ФЕДЕРАЛЬНОЕ АГЕНТСТВО

ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

ГОСТ Р ИСО/МЭК 27033-3— 2014

Информационная технология

МЕТОДЫ И СРЕДСТВА ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ

Безопасность сетей

Часть 3

Эталонные сетевые сценарии. Угрозы, методы проектирования и вопросы управления

(ISO/IEC 27033-3:2010, IDT)

Издание официальное

Москва
Стандартинформ
2019

gost.e-ecolog.ru

Предисловие

1 ПОДГОТОВЛЕН Обществом с ограниченной ответственностью «Информационно-аналитический вычислительный центр» (ООО «ИАВЦ») и Обществом с ограниченной ответственностью «Научно-производственная фирма «Кристалл» (ООО «НПФ «Кристалл») 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 9 сентября 2014 г. № 1029-ст

4 Настоящий стандарт идентичен международному стандарту ИСО/МЭК 27033-3:2010 «Информационная технология. Методы и средства обеспечения безопасности. Безопасность сетей. Часть 3. Эталонные сетевые сценарии. Угрозы, методы проектирования и вопросы управления» (ISO/IEC 27033-3:2010 «Information technology — Security techniques — Network security — Part 3: Reference networking scenarios — Threats, design techniques and control issues», IDT).

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

5 ВВЕДЕН ВПЕРВЫЕ

6 ПЕРЕИЗДАНИЕ. Январь 2019 г.

*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 (*gost.e-ecolog.ru

© ISO, 2010 — Все права сохраняются
© Стандартинформ, оформление, 2014, 2019

Настоящий стандарт не может быть полностью или частично воспроизведен, тиражирован и распространен в качестве официального издания без разрешения Федерального агентства по техническому регулированию и метрологии

Содержание

1 Область применения 1
2 Нормативные ссылки 1
3 Термины и определения 2
4 Обозначения и сокращения 2
5 Структура 3
6 Обзор 4
7 Услуги доступа к Интернету для сотрудников 6
7.1 Исходные данные 6
7.2 Угрозы безопасности 7
7.3 Методы проектирования безопасности и мер и средств контроля и управления 8
8 Услуги бизнес-бизнес 9
8.1 Исходные данные 9
8.2 Угрозы безопасности 10
8.3 Методы проектирования безопасности и меры и средства контроля и управления 10
9 Услуги бизнес-клиент 11
9.1 Исходные данные 11
9.2 Угрозы безопасности 11
9.3 Методы проектирования безопасности и меры и средства контроля и управления 12
10 Расширенное применение услуг для совместного использования 13
10.1 Исходные данные 13
10.2 Угрозы безопасности 14
10.3 Методы проектирования безопасности и меры и средства контроля и управления 14
11 Сегментация сети 15
11.1 Исходные данные 15
11.2 Угрозы безопасности 15
11.3 Методы проектирования безопасности и меры и средства контроля и управления 16
12 Сетевая поддержка работы на дому или в малых предприятиях 16
12.1 Исходные данные 16
12.2 Угрозы безопасности 16
12.3 Методы проектирования безопасности и меры и средства контроля и управления 17
13 Мобильная связь 18
13.1 Исходные данные 18
13.2 Угрозы безопасности 18
13.3 Методы проектирования безопасности и меры и средства контроля и управления 19
14 Сетевая поддержка мобильных пользователей 20
14.1 Исходные данные 20
14.2 Угрозы безопасности 21
14.3 Методы проектирования безопасности и меры и средства контроля и управления 21
15 Услуги аутсорсинга 21
15.1 Исходные данные 21
15.2 Угрозы безопасности 22
15.3 Методы проектирования безопасности и меры и средства контроля и управления 22
Приложение А (справочное) Пример политики использования объединенной сети 24
Приложение В (справочное) Каталог угроз 28
Приложение ДА (справочное) Сведения о соответствии ссылочных международных стандартов национальным стандартам 32

Введение

ИСО/МЭК 27033-3 был подготовлен совместным Техническим комитетом ИСО/МЭК СТК 1, «Информационная технология», Подкомитетом ПК 27, «Методы и средства обеспечения безопасности ИТ».

ИСО/МЭК 27033 состоит из следующих частей, под общим наименованием «Информационная технология. Методы и средства обеспечения безопасности. Безопасность сетей»:

- Часть 1: Обзор и концепции;
- Часть 2: Рекомендации по проектированию и реализации безопасности сети;
- Часть 3: Эталонные сетевые сценарии. Угрозы, методы проектирования и вопросы управления.

Следующие части находятся в процессе подготовки:

- Часть 4: Обеспечение безопасности межсетевых соединений с применением шлюзов безопасности. Угрозы, методы проектирования и вопросы, касающиеся мер и средств контроля и управления;
- Часть 5: Обеспечение безопасности виртуальных частных сетей. Угрозы, методы проектирования и вопросы, касающиеся мер и средств контроля и управления.

Могут быть выпущены очередные части стандарта для охвата таких тем, как: локальные вычислительные сети, глобальные сети, беспроводные и радиосети, широкополосные сети, сети телефонной связи, сети IP-конвергенции (данные, голос, видео), архитектуры веб-хоста, архитектуры электронной почты Интернета (в том числе исходящий онлайновый доступ к Интернету и входящий доступ из Интернета) и отсортированный доступ к сторонним организациям.

