования

Нормативные правовые требования к расположению и функционированию сети должны собираться и анализироваться с целью обеспечения соблюдения таких требований при проектировании сети. Особую осторожность следует соблюдать, когда информация передается на территорию с другой юрисдикцией или другим нормативным полем. В таких случаях должны быть задокументированы требования обеих территорий с другой юрисдикцией или другим нормативным полем.

6.3.2 Требования основной деятельности организации

Бизнес-процессы организации и типы классификации данных определяют требования по доступу к ним. Сеть должна быть настроена таким образом, чтобы разрешить доступ к и от своих информационных активов только для надлежащим образом авторизованных пользователей, и предотвратить несанкционированный доступ. Доступ к информации часто соотносится со службами на открытых портах (например, HTTP на TCP-порте 80) конкретных узлов (таких как www.example.org по IP-адресу 10.11.12.13) определенных групп узлов (например, 172.128.97.64/24 подсеть) или определенных устройств сетевого интерфейса (например, интерфейс с MAC-адресом 10:00:00:01:02:03). Организации необходимо определить службы, которые она предоставляет другим организациям и которыми сама пользуется у других организаций, и те службы, которые она предоставляет внутри своей организации.

6.3.3 Требования производительности

Данные трафика необходимы для того, чтобы задокументировать конфигурацию линий связи, серверов и шлюзов безопасности/межсетевых экранов (МЭ[2)]) таким образом, чтобы при реализации можно было обеспечить достаточный уровень обслуживания в соответствии с ожиданиями пользователей — без изменения конфигурации и связанных с этим простоев сервиса. Следует собирать информацию о таких характеристиках, как скорость передачи в существующих каналах связи, конфигурация/пропускная способность маршрутизаторов во всех сторонних организациях, количество пользователей, которым будет разрешен доступ по каждому каналу связи (одновременный доступ и количество пользователей с доступом), минимальное, среднее и максимальное требуемое время подключения пользователя, и проводить идентификацию того, к чему авторизованные пользователи будут получать доступ по

[1)] *Далее по тексту используется сокращение ИБ.*

[2)] *Далее по тексту используется сокращение МЭ.*

определенному каналу связи, необходимое количество обращений к веб-страницам, требуемое число посещений базы данных, ожидаемый рост в течение одного года и трех/пяти лет и требуется ли наличие входа в ОС. Для определения количества портов, требуемых каналов, особенно коммутируемых каналов связи, можно использовать теорию телекоммуникационных таблиц (очередей). Требования к производительности следует проанализировать, разрешить возникшие вопросы, а критерии требуемой производительности, которые должны соответствовать технической архитектуре и соответствующей архитектуре технической защиты, следует официально согласовать между пользователями и поставщиками услуг.

6.4 Анализ требований

Необходимо проанализировать текущие возможности и все запланированные технические изменения архитектуры сети и сравнить их с разрабатываемой архитектурой технической безопасности для выявления всех несоответствий. Все несоответствия необходимо проанализировать и внести изменения в соответствующие архитектуры.

Информация, которую необходимо получить во время анализа, должна включать как минимум следующее:

- идентификацию типа (типов) сетевого соединения, которое будет использоваться;
- определение рисков безопасности;
- разработку перечня требуемых технических безопасных архитектурных решений и мер обеспечения безопасности;
- сетевые протоколы, которые будут использоваться;
- сетевые приложения, используемые в сети для различных целей.

Собранная информация должна быть представлена в контексте возможностей сети. Следует собрать подробную информацию о соответствующей архитектуре сети, которую требуется проанализировать для формирования необходимого понимания и содержания для последующих этапов процесса. Понимание этих аспектов на самой ранней возможной стадии, определение соответствующих критериев идентификации требований безопасности и областей контроля, анализ вариантов архитектуры технической безопасности и решение о том, какой из вариантов должен быть принят, должны стать более эффективными и, в конечном итоге, привести к более работоспособному решению по обеспечению безопасности. Например, может случиться так, что из-за местоположения существует только один канал для всех сетевых подключений, которые должны быть установлены через него; но даже если мера обеспечения безопасности предоставляет разные каналы для резервных соединений, то это будет невыполнимо при выбранном местоположении. Тогда, возможно, для нахождения лучшего способа защиты сетевых подключений придется определить другие меры обеспечения безопасности.

Рассмотрение сетевых и прикладных архитектурных аспектов на ранней стадии даст время проанализировать эти архитектуры и, возможно, пересмотреть их, если приемлемое решение по обеспечению безопасности не может быть реально получено при текущей архитектуре.

6.5 Анализ существующих проектов и реализаций

Анализ существующих мер обеспечения безопасности должен проводиться в рамках соответствующего этапа управления рисками безопасности и анализа процессов управления рисками безопасности (подробности об управлении рисками можно найти в ИСО/МЭК 27005). Результаты оценки рисков безопасности могут указать на то, какие меры обеспечения безопасности необходимы для оцененных угроз. Чтобы определить, что не учитывается в существующей архитектуре сетевой безопасности, для нее необходимо провести анализ расхождений (англ. gap analysis).

В архитектуре безопасности сетей должны учитываться все существующие, а также все неиспользованные или планируемые к внедрению меры обеспечения безопасности.

7 Проектирование безопасности сетей

7.1 Анализ существующих проектов и реализаций

Архитектура безопасности сетей предназначена для ограничения трафика, проходящего между различными доверенными доменами. Наиболее очевидной границей между доверенными доменами является интерфейс между внутренней сетью организации и внешним миром. Организация независимо от размера также будет иметь границы между внутренними доверенными доменами, которые должны

быть идентифицированы и контролироваться. Архитектура безопасности сетей включает в себя описание интерфейсов между внутренней сетью организации/сообщества и внешним миром. Она отражает требования, упомянутые в 6.4, и рассматривает, как защитить организацию от общих угроз и уязвимостей, которые описаны в ИСО/МЭК 27033-1.

Руководство по общим лучшим практикам проектирования приведено в 7.2, а руководство по вопросам архитектуры безопасности сетей, связанным с конкретными сетевыми технологиями для удовлетворения требований сегодняшнего и ближайшего будущего, приведено в ИСО/МЭК 27033-4 и других стандартах серии ИСО/МЭК 27033. Руководство по конкретным сценариям, которые возможны для организации, изложено в ИСО/МЭК 27033-3.

Технические предположения, сделанные в ходе сбора требований, следует задокументировать, например:

- только авторизованные IP-соединения должны быть разрешены (межсетевые экраны обычно работают только с IP-соединениями, и если бы любые другие протоколы были бы разрешены, то межсетевыми экранами было бы сложно управлять);
- если требуется поддерживать не IP-протоколы, то их следует использовать либо за пределами архитектуры безопасности, либо путем туннелирования протокола.

Архитектура безопасности сетей обычно включает службы типа следующих, но не ограничивается ими:

- идентификации и аутентификации (пароли, токены, смарт-карты, сертификаты, система контроля доступа RAS/RADIUS/контроллер терминального доступа и TACACS+ и т. д.);
- логические элементы управления доступом (единая точка входа, управление доступом на основе ролей, доверенные базы данных, меры обеспечения безопасности приложений, межсетевые экраны, прокси-устройства и т. д.);
- аудит и учет безопасности (журналы регистрации событий, средства анализа журналов регистрации событий, средства обнаружения вторжений, устройства однократной записи и многократного чтения (англ. write once read many, WORM) и т. д.);
- гарантированная очистка памяти/безопасное удаление (гарантированные средства удаления);
- тестирование безопасности (сканирование уязвимостей, прослушивание (англ. sniffing) сети, тестирование на проникновение и т. д.);
- безопасная среда разработки (среды раздельной разработки и тестирования, без компиляторов и т. д.);
- меры обеспечения безопасности изменений программного обеспечения (ПО) (ПО управления конфигурацией, контроль версий и т. д.);
- безопасное распространение ПО (цифровая подпись, протокол уровня защищённых сокетов SSL[1)], безопасность транспортного уровня (TLS) (RFC 5246) и т. д.);
- безопасное обслуживание и доступность (надежные средства резервного копирования/восстановления, устойчивость, кластеризация, хранилища данных, разнообразные коммуникации и т. д.);
- безопасность передачи (использование шифрования контекста, технологии с расширенным спектром, защищаемые беспроводные LANs (WLANs), вирутальные частные сети VPNs/экстрасети).

7.2 Принципы проектирования

7.2.1 Введение

Общими областями риска, связанными с архитектурами безопасности сетей, являются сбои проекта из-за плохого проектирования и/или надлежащего рассмотрения планирования непрерывности деятельности организации, или проект не соответствует текущему или ожидаемому уровню угроз. Для разработки архитектур безопасности сетей необходимы базовые элементы, которые включают все установленные меры обеспечения безопасности и требования организации. На большинство этих элементов могут распространяться общие рекомендации по проектированию безопасности сети. ИСО/МЭК 27033-4 и другие стандарты серии ИСО/МЭК 27033 подробно описывают проектирование и реализацию некоторых аспектов наилучших практик в области архитектур технической безопасности сетей. Дополнительное подробное руководство по внедрению лучших практик можно найти в соответствующих документах.

[1)] *Протокол уровня защищенных сокетов (secure sockets layer protocol).*

В следующих разделах приведено общее руководство по лучшим практикам проектирования, которым необходимо следовать при рассмотрении архитектуры безопасности сетей.

7.2.2 Многоуровневая защита

Организациям необходимо обеспечить всеобъемлющий многоуровневый подход к рассмотрению безопасности. Безопасность должна быть всесторонней на всех уровнях сети. Выбор многоуровневого подхода — это и есть многоуровневая (глубокоэшелонированная, от англ. defence in depth) защита. Компоненты безопасности — это сочетание политики, проекта, управления и технологии. Каждой организации необходимо определить свои потребности и проектировать глубокоэшелонированную защиту на основе своих потребностей.

Многие мобильные устройства имеют USB- и сетевое подключение, а также возможности беспроводного соединения. Эти устройства могут быть подключены к внутренней сети или системам в ней специальным образом; если это будет сделано с помощью открытого и небезопасного беспроводного соединения устройства, то такие устройства могут использоваться как несанкционированные точки беспроводного доступа во внутренние сети, минуя меры обеспечения безопасности периметра. Для ограничения подключения незащищенных мобильных устройств к сети должны быть установлены строгие политики, а для обнаружения каких-либо несанкционированных точек доступа следует проводить обычное сканирование беспроводных каналов.

Все точки беспроводного доступа должны находиться в демилитаризованной зоне (ДМЗ[1)]). Те точки доступа, которые находятся во внутренней сети, должны иметь строгие настройки подключения: максимальную безопасность (защищенный WiFi-доступ WPA2, где это возможно) и фильтрацию MAC-адресов с целью ограничить устройства, которые могут подключаться к нему, только теми, которые авторизованы. ИСО/МЭК 27033-3 предоставляет более подробную информацию об угрозах, связанных с технологией мобильной связи, и соответствующих мерах обеспечения безопасности.

Принцип глубокоэшелонированной защиты означает использование нескольких мер обеспечения безопасности или методов защиты, которые позволяют снизить риск для каждого объекта защиты до того, как он будет скомпрометирован или выведен из строя. Примером может служить антивирусное ПО, установленное на отдельных рабочих станциях, если в этой среде на межсетевых экранах и серверах уже есть антивирусная защита. Для защиты различных потенциальных направлений от атак внутри сети могут быть размещены средства защиты от различных поставщиков, предотвращающие нарушения на всех уровнях безопасности, что и реализует «многоуровневый подход».

На рисунке 1 показано, как обеспечивается защита, начиная с периметра, более «узкой» защиты инфраструктуры, еще более узкой для хостов и приложений, и заканчивая данными. Все слои предназначены для защиты данных.

Рисунок 1 — Многоуровневая защита сети

Решения по обеспечению безопасности, основанные на многоуровневом подходе, являются гибкими и масштабируемыми. Такое решение адаптируется к потребностям безопасности организации.

[1)] *Далее по тексту используется сокращение ДМЗ.*

7.2.3 Сетевые сегменты

Сегментирование сети использует концепцию, согласно которой системным ресурсам с разными уровнями чувствительности (т.е. с разными значениями устойчивости к риску и восприимчивости к угрозам) следует находиться в разных доменах безопасности. Тогда в конкретном сегменте сети следует сделать доступными только те данные, которые необходимы для выполнения задач (например, в общедоступной системе доменных имен (DNS) зарегистрированы только серверы, предоставляющие услуги в Интернете).

Основным средством поддержания и ограничения потока сетевого трафика там, где это требуется, является шлюз безопасности: выделенные МЭ, функции МЭ в СПВ и списки управления доступом в сетевых маршрутизаторах и коммутаторах.

При правильном размещении и настройке шлюзы безопасности помогают создавать безопасные архитектуры, разделяя сетевую инфраструктуру на домены безопасности и управляя связью между ними. Дополнительную информацию о том, как размещать и настраивать шлюзы безопасности, можно найти в ИСО/МЭК 27033-4.

Принцип разделения описывает следующие правила проектирования безопасности сети:

- сети с разным уровнем чувствительности следует разграничивать на сегменты с соответствующими уровнями безопасности;
- устройства и компьютерные системы, предоставляющие услуги для внешних сетей (например, сеть Интернет), должны быть расположены в других сегментах (в ДМЗ), отличных от тех, где находятся внутренние сетевые устройства и компьютерные системы;
- стратегические активы следует располагать в выделенных доменах безопасности;
- устройства и компьютерные системы с низким уровнем доверия, такие как серверы удаленного доступа и точки доступа беспроводной сети, следует располагать в выделенных доменах безопасности;
- сети разных типов следует располагать в отдельных доменах безопасности;
- рабочие станции пользователей следует располагать в разных с серверами доменах безопасности;
- системы управления сетью и безопасностью следует располагать в выделенных доменах безопасности;
- системы в стадии разработки следует располагать в разных с эксплуатируемыми системами сегментах.