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

Информационная технология

МЕТОДЫ И СРЕДСТВА ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ

Безопасность сетей

Часть 3

Эталонные сетевые сценарии. Угрозы, методы проектирования и вопросы управления

Information technology. Security techniques. Network security. Part 3. Reference networking scenarios. Threats, design techniques and control issues

Дата введения — 2015—11—01

1 Область применения

В настоящем стандарте изложены угрозы, методы проектирования и вопросы, касающиеся мер и средств контроля и управления, связанные с типовыми сетевыми сценариями. Для каждого сценария в ней представлены подробные руководства по угрозам безопасности, методам проектирования безопасности и мерам и средствам контроля и управления, требуемым для уменьшения связанных рисков.

Информация, содержащаяся в настоящем стандарте, предназначена для использования при пересмотре технической архитектуры/вариантов проектирования безопасности, а также при выборе и документировании предпочтительной технической архитектуры/проектирования безопасности и связанных с ними мер и средств контроля и управления, в соответствии с ИСО/МЭК 27033-2.

Выбор конкретной информации (наряду с информацией, взятой из ИСО/МЭК 27033-4 — ИСО/МЭК 27033-6) будет зависеть от анализа характеристик сетевой среды, т. е. конкретного сценария сети(ей) и «технического решения» вопросов, имеющих к этому отношение.

В целом, настоящая часть ИСО/МЭК 27033 будет способствовать всестороннему определению и реализации безопасности для сетевой среды любой организации.

2 Нормативные ссылки

В настоящем стандарте использованы нормативные ссылки на следующие международные стандарты. Для датированных ссылок используют только указанное издание. Для недатированных — последнее издание ссылочного стандарта (с учетом всех его изменений).

ISO/IEC 27000, Information technology — Security techniques — Information security management systems — Overview and vocabulary (Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Обзор и терминология)

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

Издание официальное

3 Термины и определения

В настоящем стандарте применены термины по ИСО/МЭК 27000 и ИСО/МЭК 27033-1, а также следующие термины с соответствующими определениями:

3.1 **вредоносная программа** (malware, malicious software): Категория программы, разработанной со злым умыслом, содержащей функции и возможности, которые потенциально могут прямо или косвенно причинить вред пользователю и (или) компьютерной системе пользователя.

Примечание — См. ИСО/МЭК 27032.

3.2 **непрозрачность** (opacity): Защита от выделения информации, которая может быть получена посредством наблюдения за сетевой деятельностью, такой как адреса конечных точек обмена голосовым трафиком по сети Интернет.

Примечание — Непрозрачность касается необходимости защиты операций с информацией в дополнение к защите самой информации.

3.3 **аутсорсинг** (outsourcing): Приобретение покупателем услуг для выполнения деятельности, требуемой для поддержки функций бизнеса покупателя.

3.4 **социальная инженерия** (social engineering): Действие по манипулированию людьми в совершении действий или разглашении конфиденциальной информации.

4 Обозначения и сокращения

В настоящем стандарте применены следующие сокращения и условные обозначения:

AAA — аутентификация, санкционирование и учет (authentication, authorization and accounting);

DHCP — протокол динамического конфигурирования хоста[1)] (dynamic host configuration protocol);

DNS — служба доменных имен (domain name service);

DNSSEC — расширение безопасности службы доменных имен (DNS Security extensions);

DoS — отказ в обслуживании (denial of service);

FTP — протокол передачи файлов (file transfer protocol);

IDS — система обнаружения вторжений (intrusion detection system);

IP — Интернет-протокол (Internet protocol);

IPSec — протокол безопасности Интернет-протокола (IP security protocol);

OAM&P — эксплуатация, администрирование, техническое обслуживание и обеспечение (operations, administration, maintenance & provisioning);

PDA — персональное информационное устройство (personal data assistant);

QoS — качество обслуживания (quality of service);

SIP — протокол инициации сеанса (session initiation protocol);

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

SNMP — простой протокол сетевого управления (simple network management protocol);

SSL — протокол безопасных соединений (протокол шифрования и аутентификации) (secure socket layer (encryption and authentication protocol));

VoIP — передача голоса по Интернет-протоколу (voice over Internet Protocol);

VPN — виртуальная частная сеть (virtual private network);

ВОС — взаимодействие открытых систем (open systems interconnection — OSI);

ТфОП — телефонная коммутируемая сеть общего пользования (public switched telephone network — PSTN).

[1)] Хост — Любое устройство, подключенное к сети и использующее протоколы TCP/IP.

5 Структура

Структура настоящего стандарта состоит из:

- краткого обзора подхода к решению проблемы безопасности для каждого типового сценария, перечисленного в настоящем стандарте (раздел 6);
- раздел для каждого базового сценария (разделы 7—15), в котором описываются:
  - угрозы для базового сценария;
  - представление мер и средств контроля и управления безопасности и методы, основанные на подходе, изложенном в разделе 6.

Сценарии в настоящем документе упорядочены в представленную ниже структуру, цель которой заключается в оценивании данного сценария в зависимости от:

- **типа доступа пользователя**, является ли пользователь работающим внутри предприятия или пользователем является сотрудник, который получает доступ к корпоративным ресурсам извне, или пользователь является клиентом, поставщиком или деловым партнером;
- **типа доступности информационных ресурсов**, открытые, ограниченные или внешние ресурсы.

Таким образом, структура помогает представить согласованную систему и делает добавление новых сценариев управляемым, а также обосновывает необходимость различных сценариев, представленных в настоящем стандарте.

Таблица 1 — Структура упорядочения сетевых сценариев

<table>
<tr><td colspan="2" rowspan="2"></td><td colspan="3">Пользователи</td></tr>
<tr><td>внутренние</td><td>сотрудники, работающие вне предприятия</td><td>внешние</td></tr>
<tr><td rowspan="6">Доступность информационных ресурсов</td><td rowspan="2">открытые</td><td>- услуги доступа к Интернету для сотрудников</td><td rowspan="2"></td><td rowspan="2">- услуги бизнес-клиент</td></tr>
<tr><td>- услуги бизнес-бизнес</td></tr>
<tr><td rowspan="4">ограниченные</td><td>- расширенное применение услуг для совместного использования</td><td>- мобильная связь</td><td>- расширенное применение услуг для совместного использования</td></tr>
<tr><td>- услуги бизнес-бизнес</td><td>- сетевая поддержка мобильных пользователей</td><td>- услуги бизнес-бизнес</td></tr>
<tr><td>- сегментация сети</td><td></td><td>- услуги бизнес-клиент</td></tr>
<tr><td>- сетевая поддержка работы на дому или в малых предприятиях</td><td></td><td></td></tr>
<tr><td>внешние</td><td>- услуги аутсорсинга</td><td></td><td>- услуги аутсорсинга</td></tr>
</table>

Таким образом, порядок, в котором сценарии перечислены в настоящем стандарте, является следующим:

- услуги доступа к Интернету для сотрудников (раздел 7);
- услуги бизнес-бизнес (раздел 8);
- услуги бизнес-клиент (раздел 9);
- расширенное применение услуг для совместного использования (раздел 10);
- сегментация сети (раздел 11);
- сетевая поддержка работы на дому или в малых предприятиях (раздел 12);
- мобильная связь (раздел 13);
- сетевая поддержка мобильных пользователей (раздел 14);
- услуги аутсорсинга (раздел 15).

6 Обзор

Руководства, представленные в настоящем стандарте для каждого из определенных типовых сетевых сценариев, основаны на нижеперечисленных подходах:

- проверка вводной информации и рамок сценария;
- описание угроз, соответствующих сценарию;
- проведение анализа риска относительно обнаруженных уязвимостей;
- анализ влияния на бизнес рассматриваемых уязвимостей;
- определение рекомендаций по реализации обеспечения безопасности сети.

В целях решения вопросов безопасности любой сети, желательным является систематическое и всеобъемлющее оценивание. Сложность подобного анализа зависит от характера и размера сети в области действия. Тем не менее, последовательная методика очень важна для менеджмента безопасности, особенно в связи с развивающимся характером технологий.

Первым рассмотрением при оценке безопасности является определение активов, нуждающихся в защите. Они могут быть в значительной степени категоризированы на активы инфраструктуры, услуг или приложений. Предприятие может выбрать и определить свои собственные категории, но такое различие важно, поскольку подверженность угрозам и атакам является уникальной для каждой категории или типа активов. Например, если маршрутизатор относится к категории активов инфраструктуры, а передача голоса по IP рассматривается как услуга конечного пользователя, то атака «отказ в обслуживании» (DoS) в каждом случае потребует различного рассмотрения. В частности, маршрутизатор нуждается в защите от лавинного распространения фиктивных пакетов на физический порт маршрутизатора, которые могут помешать или воспрепятствовать прохождению легитимного трафика. Аналогично, услуга передачи голоса по IP (VoIP) нуждается в защите информации учетной записи абонента/услуги от удаления или повреждения, исходя из условия, что доступ к услуге для законного пользователя не был предотвращен.

Безопасность сети также предполагает защиту различных деятельностей, поддерживаемых в сети, таких как, управленческая деятельность, а также сигналы управления/оповещения, и данные (резидентные и передаваемые) конечных пользователей. Например, управление GUI[1)] может быть предметом раскрытия в результате несанкционированного доступа (простой для отгадывания пароль и идентификатор администратора). Управление трафиком само является предметом искажения в результате ложных команд OA&M[2)] с ложными IP адресами операционных систем, или раскрытия путем пассивного прослушивания сети или прерывания в результате атаки лавинного распространения пакетов.

Такой подход к определению активов и деятельностей делает возможным модульное и систематическое рассмотрение угроз. Каждый типовой сетевой сценарий исследуется в отношении известного набора угроз для выяснения того, какие угрозы являются применимыми. В приложении В приведен перечень известных отраслевых угроз. Хотя этот перечень не следует рассматривать как исчерпывающий, он служит отправной точкой для любого анализа. Как только выводится профиль угрозы сети, анализируются уязвимости, чтобы определить, каким образом угрозы могут быть реализованы в контексте конкретного рассматриваемого актива. Такой анализ поможет определить, какие ограничения отсутствуют, и какие контрмеры требуется применить для достижения целей защиты. Контрмеры снизят вероятность того, что угроза будет успешной и (или) ослабят ее воздействие. При анализе риска исследуется риск, соответствующий обнаруженным уязвимостям. Анализ влияния на бизнес заключается в принятии решения о том, какие меры принимать по каждой уязвимости: меры по исправлению, принятию риска или переносу риска.

Проектирование контрмер и реализация мер и средств контроля и управления, защищающих слабые места активов от угроз, является частью любой методики оценки безопасности. В соответствии с требованиями стандартов серии ИСО/МЭК 27000 отбор и реализация соответствующих мер и средств контроля и управления имеет решающее значение для защиты активов/информации. Стандарт требует сохранения конфиденциальности, целостности и доступности информации, и дополнительно он затрагивает и другие свойства, такие как подлинность, неотказуемость и достоверность.

---

1) GUI (Graphical User Interface) — Графический интерфейс пользователя.

2) OA&M (operations, administration and management) — Пакет прикладных программ по эксплуатации, администрированию и управлению сети.