7.2.4 Отказоустойчивая архитектура проекта сети

Проект безопасности сетей должен включать разумную избыточность средств защиты, чтобы исключить единые точки отказа и максимизировать доступность сетевой инфраструктуры. Это означает использование дополнительных интерфейсов, модулей резервного копирования, резервных устройств и резервных путей передачи данных. Также в проектах используется широкий набор функций, предназначенных для повышения устойчивости сети к атакам и сбоям.

7.2.5 Сценарии реализации угроз

Рассматриваемая сетевая среда часто может характеризоваться определенным сетевым сценарием(ями) и элементом(ами) технологии, которые связаны с четко определенными угрозами, рекомендациями по проектированию и вопросами управления. Такая информация очень полезна при рассмотрении вариантов архитектуры технической безопасности/проекта, а также при выборе и документировании предпочтительного варианта архитектуры технической безопасности/проекта и соответствующих мер обеспечения безопасности.

Такие сценарии упоминаются в ИСО/МЭК 27033-3, и для каждого сценария дается подробное руководство по угрозам безопасности, а также методам проектирования и мерам обеспечения безопасности, необходимым для противодействия этим угрозам.

7.2.6 Модель и структура безопасности сетей

Исторически разработка системы безопасности включает в себя выбор, использование или разработку модели или структуры безопасности.

Модель безопасности используется для описания сущностей (субъектов, регулируемых политикой безопасности организации) и определяет правила доступа, необходимые для реализации указанной политики. Модель безопасности ориентирована на обеспечение конфиденциальности, целостности и доступности информации, причем некоторые из мер обеспечения безопасности определены формально, а другие неформально.

Структуры безопасности обычно способствуют организации в составлении общего представления о том, как сформировать защищенную систему. Примером структуры может служить МСЭ-Т X.805

как всеобъемлющая основа серии рекомендаций МСЭ-Т X.800, которую можно использовать для обеспечения сквозной безопасности сети. С этой целью в МСЭ-Т X.805 определяется концепция измерений защиты, включающих инструментальные средства, технологии, стандарты, правила, процедуры и т.д., которые охватывают различные элементы безопасности. МСЭ-Т X.805 признает, что избыточности средств обеспечения безопасности можно избежать с помощью определения возможностей обеспечения безопасности на одном уровне, которые защищают другой уровень (уровень здесь используется в контексте МСЭ-Т X.805), таким образом, уменьшая общую стоимость решения по обеспечению безопасности. МСЭ-Т X.805 является общей структурой безопасности и поэтому не дает спецификации для какой-либо конкретной информационной системы или компонента. Скорее, он определяет принципы безопасности и целевые возможности обеспечения безопасности, способствующие сквозной безопасности сети. Пример того, как МСЭ-Т X.805 может применяться для поддержки мер обеспечения безопасности ИСО/МЭК 27001, приведен в приложении С.

7.3 Подписание проекта

Завершенный проект безопасности сети должен быть подписан на соответствующих уровнях управления.

8 Реализация

8.1 Введение

Реализацию безопасности сетей следует осуществлять на основе проекта сетевой безопасности, приведенного в разделе 7.

Реализация безопасности сетей состоит из следующего:

- сегментации и разделения;
- критериев выбора компонентов сети;
- критерия выбора продукта или поставщика;
- управления сетью;
- регистрации, мониторинга и реагирования на инциденты;
- документации;
- планов испытаний и проведения испытаний;
- утверждение реализации.

8.2 Критерии выбора компонентов сети

Для каждого проекта безопасной сети существует комбинация общих компонентов, которую можно использовать. Эти компоненты используются в комбинации, что позволит создать технический проект безопасной сети. В оставшейся части раздела 8 и ИСО/МЭК 27033-3 и других стандартах серии ИСО/МЭК 27033 подробно рассматриваются технические подробности некоторых компонентов, перечисленных ниже. Для выполнения требований, приведенных в 6.4, эти компоненты будут использоваться в некоторой комбинации. Некоторые из этих компонентов могут включать в себя следующее:

- сегментации и разделения;
- системы управления безопасностью (например, мониторинг и управление конфигурацией);
- базовые технологии безопасности, такие как управление идентификацией, криптография и т. д.;
- устройства контроля доступа в сеть;
- методы снижения угрозы;
- устройства периметра;
- сетевые фильтры, такие как межсетевые экраны и службы проверки содержимого;
- устройства удаленного доступа;
- системы обнаружения вторжений/системы предотвращения вторжений;
- защита оконечных устройств;
- маршрутизаторы и коммутаторы;
- экстранет-соединения.

8.3 Критерии выбора продукта или поставщика

Выбор конкретного продукта не следует осуществлять отдельно от других средств защиты; это итеративный процесс, связанный с разработкой архитектуры безопасности сетей.

Некоторые примеры того, на чем должен основываться выбор продукта:

- техническая пригодность и достоинства продукта;
- производительность;
- поддержка протоколов;
- устойчивость;
- совместимость;
- расширяемость;
- возможности управления сетью;
- способность проведения аудита;
- соответствие;
- техническая документация;
- обслуживание;
- средства удаленной диагностики;
- безопасность на уровне логики;
- доверие к способности обеспечивать безопасность по результатам оценки по ИСО 15408 (или эквивалентная);
- «характеристики» поставщика (возможности, репутация, приверженность качеству, положение на рынке, размер, общая компетенция, в том числе для рассматриваемых продуктов, организационная/финансовая стабильность, рекомендации и возможности для обучения);
- сроки поставки;
- расходы.

8.4 Управление сетью

Управление сетью — это действия, методы, процедуры и инструментальные средства, которые относятся к эксплуатации, администрированию, обслуживанию и обеспечению сетевых систем, описанным ниже:

- эксплуатация заключается в обеспечении бесперебойной работы сети (и услуг, предоставляемых сетью). Оно включает в себя мониторинг сети для как можно более быстрого выявления проблем, в идеале, до того, как это повлияет на пользователей;
- администрирование заключается в отслеживании ресурсов в сети и того, как они назначаются. Оно включает в себя все средства, которые необходимы, чтобы сеть была управляемой;
- обслуживание связано с выполнением ремонтных работ и обновлений — например, когда необходимо заменить оборудование, когда маршрутизатору требуется обновление безопасности для образа ОС, когда в сеть добавлен новый коммутатор. Обслуживание также включает корректирующие и предупреждающие меры для «лучшей» работы управляемой сети, такие как регулирование параметров конфигурации устройств.

Неверная конфигурация компонентов сети, вызванная преднамеренными или непреднамеренными действиями, создает значительные риски не только в отношении доступности, но также часто и в отношении целостности и конфиденциальности данных.

Поэтому для устранения этих рисков необходимы меры обеспечения безопасности. Такие меры могут быть распределены по категориям организационных или технических мер обеспечения безопасности.

Организационные меры обеспечения безопасности могут включать в себя правильное назначение прав административного персонала, эксплуатационные принципы, такие как принцип «четырех глаз» (для принятия решения требуется одобрение сразу нескольких людей), надлежащее разделение обязанностей, а также процедуры и политики, позволяющие избежать использования нестойких паролей или паролей по умолчанию. Эксплуатационные меры обеспечения безопасности могут включать в себя управление конфигурациями и контроль версий для устранения возможных неправильных настроек или отслеживания изменений в конфигурации устройств.