Ниже перечислены свойства безопасности, которые используются в настоящем стандарте для совершенствования сдерживающих мер и контрмер объективным способом. Уточнения, касающиеся каждого свойства безопасности (в дополнение к конфиденциальности, целостности и доступности), описываются ниже:

- конфиденциальность связана с защитой данных от несанкционированного раскрытия;
- целостность связана с сохранением правильности или точности данных и защитой от несанкционированного изменения, удаления, создания и тиражирования;
- доступность связана с обеспечением уверенности в том, что не существует отказа в санкционированном доступе к элементам сети, хранимой информации, информационным потокам, услугам и приложениям;
- управление доступом обеспечивает, с помощью аутентификации и авторизации, управление доступом к сетевым устройствам и услугам, а также обеспечивает уверенность в том, что только уполномоченному персоналу или устройствам разрешен доступ к элементам сети, хранимой информации, информационным потокам, услугам и приложениям. Например, при использовании IPTV[1)] одна из известных рекомендаций по безопасности — отключение интерфейса отладки на абонентском комплекте приставки — получена исходя из рассмотрения свойств элемента управления доступом. Анализ конфиденциальности, целостности или доступности не приведет к каким-либо другим рекомендациям;
- аутентификация связана с подтверждением или доказательством заявленной идентичности пользователя или взаимодействующих сторон при использовании управления доступом для авторизации, а также она обеспечивает уверенность в том, что сущность не пытается имитировать или несанкционированно воспроизводить предыдущее сообщение. Например, человек может получить доступ к системе управления сетью, но потребуется осуществить аутентификацию для обновления записей абонентских услуг. Таким образом, возможность осуществления деятельности по управлению сетью не может быть обеспечена посредством простого рассмотрения конфиденциальности, целостности, доступности или управления доступом.

Примечание — В управлении доступом, основанном на ролях, авторизация осуществляется в отношении пользователя, назначенного на роль. Также в процессе управления доступом до предоставления доступа проверяется роль, назначенная пользователю. Кроме того, по спискам управления доступом доступ предоставляется всем, кто удовлетворяет политике, таким образом, если вы удовлетворяете требованиям политики, вы имеете право доступа. В этом случае функции аутентификации и авторизации являются несущественными;

- безопасность связи и безопасность передачи информации касается обеспечения уверенности в том, что информация только перемещается между авторизованными конечными точками без перенаправления и перехватов;
- неотказуемость связана с поддержанием контрольных записей с тем, чтобы не могло быть отказано в информации об исходных данных, причинах события или действия. Определение авторизованного лица, которое осуществило несанкционированное действие с защищенными данными, не связано с конфиденциальностью, целостностью, доступностью данных;
- непрозрачность связана с защитой информации, которая может быть получена из наблюдений за сетевой активностью. Непрозрачность признает необходимость защиты действий в дополнение к информации. Защита информации решается путем обеспечения конфиденциальности. Защита телефонного разговора между лицом А и лицом Б защищает их конфиденциальность. Защита того факта, что лицо А и лицо Б вели телефонный разговор, обеспечивает уверенность в непрозрачности.

Для всех сценариев, описанных в настоящем стандарте, вышеуказанные свойства безопасности рассматриваются как часть методики проектирования безопасности и фазы контроля. В таблице 2 приведены примеры механизмов обеспечения безопасности сети, которые могут быть реализованы для обеспечения свойств безопасности, выбранных для уменьшения потенциального риска.

[1)] IPTV (Internet Protocol Television) — Передача цифрового телевизионного сигнала по протоколу IP.

Таблица 2 — Примеры методов обеспечения безопасности сети

Рассмотрения безопасности	Механизмы/методы обеспечения безопасности
Управление доступом	Система пропусков (идентификационных карточек), списки управления доступом (ACL — Access Control List), разделение обязанностей
Аутентификация	Несложная регистрация входа в систему/пароль, цифровые сертификаты, цифровые подписи, TLS[1] версии 1.2, SSO[2], CHAP[3]
Доступность	Избыточность и резервное копирование, межсетевые экраны, IDS/IPS[4] (для блокирования атаки DoS), непрерывность бизнеса, сетевой менеджмент и менеджмент услуг с SLAs[5]
Безопасность связи	IPSec/L2TP[6], частные линии связи, обособленные сети
Конфиденциальность	Шифрование (3DES[7], AES[8]), списки управления доступом, права доступа к файлам
Целостность	IPSec HMACs[9] (например, SHA[10]-256), циклический избыточный контроль, антивирусное программное средство
Неотказуемость	Регистрация событий, управление доступом, основанное на ролях, и цифровые подписи
Непрозрачность	Шифрование IP-заголовков (например, VPN с режимом туннелирования IP-Sec, NAT[11] (для IP версии 4)

В настоящей части стандарта ИСО/МЭК 27033, все рассмотренное выше является неотъемлемой частью проектирования и реализации, обсуждаемых в контексте каждого типового сетевого сценария. Как правило, для удовлетворения своих целей бизнеса организация выбирает меры и средства контроля и управления, соответствующие ИСО/МЭК 27002, а также рекомендации настоящей части стандарта ИСО/МЭК 27033, предназначенные для обеспечения анализа сетевого уровня, необходимого для реализации выбранных мер и средств контроля и управления.

7 Услуги доступа к Интернету для сотрудников

7.1 Исходные данные

Организации, которые должны предоставлять услуги доступа к Интернету для своих сотрудников, должны продумать этот сценарий, чтобы обеспечить уверенность в том, что осуществляется доступ с четко определенными и санкционированными целями, а не общий открытый доступ. Организации должны быть обеспокоены вопросами управления доступом, чтобы избежать потери пропускной способности сети и способности к реагированию, а также привлечения к правовой ответственности сотрудников, имеющих неконтролируемый доступ к услугам Интернета.