Технические меры обеспечения безопасности включают в себя использование административных интерфейсов и инструментальных средств, обеспечивающих надлежащее качество и конфиденциальность аутентификации и авторизации. Для ряда компонентов сети требуется техническое управление. Шлюзы безопасности могут управляться локально или удаленно, но при удаленном управлении следует использовать инструменты, которые обеспечивают стойкую или двухфакторную аутентификацию или, по крайней мере, технически исключают нестойкие пароли или пароли по умолчанию и которые

обеспечивают использование везде, где это возможно, адекватных функций по обеспечению целостности и конфиденциальности. Примерами являются использование зашифрованных VPN-туннелей, настроенных с соответствующими уровнями шифрования, или SSH[1)] —эмуляция терминала. Серверы также могут управляться локально или удаленно. Если серверы содержат чувствительную информацию, то при удаленном управлении также следует использовать инструментальные средства, которые обеспечивают стойкую или двухфакторную аутентификацию или, по крайней мере, технически исключают нестойкие пароли или пароли по умолчанию, и которые обеспечивают везде, где это возможно, использование адекватных функций по обеспечению целостности и конфиденциальности.

Компоненты инфраструктуры, такие как коммутаторы и маршрутизаторы, могут управляться локально с консольного порта, удаленно с центральной станции управления, используя программу эмуляции терминала для работы в режиме онлайн на удаленном компьютере или из распределенной системы управления. Однако известно, что используемые при этом протоколы (например, SSH) не являются безопасными, пока они не будут настроены на полное шифрование соединения. Одним из примеров безопасного удаленного соединения, которое может быть полностью зашифровано и включает в себя средство безопасной передачи файлов, является SSH. Кроме того, доступ к компонентам инфраструктуры следует контролировать сервером аутентификации.

Сети, находящиеся на аутсорсинге провайдера, обычно имеют свои собственные системы управления. Однако ими следует управлять с центральной станции управления, используя безопасные методы удаленного управления. Методы удаленного управления должны включать в себя шифрование и аутентификацию с использованием криптографии с открытым ключом. Примерами безопасных методов, которые можно использовать, являются Telnet и TFTP в VPN-туннеле или SSH, который контролируется сервером аутентификации.

Многие организации для непосредственного мониторинга таких сетей используют простой протокол управления сетью (SNMP[2)]). Существуют значительные риски, связанные с SNMP версии 1 и версии 2, которые имеют слабую безопасность или она вовсе отсутствует. Поэтому, если организация решает использовать SNMP, она должна использовать версию 3 с полным набором мер обеспечения безопасности.

8.5 Регистрация, мониторинг и реагирование на инциденты

Сервер аудита должен быть сконфигурирован со всеми шлюзами безопасности, расположенными в ДМЗ, защищенной как от внешней, так и от внутренней сетей, а также от всех других соответствующих устройств безопасности, расположенных внутри или за пределами ДМЗ. Сервер аудита не следует располагать в домене внутренней сети, а непосредственный доступ к нему следует предоставлять назначенному администратору безопасности, ответственному за шлюзы/межсетевые экраны. Однако потребуется право записи для выгрузки журналов регистрации событий с помощью безопасного протокола (например, Secure Copy Protocol, SCP) из компонентов инфраструктуры, серверов и межсетевых экранов. Все журналы регистрации событий МЭ и связанных с ним систем следует направлять на этот сервер аудита для последующего изучения сотрудниками службы безопасности с помощью ПО для анализа журналов регистрации событий.

Управление информацией о безопасности включает в себя сбор и стандартизацию собранной информации, чтобы решения могли приниматься на основе этой информации. Собранная информация может включать в себя системные журналы (syslogs), информацию SNMP, предупреждение об опасности СОВ/СПВ и информацию о потоках данных.

Сервер аудита и/или СОВ/СПВ следует по возможности сконфигурировать для оповещения назначенного сотрудника службы безопасности по электронной почте, СМС или обоими способами в соответствии с уровнем приоритета каждой обнаруженной ненормальной активности. Если обнаружена какая-либо ненормальная активность, которая может представлять собой попытку атаки, то назначенному сотруднику службы безопасности следует реализовать процедуры реагирования на инциденты в соответствии с уровнем приоритета предупреждения об опасности. Управление инцидентами информационной безопасности более подробно описано в ИСО/МЭК 27035.

---

1) *Протокол прикладного уровня для создания «безопасной оболочки» (secure shell).*

2) *Далее по тексту используется сокращение SNMP.*

8.6 Документация

Документ по архитектуре безопасности сетей является одним из важнейших документов технической безопасности и, как указывалось ранее, он должен быть согласован с соответствующими результатами оценки рисков безопасности и анализа процессов управления рисками, политиками безопасности сети и информации организации/сообщества, а также другими соответствующими политиками безопасности. Как и для всей критически важной документации, для этих документов следует осуществлять контроль изменений. Пример шаблона приведен в В.1 приложения В. В нем следует указать ссылку на соответствующую документацию технической архитектуры и другие документы технической безопасности. Основные относящиеся к этому документы включают в себя следующее:

- документацию с требованиями по обеспечению ИБ для всех управляемых компонентов сети (таких как шлюзы, межсетевые экраны, маршрутизаторы и т. д.). Эти требования включают в себя функциональные требования безопасности, такие как требования к базе правил МЭ. Пример шаблона приведен в В.2 приложения В;
- документацию по требованиям к ПО для анализа журналов регистрации событий;
- отчеты об анализе продукта.

8.7 Планы испытаний и проведение испытаний

Для обоснования архитектуры технической безопасности сети следует разработать документ по стратегии тестирования безопасности, описывающий подход, который следует использовать при тестировании. В нем нужно сосредоточиться на том, как следует тестировать основные технические меры обеспечения безопасности для проверки того, что определенные требования безопасности соблюдены, и что политики реализуются надлежащим образом. Для проверки этого проводятся тестирование систем и проверка на основе контрольных списков.

В документ по стратегии тестирования следует включить, например, такую информацию:

- средства идентификации и аутентификации;
- устойчивость проекта;
- средства авторизации;
- реализация мер обеспечения безопасности;
- проверка усиленных ОС;
- проверка журнала регистрации событий.

Чтобы обеспечить пригодность проекта в стратегию тестирования следует включать блочное тестирование и тестирование удобства использования.

Перед проведением тестирования систем следует подготовить план тестирования. В план тестирования следует включать тестовые данные со сценариями тестирования для его подтверждения. В план тестирования следует также включать соответствующий период тестирования. Тестовые данные следует тщательно подготовить, чтобы иметь возможность проверить функциональность технических мер обеспечения безопасности.

8.8 Утверждение

Утверждение завершенной реализации безопасности сети следует проводить на соответствующем уровне управления организации.