---

[1] TLS (Transport Layer Security) — Протокол безопасности транспортного уровня.

[2] SSO (Single Sign On) — Технология единого входа [в систему].

[3] CHAP (Challenge Handshake Authentication Protocol) — Протокол взаимной аутентификации.

[4] IPS (Intrusion Prevention System) — Система предотвращения вторжения.

[5] SLA (Service Level Agreement) — Соглашение об уровне услуг.

[6] L2TP (Layer 2 Tunneling Protocol) — Протокол туннелирования второго уровня.

[7] 3DES (Triple Data Encryption Standard) — Протокол тройного шифрования.

[8] AES (Advanced Encryption Standard) — Улучшенный протокол шифрования.

[9] HMAC (Hash-based Message Authentication Code) — Механизм, использующий криптографические хеш-функции в сочетании с секретным ключом.

[10] SHA (Secure Hash Algorithm) — Алгоритм аутентификации и проверки целостности информации.

[11] NAT (Network Address Translation) — Протокол преобразования сетевых адресов.

Управление доступом сотрудников к Интернету вызывает растущее беспокойство, учитывая количество появляющихся судебных прецедентов связанных с Интернетом. Таким образом, организация несет ответственность за установление, мониторинг и претворение в жизнь точно выраженной политики использования Интернета посредством оценивания следующих сценариев и обеспечения соответствующих требований в политике:

- доступ к Интернету предоставлен в интересах бизнеса;
- если доступ к Интернету также разрешен (ограниченно) в личных целях, то какими услугами разрешено пользоваться;
- разрешено ли расширенное применение услуг для совместного использования;
- разрешено ли сотрудникам участвовать в чате, форумах и т. д.

Хотя, зачастую, написанная политика выступает как существенный сдерживающий фактор неприемлемого использования Интернета, организация все еще подвергается значительным рискам информационной безопасности. Угрозы безопасности, рекомендации по методам проектирования безопасности, а также меры и средства контроля и управления, направленные на уменьшение рисков безопасности, излагаются в нижеследующих пунктах, как только для внутреннего, так и для внутреннего и внешнего использования.

7.2 Угрозы безопасности

Угрозами безопасности, связанными с услугами доступа к Интернету для сотрудников, являются:

- вирусные атаки и внедрение вредоносных программ:
- сотрудники, пользующиеся Интернетом, являются также основной мишенью для вредоносных программ, которые могут привести к потере или повреждению информации, потере контроля над инфраструктурой информационных технологий и огромному риску для безопасности сети организации,
- загружаемые пользователем файлы или программы могут содержать вредоносные программные коды. Учитывая повсеместное использование таких приложений, как обмен мгновенными сообщениями, одноранговое совместное использование файлов и IP-телефония, сотрудники могут случайно загрузить и установить вредоносные приложения, которые обходят защиту сети, используя такие методы, как быстрота прохождения порта (скачкообразность вблизи открытых портов), и шифрование. Кроме того, одноранговые приложения могут быть использованы в качестве скрытых каналов для сетевых агентов-роботов,
- уязвимости веб-браузеров или других веб-приложений могут быть использованы вредоносными программами, что приведет к заражению вирусом и установке троянов («Троянских коней»). После заражения доступность может серьезно пострадать из-за распространения деятельности вируса, приводящего к перегрузке сети. Трояны могут разрешать несанкционированный внешний доступ, приводящий к нарушению конфиденциальности;
- утечка информации:
- приложения, позволяющие пересылать информацию на веб-серверы, могут быть причиной неконтролируемой передачи данных из организации через Интернет. Если используются зашифрованные сеансы (например, TLS), то даже регистрация такой деятельности может оказаться невозможной. Подобные риски безопасности привносятся в тех случаях, когда недостоверный переносимый код выполняется на системах внутри организации;
- несанкционированное использование и доступ:
- потеря мер и средств контроля и управления инфраструктуры, систем и приложений может привести к мошенничеству, отказу в обслуживании, а также злоупотреблению возможностями;
- ответственность за несоблюдение нормативов:
- юридическая ответственность за несоблюдение законодательства и нормативных обязательств,
- несогласованность с используемой политикой организации может привести к нормативному несоответствию;
- снижение доступности сети связи, вызванное недостаточной пропускной способностью или стабильными проблемами:
- чрезмерное использование услуг, связанных с пропускной способностью, например, потоковые мультимедийные средства или одноранговое совместное использование файлов может привести к перегрузке сети.

7.3 Методы проектирования безопасности и мер и средств контроля и управления

Методы проектирования безопасности и меры и средства контроля и управления, связанные с сотрудниками, рассматриваются в таблице 3.

Для установленной угрозы безопасности, каждое свойство безопасности рассматривается для применения с целью снижения риска, во втором столбце приведен соответствующий пример технической реализации. Например, целостность, контроль доступа и аутентификация применяются для защиты от вредоносного программного кода.