Приложение А
(справочное)

Соответствие между мерами обеспечения безопасности сети из ИСО/МЭК 27001:2005 / ИСО/МЭК 27002:2005 и пунктами ИСО/МЭК 27033-2:2012

Пункт ИСО/МЭК 27001:2005/ ИСО/МЭК 27002:2005		Пункт ИСО/МЭК 27033-2:2012
10.6.1 Средства контроля сети	Сети должны быть адекватно управляемыми и контролируемыми в целях защиты от угроз и поддержания безопасности систем и приложений, использующих сеть, включая информацию, передаваемую по сетям	См. ниже в отношении пунктов 10.6.1 IG от a) до e) ИСО/МЭК 27001 / ИСО/МЭК 27002
10.6.1 IG a)	Ответственность за эксплуатацию сети при необходимости должна быть отделена от ответственности за выполнение компьютерных операций	8.3 Управление сетью
10.6.1 IG d)	Следует применять соответствующую регистрацию и мониторинг, чтобы обеспечить запись действий, относящихся к безопасности	8.4 Регистрация и мониторинг
10.6.1 IG e)	Действия управления следует тесно скоординировать как для оптимизации обслуживания организации, так и для обеспечения того, чтобы средства управления последовательно применялись во всей инфраструктуре обработки информации	8.3 Управление сетью
10.6.2 Безопасность сетевых сервисов	Меры обеспечения безопасности, уровни обслуживания для всех сетевых услуг и требования управления должны быть определены и включены в каждый договор о сетевых услугах независимо от того, предоставляются ли эти услуги своими силами или сторонней организацией	6.3 Сбор требований 6.4 Анализ требований
10.8.1 Политики и процедуры обмена информацией	Должны существовать формализованные процедуры, требования и меры контроля, обеспечивающие защиту обмена информацией при использовании связи всех типов	8.5 Документация
11.4.1 Политика в отношении использования сетевых услуг	Пользователям следует предоставлять доступ только к тем услугам, по отношению к которым они специально были авторизованы	8.3 Управление сетью
11.4.2 Аутентификация пользователей для внешних соединений	Для контроля доступа удаленных пользователей должны быть применены соответствующие методы аутентификации	8.3 Управление сетью

Приложение В
(справочное)

Примеры шаблонов документации

В.1 Пример шаблона документа по архитектуре безопасности сети

В.1.1 Введение

Включает такие разделы, как:
- назначение/цели/область применения;
- предположения, как технические, так и иные;
- статус документа;
- структура документа.

В.1.2 Бизнес-требования

Включает такие разделы, как:
- введение;
- контекст (содержание);
- сетевые и другие ИТ-службы.

В.1.3 Техническая архитектура

Включает такие разделы, как:
- введение;
- технический обзор;
  - реферат;
  - основной домен 1;
  - основной домен 2;
  - основной домен 3 и т. д.;
  - серверы;
  - рабочие станции;
  - регистрация;
  - управление;
  - аутентификация и контроль доступа;
  - область действия услуг и устойчивость;
- местоположения систем;
- компоненты систем;
- взаимные соединения;
- компонент 1;
  - обзор;
  - конфигурация;
  - регистрация;
  - управление;
- компонент 2;
  - обзор;
  - конфигурация;
  - регистрация;
  - управление;
- компонент 3;
  - обзор;
  - конфигурация;
  - регистрация;
  - управление;
- компонент «x» и т. д.;
- управление серверами;
  - введение;
  - мониторинг служб;
  - расширенное системное администрирование (XSA);
  - менеджер по безопасности предприятия (ESM);
  - все другие менеджеры;
- межсетевые экраны;
  - введение;
  - обзор;
  - резервное копирование конфигурации МЭ;

- критерии проектирования и конфигурации;
- базы правил;
- управление межсетевыми экранами;
- конфигурация;
- предупреждения об опасности МЭ;
- удаленный доступ;
- регистрация;
- система резервного копирования;
- введение;
- межсетевые экраны;
- серверы;
- приложения;
- сетевые коммуникации;
- локальные сети, например, VLAN, WLAN;
- маршрутизаторы;
- коммутаторы;
- IP-адресация;
- управленческие обязанности;
- серверы;
- межсетевые экраны;
- инфраструктура;
- управление приложениями.

B.1.4 Сетевые службы

Включает такие разделы, как:

- введение;
- службы в местоположении x;
- службы в местоположении y.

Должен быть составлен список всех сетевых служб по местоположению, включая такие как:

- службы KiloStream;
- службы MegaStream;
- службы ретрансляции кадров (frame relay);
- ATM;
- открытый IP/MPLS[1)];
- служба широкополосного доступа;
- Wi-Fi/WiMax;
- службы подключения к локальной сети;
- GSM;
- ISDN первичного уровня (до 30 из 64 кбит/с каналов, предоставаемых через MegaStream);
- интерфейс базового уровня (BRI) ISDN, (2 канала x 64 Кбит/с);
- аналоговые линии прямого обмена (DELs);
- службы интранет/экстранет;
- Интернет-провайдеры (ISPs);

со всеми включенными линиями и услугами.

Если список обширный, то его следует включить в приложение со ссылками на него из основной части документа.

B.1.5 Аппаратное/физическое расположение

Включает такие разделы, как:

- введение;
- место расположения.

Должен быть составлен список всего оборудования с планами этажей и схемами шкафов — по местоположению, включая, например, сегмент размещения серверов, маршрутизаторов, коммутаторов и другого коммуникационного оборудования. Поскольку все аппаратное обеспечение необходимо маркировать, то следует разработать и использовать план маркирования.

В таблице B.1 приведен пример таблицы со списком оборудования. Должна быть составлена таблица для каждого типа оборудования — таблица из примера рассматривает компоненты сервера.

[1)] *Многопротокольная коммутация по меткам (multiprotocol label switching, MPLS).*

Таблица В.1 — Пример таблицы со списком оборудования

Серверный компонент	Оборудование	Программное обеспечение	Комментарий
Наименование и производитель сервера	Номер партии (Part number)	ПО и его версия	При необходимости специальный комментарий, такой как вертикально масштабируемый или кластеризованный

В.1.6 Программное обеспечение

Включает такие разделы, как:

- введение;
- список ПО;
  - ПО в местоположении x;
  - ПО в местоположении y и т. д.;

В список всего ПО, включая номера версий, следует включить следующее:

- ПО Windows;
- МЭ;
- RAS/RADIUS;
- ПО маршрутизаторов;
- ПО коммутаторов;
- ПО прокси-серверов;
- управление аудитом;
- почтовые серверы;
- ретранслятор почты SMTP;
- управление содержанием;
- экранирование апплетов Java/ActiveX;
- веб-серверы;
- FTP-серверы;
- контроллеры доменов;
- ПО резервного копирования;
- другое ПО.

Список должен быть включен в приложение со ссылками на него из основной части документа.

В.1.7 Производительность

Включает детали предполагаемой производительности, включая такие «подсистемы», как:

- настольные компьютеры;
- серверы;
- локальные вычислительные сети (ЛВС);
- глобальная сеть;
- шлюзы;
- внешние службы.

В.1.8 Известные проблемы

Включает подробную информацию об известных проблемах, в том числе в отношении областей несоответствия, под такими заголовками, как технические, физические и относящиеся к среде со следующими разделами:

- введение;
- области несоответствия.

В.1.9 Ссылочные материалы

Включает ссылки на все соответствующие документы, например следующие:

- результаты оценки риска безопасности и анализа со стороны руководства;
- политику сетевой безопасности;
- политику ИБ;
- другие политики безопасности (при их наличии);
- документацию по технической архитектуре;
- документы с требованиями по доступу к службам (безопасности) для каждого МЭ (которые включают базу(ы) правил МЭ);
- документацию с требованиями к ПО анализа журналов (аудита);
- отчеты по анализу продуктов;
- общие планы и стратегии тестирования;
- схему управления инцидентами ИБ;
- действия по обеспечению безопасности;
- условия безопасного подключения к сторонним организациям;
- руководства для пользователей сторонних организаций.

B.1.10 Приложения

Включает такие детали, как:

- аппаратная конфигурация;
- конфигурации сервера/консоли;
- конфигурации МЭ;
- конфигурации маршрутизатора;
- конфигурация ПО;
- конфигурация базы данных;
- план IP-адресации;
- конфигурация SNMP;
- системные ловушки;
- ловушки приложений;
- стандарты.

B.1.11 Глоссарий

B.2 Пример шаблона документа функциональных требований безопасности

Примечание — Для каждой системы МЭ следует разработать свой документ.

B.2.1 Введение

Включает такие разделы, как:

- предыстория/область действия/задачи;
- название системы МЭ;
- расположение МЭ;
- назначение МЭ;
- имя сотрудника/группы, ответственной за работу МЭ;
- запись об изменениях содержания документа;
- ссылки.

B.2.2 Конфигурация МЭ

Включает такие разделы, как:

- введение;
- идентификация каналов связи, проходящих через МЭ;
- обзор архитектуры МЭ;
- подробные сведения о МЭ;
- аппаратные средства;
- ПО;
- архитектура МЭ;
- служба МЭ;
- управление МЭ;
- внутренний маршрутизатор;
- внешний маршрутизатор;
- сетевой концентратор ДМЗ;
- сервер защиты от вредоносного кода;
- почта SMTP;
- веб-страницы;
- почтовый сервер SMTP;
- сервер регистрации (аудита);
- источники бесперебойного питания;
- другие компоненты;
- другие требуемые меры обеспечения безопасности;
- описание входящих и исходящих каналов связи с другими системами;
- виды обрабатываемой информации и их конфиденциальность;
- виды пользователей и их число и т. д.

B.2.3 Риски безопасности

Включает такие разделы, как:

- введение;
- потенциальные неблагоприятные воздействия на деятельность (иногда называемые оценкой активов);
- оценка угроз;
- оценка уязвимостей;
- оценки рисков;
- в контексте использования МЭ.

В.2.4 Управление безопасностью

Включает разделы об ответственности, такие как:

- администратор/группа безопасности;
- сетевой персонал;
- персонал по поддержке МЭ;
- сетевое управление;
- другой персонал по управлению ИТ;
- пользователи.

В.2.5 Администрирование безопасности

Включает такие разделы, как:

- действия по обеспечению безопасности;
- анализ совместимости по требованиям безопасности;
- доступность;
- обслуживание;
- контроль конфигураций;
- управление пропускной способностью;
- управление проблемами;
- управление уровнем служб;
- срок действия документа.

В.2.6 Аутентификация и управление доступом

Включает такие разделы, как:

- введение;
- логическое управление доступом для администраторов МЭ, внутренних и удаленных пользователей;
- меры управления внешним доступом такие, как база правил доступа «сеть-МЭ», безопасная платформа и прокси-серверы приложений;
- защита на уровне сети.

В.2.7 Регистрация (Аудит)

Включает такие разделы, как:

- информация, подлежащая регистрации;
- анализ, который необходимо проводить, и с помощью каких инструментальных средств;
- безопасность.

В.2.8 Управление инцидентами ИБ

Включает такие разделы, относящиеся к регистрации, как:

- введение;
- сообщение об инцидентах;
- обработка инцидентов и т. д.;

В.2.9 Физическая безопасность

Включает разделы по ответственности управления доступом, например, следующие:

- МЭ;
- кабельные соединения.

В.2.10 Безопасность персонала

Включает разделы, относящиеся к персоналу, имеющему отношение к МЭ, в том числе:

- отбор/проверка персонала;
- осведомленность и обучение в области безопасности.

В.2.11 Приложения

Включает подробные сведения о службах и протоколах:

- доступ в и из сети;
- удаленное управление;
- управление МЭ;
- управление сервером в ДМЗ;
- все подробные сведения о соответствующих службах и протоколах.

В.2.12 Глоссарий

Приложение С
(справочное)

Сопоставление архитектуры безопасности МСЭ-Т X.805 и мер обеспечения безопасности ИСО/МЭК 27001:2005

МСЭ-Т X.805 может также использоваться для технического расширения мер обеспечения безопасности ИСО/МЭК 27001. В частности, как показано на рисунке С.1, МСЭ-Т X.805 может дополнять четыре меры обеспечения безопасности в ИСО/МЭК 27001:2005: политика безопасности, управление активами, управление доступом и управление инцидентами ИБ. Специфические для МСЭ-Т X.805 уровни, плоскости и параметры, применимые к каждому из этих мер обеспечения безопасности, изображены на рисунке. Например, для управления активами наиболее применимы уровни инфраструктуры и служб, а также плоскости контроля и управления, при этом наибольшее внимание уделяется параметрам «Контроль доступа» и «Доступность».

Рисунок С.1 — Расширение МСЭ-Т X.805 для мер обеспечения безопасности ИСО/МЭК 27001

Например, расширение может использоваться для систематической оценки и проектирования безопасности для центра обработки данных (ЦОД) предприятия, в котором хранится информация о его сотрудниках, в частности, персональные данные, доступ к которым следует предоставлять только авторизованным пользователям. Информация о сотрудниках доступна нескольким обеспечивающим поддержку организациям, нанятым предприятием, примером которой является служба поддержки. Кроме того, ЦОД и системы, содержащиеся в нем, обслуживаются корпоративной ИТ-организацией. Как видно из рисунка С.2, служба поддержки обращается к информации о сотрудниках для обработки жалоб, поддержки заказов на новые ИТ-услуги, решения проблем сотрудников, возникающих при работе с ИТ-услугами (например, удаленный доступ) и т. д. Кроме этого, корпоративная ИТ-организация обращается к информации о сотрудниках в рамках своей деятельности по сопровождению файловой системы, обновлению системы, управлению обновлениями безопасности (патчами) и т. д.