Таблица 3 — Меры и средства контроля и управления безопасности для сценария доступа сотрудников к Интернету

Применяемые свойства безопасности для идентифицированных угроз	Реализуемые проекты и методы
Вирусные атаки и введение вредоносных программ	
- Целостность - Управление доступом - Аутентификация	- Предоставление сотрудникам Интернет-услуг, только соответствующих бизнесу. Использование черных списков авторизованных услуг, чтобы сделать возможной поправку в каналах чата, услугах веб-почты или одноранговых сетевых протоколах. - Использование антивирусных программ на пути доступа к Интернету для сканирования всего трафика от сотрудника до Интернета. Процесс сканирования должен включать в себя все сетевые протоколы, разрешенные к применению. Обеспечение уверенности в том, что антивирусные обновления устанавливаются автоматически, или пользователь предупреждается о факте проведения обновлений. - Использование антивирусного программного средства на всех клиентских системах, особенно на тех, которые используются сотрудниками для доступа к Интернету. - Сканирование файлов и всех хранимых данных на наличие вирусов и троянов, а также других видов вредоносных программ. - Верификация целостности данных/файлов с использованием алгоритмов, таких как хэширование/контрольные суммы, сертификаты. - Блокирование появляющихся окон и вэб-рекламы. - Маршрутизация трафика, используемого для услуг доступа к Интернету, посредством небольшого количества контролируемых шлюзов безопасности. - Активное установление подлинности содержания.
Утечка информации	
- Безопасность связи - Целостность - Управление доступом	- Реализация фильтров для мобильного кода на шлюзах доступа к Интернету. - Прием мобильного кода только с некритичных сайтов, занесённых в белый список. - Прием мобильного кода, подписанного цифровой подписью только от доверенных органов сертификации или от доверенных поставщиков, включая соответствующие параметры настройки на стороне клиента, например, путем осуществления активного управления и реализации белого списка разрешенных органов сертификации, подписывающих код.
Несанкционированное использование и доступ	
- Управление доступом - Неотказуемость	- Предоставление служащим только соответствующих бизнесу Интернет-услуг. Использование черных списков неавторизованных услуг, например, каналов обмена информацией (текстового диалога) в реальном времени, или услуг веб-почты. Реализация фильтров для неавторизованных протоколов, например, одноранговых сетевых протоколов. - Ограничения на использование услуг, которые беспрепятственно осуществляют передачу больших объемов данных. - Обеспечение уверенности в проведении надлежащей регистрации и мониторинга в отношении всех услуг, которые допускают возможность передачи данных через Интернет.

Окончание таблицы 3

Применяемые свойства безопасности для идентифицированных угроз	Реализуемые проекты и методы
- Управление доступом - Неотказуемость	- Четкое определение авторизованного и неавторизованного использования доступа к Интернету в специальной политике (см. примерную форму в приложении А). - Обеспечение уверенности в осведомленности пользователей посредством соответствующего уровня образования и профессиональной подготовки.
Ответственность за несоблюдение нормативов	
- Неотказуемость	- Использование записи событий, отметок времени. - Осведомленность и профессиональная подготовка пользователей.
Снижение доступности сети связи	
- Целостность - Доступность	- Надлежащий менеджмент уязвимостей и исправления известных системных уязвимостей в рамках выделенного интервала времени, основанного на критичности уязвимости. - В центре внимания менеджмента уязвимостей должны быть все системы приема Интернет-трафика, либо на транспортном, либо на прикладном уровне, включая все системы, используемые с учетом шлюзов по направлению к Интернету, а также системы конечного пользователя, используемые для доступа к Интернет-услугам, особенно, если они используют операционную систему Windows. - Прерывание пропускной способности для потоковых мультимедийных средств, (если только это разрешено политикой бизнеса). - Сети и системные ресурсы должны быть проверены (IDS, журналы регистрации, аудиты и т. д.) на предмет обнаружения системных событий, событий безопасности и операционных событий.

8 Услуги бизнес-бизнес

8.1 Исходные данные

Этот сценарий должны рассматривать организации, которые осуществляют транзакции с другими организациями, такими как изготовитель, оптовик, розничный торговец.

Обычно услуги бизнес-бизнес реализуются с помощью специально выделенных линий или сетевых сегментов. Интернет и связанные с ним технологии предоставляют больше возможностей, но также вводят новые угрозы безопасности, связанные с реализацией таких услуг. Развивающаяся модель электронной торговли бизнес-бизнес позволяет организациям вести бизнес через Интернет и сосредоточиться на приложениях, использующих Интернет, экстранет или и то и другое, чтобы наладить партнерство в бизнесе, при котором организации известны друг другу и все пользователи, в отличие от сценария бизнес-клиент, регистрируются.

Обычно услуги бизнес-бизнес имеют свои собственные требования. Например, доступность и достоверность являются очень важными требованиями, поскольку часто организации напрямую зависят от действующих услуг бизнеса-бизнес.

При использовании Интернета в качестве базовой сетевой связи для реализации услуг бизнес-бизнес, такие требования как доступность и достоверность должны обрабатываться иначе, чем раньше. Проверенные подходы, такие как предполагаемое качество услуг, используемое, например, в сочетании с выделенным каналом связи, больше не работают. Новые риски безопасности должны быть уменьшены с помощью соответствующих методов проектирования и мер и средств контроля и управления. Основной упор делается на укрепление доверия между организациями, путем предотвращения несанкционированного доступа к данным и поддержки разделения систем бизнеса.

В нижеследующих пунктах описываются угрозы безопасности и рекомендации по методам проектирования безопасности, а также меры и средства контроля и управления, снижающие риски безопасности, как только для внутреннего, так и для внутреннего и внешнего использования.

8.2 Угрозы безопасности

Угрозы безопасности, связанные с услугами бизнес-бизнес, следующие:

- вирусные атаки и внедрение вредоносных программ:
- использование вредоносных программ приводит к проникновению в системы, ведущему к сбоям или несанкционированному доступу к конфиденциальной информации;
- уязвимости веб-браузеров или других веб-приложений могут быть использованы вредоносными программами, что приведет к заражению вирусом и установке троянов;
- атаки типа «отказ в обслуживании» (DoS) и «распределенный отказ в обслуживании» (DDoS — distributed denial of service) на порталы или расширенные сети услуг бизнес-бизнес;
- инсайдерские атаки с помощью авторизованных партнеров по бизнесу;
- фальсификация информационного наполнения транзакции (сообщения не передаются получателю или данные изменяются в процессе передачи).