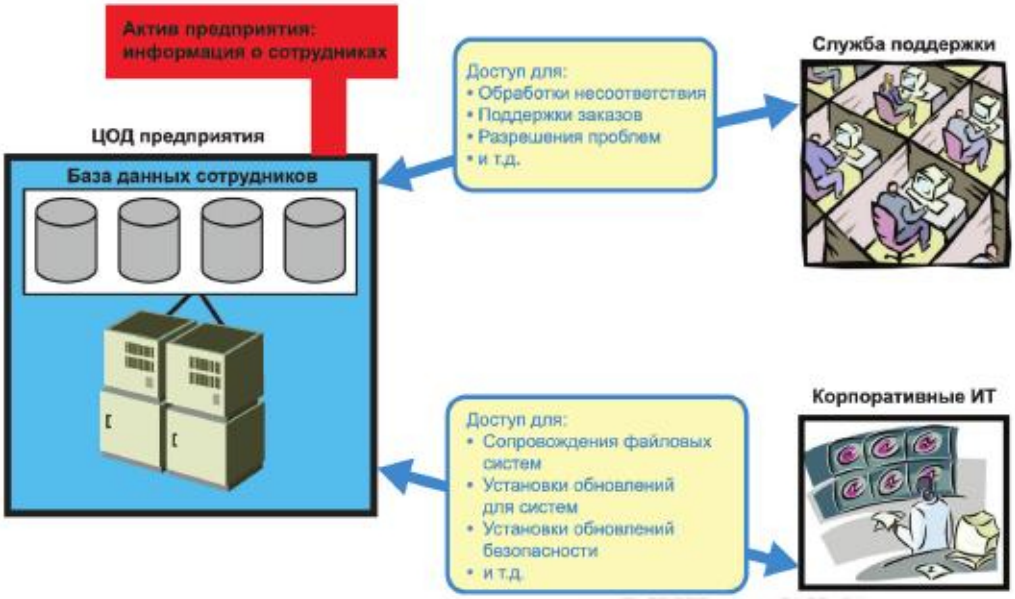

Рисунок С.2 — Сценарий доступа к корпоративному активу

Анализ угроз/уязвимостей МСЭ-Т Х.805 показывает, что члены корпоративной ИТ-организации могут просматривать и изменять информацию о сотрудниках, что делает ее уязвимой для разглашения и искажения на Уровне инфраструктуры (см. Рисунок С.3). Кроме того, в рамках решения проблем информация о сотрудниках передается в открытом виде между ЦОД и службой поддержки, тем самым делая ее уязвимой для разглашения, искажения и перехвата на уровне служб. Таким образом, необходимо определить и выбрать меры обеспечения безопасности для защиты информации о сотрудниках от угроз и уязвимостей в плоскости уровней инфраструктуры управления и службы управления. Следует отметить, что пошаговый анализ МСЭ-Т Х.805 в этом документе не представлен. Для краткости предлагается только результат такого анализа.

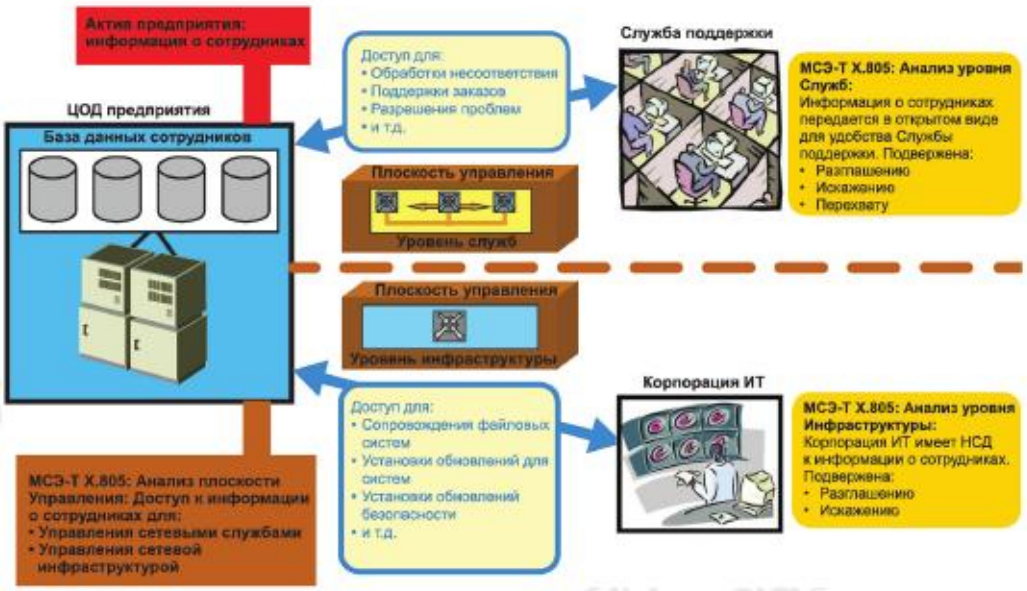

Рисунок С.3 — Результаты анализа угроз и уязвимостей МСЭ-Т X.805 для актива предприятия

Мера обеспечения безопасности А.10.9.2 ИСО/МЭК 27001 идентифицирована и выбрана как необходимая для защиты управления информацией о сотрудниках на уровнях инфраструктуры управления и службы управления из-за уязвимостей и угроз, выявленных там в результате анализа МСЭ-Т X.805 (рисунок С.4). В мере обеспечения безопасности А.10.9.2 ИСО/МЭК 27001 утверждается, что информация, участвующая в онлайн-транзакциях, должна быть защищена для предотвращения неполной передачи, неправильной маршрутизации, несанкционированного изменения сообщения, несанкционированного разглашения, несанкционированного дублирования или повторной передачи сообщения.

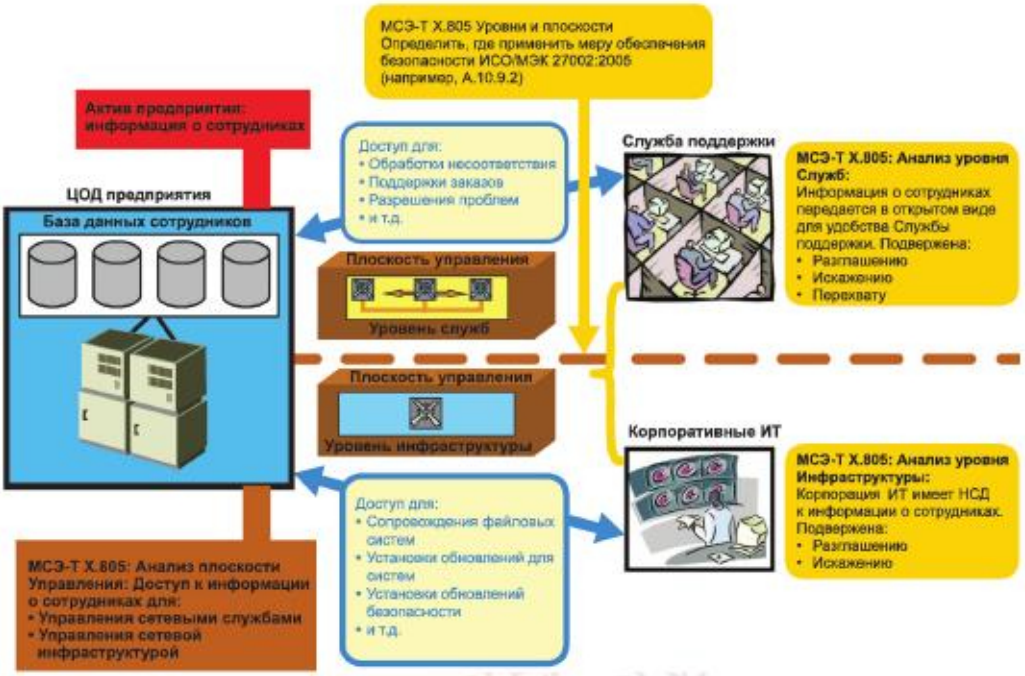

Рисунок С.4 — Меры обеспечения безопасности ИСО/МЭК 27001:2005

Параметры МСЭ-Т X.805 предоставляют подробные сведения о реализации и работе меры обеспечения безопасности A.10.9.2 на уровнях службы и инфраструктуры для информационного актива о сотрудниках. На уровне службы параметр «Безопасность связи» предусматривает использование VPN для предотвращения неправильной маршрутизации. Параметр «Целостность» данных предусматривает использование IPSec AH для предотвращения неполной передачи, несанкционированного изменения и повторной отправки сообщений, а также предотвращения повторной передачи сообщений. Параметр «Конфиденциальность» данных предусматривает использование IPSec ESP для предотвращения несанкционированного разглашения. На уровне инфраструктуры параметр «Целостность» данных обеспечивает использование контрольных сумм файлов для предотвращения несанкционированного изменения, параметр «Конфиденциальность» данных обеспечивает шифрование файлов, а параметр «Контроль доступа» предусматривает использование ACL к файловой системе для предотвращения несанкционированного копирования. На рисунке С.5 показано, как параметры МСЭ-Т X.805 обеспечивают реализацию и эксплуатацию меры обеспечения безопасности A.10.9.2 для защиты информационного актива о сотрудниках.

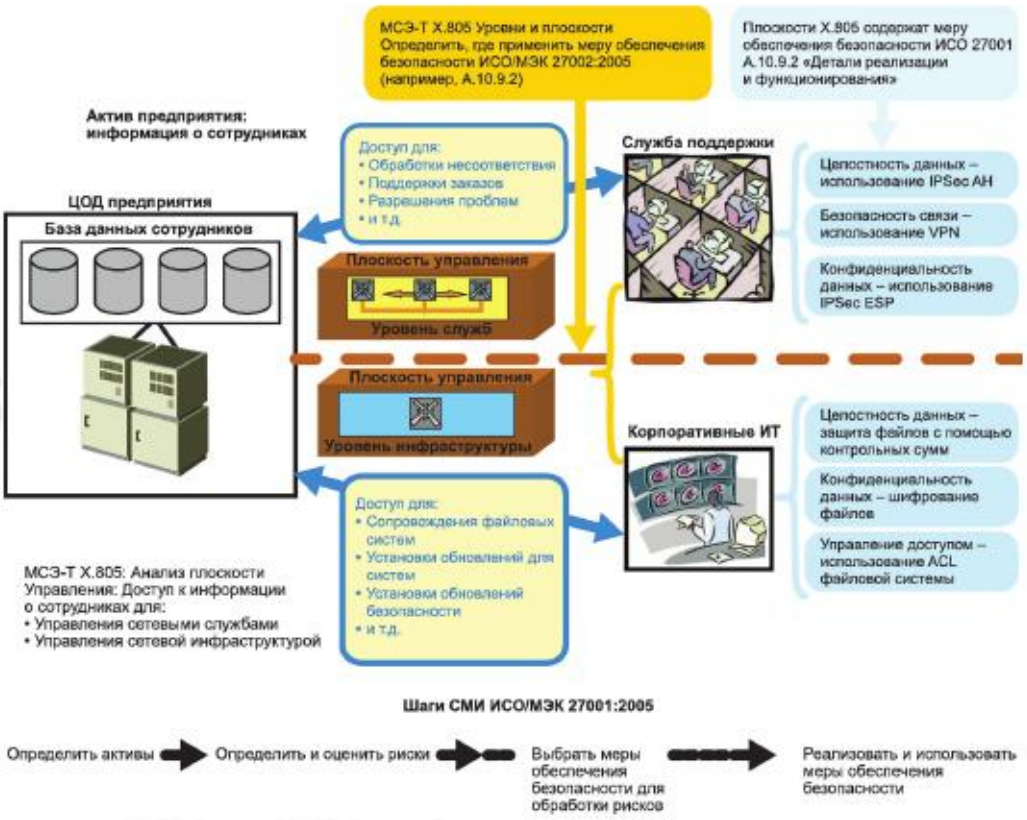

Рисунок С.5 — МСЭ-Т X.805 для реализации ИСО/МЭК 27001

Приложение ДА
(справочное)

Сведения о соответствии ссылочных международных стандартов национальным стандартам

Таблица ДА.1

Обозначение ссылочного международного стандарта	Степень соответствия	Обозначение и наименование соответствующего национального стандарта
ISO/IEC 7498 (all parts)	IDT	ГОСТ Р ИСО/МЭК 7498-1—99 «Информационная технология. Взаимосвязь открытых систем. Базовая эталонная модель. Часть 1. Базовая модель»; ГОСТ Р ИСО 7498-2—99«Информационная технология. Взаимосвязь открытых систем. Базовая эталонная модель. Часть 2. Архитектура защиты информации»; ГОСТ Р ИСО 7498-3—97 «Информационная технология. Взаимосвязь открытых систем. Базовая эталонная модель. Часть 3. Присвоение имен и адресация»; ГОСТ Р ИСО/МЭК 7498-4—99 «Информационная технология. Взаимосвязь открытых систем. Базовая эталонная модель. Часть 4. Основы административного управления»
ISO/IEC 27001:2005	IDT	ГОСТ Р ИСО/МЭК 27001—2006 «Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования»
ISO/IEC 27002:2005	IDT	ГОСТ Р ИСО/МЭК 27002—2012 «Информационная технология. Методы и средства обеспечения безопасности. Свод норм и правил менеджмента информационной безопасности»
ISO/IEC 27005: 2011	—	*
ISO/IEC 27033-1:2009	IDT	ГОСТ Р ИСО/МЭК 27033-1—2011 «Информационная технология. Методы и средства обеспечения безопасности. Безопасность сетей. Часть 1. Обзор и концепции»

* Соответствующий национальный стандарт отсутствует. До его принятия рекомендуется использовать перевод на русский язык данного международного стандарта.

Примечание — В настоящей таблице использовано следующее условное обозначение степени соответствия стандартов:

- IDT — идентичные стандарты.

Библиография

[1] ITU-T X.805, Security architecture for systems providing end-to-end communications

[2] RFC 5246, The Transport Layer Security (TLS) Protocol Version 1.2, IETF, August 2008

УДК 006.354:004.056.5:006.354 ОКС 35.040

Ключевые слова: методы и средства обеспечения безопасности, безопасность сетей, обмен данными в сетях, шлюзы безопасности, межсетевой экран

Технический редактор *И.Е. Черепкова*
Корректор *Е.Ю. Митрофанова*
Компьютерная верстка *Е.А. Кондрашовой*

Сдано в набор 19.05.2021. Подписано в печать 02.06.2021. Формат 60×84⅛. Гарнитура Ариал.
Усл. печ. л. 3,26. Уч.-изд. л. 2,95.

Подготовлено на основе электронной версии, предоставленной разработчиком стандарта

Создано в единичном исполнении во ФГУП «СТАНДАРТИНФОРМ»
для комплектования Федерального информационного фонда стандартов,
117418 Москва, Нахимовский пр-т, д. 31, к. 2.
www.gostinfo.ru info@gostinfo.ru