8.3 Методы проектирования безопасности и меры и средства контроля и управления

Методы проектирования информационной безопасности и меры и средства контроля и управления, связанные с услугами бизнес-бизнес, приведены в таблице 4.

Таблица 4 — Меры и средства контроля и управления безопасности для сценария услуг бизнес-бизнес

Применяемые свойства безопасности для идентифицированных угроз	Реализуемые проекты и методы
Вирусные атаки и введение вредоносных программ	
- Целостность - Управление доступом - Аутентификация	- Использование антивирусных программ на шлюзах к Интернету для сканирования всего трафика, от сотрудника до Интернета. Процесс сканирования должен охватывать все сетевые протоколы, разрешенные к применению. Обеспечение уверенности в том, что антивирусные обновления устанавливаются автоматически, или пользователь предупреждается о факте проведения обновлений. - Сканирование файлов и всех хранимых данных на наличие вирусов и троянов, а также других видов вредоносных программ. - Верификация целостности данных/файлов с использованием алгоритмов, таких как хэширование/контрольные суммы, сертификаты. - Маршрутизация трафика, используемого для услуг доступа к Интернету, посредством небольшого количества контролируемых шлюзов безопасности. - Активное установление подлинности содержания.
Атаки «отказ в обслуживании»	
- Доступность - Непрозрачность	- Блокирование неиспользуемых портов и услуг, чтобы предотвратить их реагирование на неавторизованное сканирование/зондирование, которое приводит к возможности лавинного распространения трафика DoS. - Исключение описательной информации из предупреждающих баннеров предотвращает получение злоумышленниками специальной информации.
Инсайдерские атаки	
- Управление доступом - Неотказуемость	- Четко определенные политики безопасности по управлению доступом (для управления взаимоотношениями в бизнесе). - Четко определенные роли и обязанности. - Внесение изменений в предупреждающие баннеры. - Ограничение привилегий. - Регистрация пользователями всех критичных/некритичных транзакций.
Фальсификация информационного наполнения транзакции	
- Неотказуемость	- Подробные журналы регистрации транзакций. - Использование цифровых подписей.

9 Услуги бизнес-клиент

9.1 Исходные данные

Этот сценарий должен рассматриваться организациями, осуществляющими операции с клиентами.

Услуги бизнес-клиент, также известные как услуги электронного бизнеса, включают в себя такие услуги, как электронная торговля, электронные банковские услуги, а также электронное правительство. В услугах бизнес-клиент безопасность должна уравновешивать возможность сделок с сохранением торговой марки и ценности бизнеса.

К требованиям информационной безопасности относятся требования, связанные с:

- конфиденциальностью (особенно в отношении оказания электронных банковских услуг);
- аутентификацией;
- целостностью;
- безопасностью передачи данных там, где конечный пользователь ожидает обеспечения услугами бизнеса для защиты маршрута транзакции между пользователем и поставщиком. Сопротивление изощренным атакам (таким как, атаки «человек посредине» или «человек в браузере»);
- доступностью, которая является важным аспектом для поставщика электронного бизнеса.

Характеристики информационной безопасности включают:

- безопасность, которая «гарантирована» только на оконечной платформе[1)], обычно находящейся под управлением организации, что обеспечивает благоприятные условия для реализации мер и средств контроля и управления, а также поддержки хорошего уровня безопасности платформы;
- безопасность на клиентской платформе, часто это персональный компьютер, как правило, может быть недостаточной. Меры и средства контроля и управления реализовать в такой среде труднее, поэтому клиентская платформа будет представлять значительный риск (без «условий для безопасного соединения» — набора требований в договоре, которые может быть трудно навязать в таких условиях).

В нижеследующих пунктах описываются угрозы безопасности и рекомендации по методам проектирования безопасности, а также меры и средства контроля и управления для уменьшения сопутствующих рисков, как только для внутреннего, так и для внутреннего и внешнего использования.

9.2 Угрозы безопасности

Угрозы безопасности, связанные с услугами бизнес-клиент, следующие:

- вирусные атаки и внедрение вредоносных программ:
  - использование вредоносных программ приводит к проникновению в системы, ведущему к сбоям или несанкционированному доступу к конфиденциальной информации,
  - уязвимости веб-браузеров или других веб-приложений могут быть использованы вредоносными программами, что приведет к заражению вирусом и установке троянов;
- неавторизованный доступ:
  - неавторизованный доступ к серверным базам данных (например, атаки, распространяемые на языке SQL[2)], и межсайтовые скриптовые[3)] атаки),
  - сбор учетных записей, что дает возможность, в зависимости от того, как веб-приложение реагирует на попытки аутентифицировать пользователя, получить достоверную информацию об активности пользователя. Автоматизированные сценарии часто используются для сбора действительных идентификаторов и имен учетных записей пользователей,
  - кража идентификационных данных в режиме онлайн, используя успешные атаки социальной инженерии (с использованием мошеннических методов), например, атаки фишинга и атаки на основе DNS, соединяющие пользователей с мошенническим веб-сервером, который выглядит легитимным, но не является таковым,

---

[1)] Платформа — общий термин, обозначающий программную, аппаратную и (или) сетевую среду, в (на) которой выполняется или строится, например, прикладная система (приложение).

[2)] SQL (Structured Query Language) — язык структурированных запросов.

[3)] Скрипт — небольшая программа или макрос, исполняемые приложением или операционной системой при конкретных обстоятельствах, например, при регистрации пользователя в системе. Скрипты часто хранятся в виде текстовых файлов, которые интерпретируются во время исполнения.

- несанкционированный доступ к системам или сетям со злым умыслом, чтобы скопировать, изменить или уничтожить данные,
- незаконная расшифровка содержания приводит к нарушению авторских прав и краже содержания;
- атаки «отказ в обслуживании»;
- подделка информационного наполнения транзакции (сообщения не доходят до получателя или данные изменяются при передаче).

9.3 Методы проектирования безопасности и меры и средства контроля и управления

Методы проектирования безопасности и меры и средства контроля и управления, относящиеся к услугам бизнес-клиент, приведены в таблице 5.

Таблица 5 — Меры и средства контроля и управления безопасности для сценария услуг бизнес-клиент

Применяемые свойства безопасности для идентифицированных угроз	Реализуемые проекты и методы
Вирусные атаки и введение вредоносной программы	
- Целостность - Управление доступом - Аутентификация	- Использование антивирусных программ на шлюзах к Интернету для сканирования всего трафика от сотрудника до Интернета. Процесс сканирования должен охватывать все сетевые протоколы, разрешенные к применению. - Сканирование файлов и всех хранимых данных на наличие вирусов и троянов, а также других видов вредоносных программ. - Верификация целостности данных/файлов с использованием алгоритмов, таких как хэширование/контрольные суммы, сертификаты. - Маршрутизация трафика, используемого для услуг доступа к Интернету, посредством небольшого количества контролируемых шлюзов безопасности. - Активное установление подлинности содержания.
Неавторизованный доступ	
- Управление доступом - Аутентификация - Конфиденциальность - Безопасность связи - Целостность - Непрозрачность	- Ограниченное количество разрешений для веб-приложений при доступе к серверной базе данных. - Сегментация сети и уровни безопасности внутри демилитаризованной зоны (DMZ) для предотвращения каналов связи, направленных к корпоративным активам данных. - Безопасная регистрация пользователя для обеспечения уверенности в том, что полномочия доступа выданы подлинным пользователям — например, с привлечением к данному процессу независимого органа регистрации. - Аутентификация с использованием цифровых сертификатов, паролей, биометрии или смарт-карт. - Межсетевые экраны и списки управления доступом для предотвращения несанкционированного доступа пользователей. - Управление доступом, основанное на ролях, для ограничения функций пользователя, разрешенных к выполнению. - Анализ регистрационных журналов веб-приложений для идентификации атак и их сдерживания. - Надлежащие уровни шифрования хранимой информации. - Обеспечение уверенности в безопасном соединении между веб-браузерами и веб-серверами с использованием таких технологий, как SSLv3/TLS. - Защита основной связи с веб-сервисами с помощью, например сообщений SOAP[1)].

[1)] SOAP (Simple Object Access Protocol) — Простой протокол доступа к объектам.

Окончание таблицы 5

Применяемые свойства безопасности для идентифицированных угроз	Реализуемые проекты и методы
- Управление доступом - Аутентификация - Конфиденциальность - Безопасность связи - Целостность - Непрозрачность	- Верификация целостности данных/файлов с использованием алгоритмов, таких как хэширование/контрольные суммы, сертификаты. - На уровне веб-приложений целостность данных URL[1], куки-файлов[2] или элементов скрытых форм обеспечивается: - шифрованием всех данных (даже если используется SSLv3); - использованием изменяемых временны́х меток; - использованием цифровой подписи или ключевого хэша для чувствительных данных. - Использование «инвертированного» прокси-сервера между веб-сервером и внешней сетью.
Атаки «отказ в обслуживании»	
- Доступность - Непрозрачность	- Блокирование неиспользуемых портов протоколов и услуг, чтобы предотвратить их реагирование на несанкционированное сканирование/зондирование, которые приводят к возможности лавинного распространения трафика DoS. - Исключение описательной информации из предупреждающих баннеров предотвращает получение злоумышленниками специальной информации.
Фальсификация информационного наполнения транзакций	
- Неотказуемость	- Подробные журналы регистрации транзакций. - Использование цифровых подписей.

10 Расширенное применение услуг для совместного использования

10.1 Исходные данные

Этот сценарий должны рассматривать организации, которые используют услуги, касающиеся многих сотрудников. Примерами таких услуг являются:

- программное средство коллективного пользования;
- файловые серверы;
- список адресов для рассылки по электронной почте;
- услуги, базирующиеся на Интернет-технологиях.

Расширенное применение услуг для совместного использования, объединяющих различные средства связи и возможности совместного использования документов, является важным аспектом среды бизнеса.

Такое расширенное применение услуг для совместного использования обычно объединяет видео-телефонию, голосовую связь с чат-каналов, системы электронной почты, а также совместное использование документов и совместное использование оборудования в режиме онлайн.

Существуют два основных способа использования таких услуг для организаций:

- использование их только в качестве внутренних услуг, но недостатком этого способа является то, что услуги не могут быть использованы при работе с внешними партнерами и т. д.;
- использовать их в качестве внутренних услуг и услуг, внешних по отношению к организации. Такое использование услуг более выгодно, но имеет больше связанных с ними рисков безопасности по сравнению с использованием услуг только для внутреннего пользования.

Что касается реализации, услуги могут быть:

- реализованы внутри; или
- третьей стороной.

---

[1] URL (Uniform Resource Locator) — Унифицированный указатель ресурса (Интернет).

[2] Куки — небольшой фрагмент данных о предыстории обращений данного пользователя к веб-серверу, автоматически создаваемый сервером на машине пользователя.

Если услуги должны быть использованы внутри и вне организации, то более подходящим решением может быть покупка услуг для совместного использования у третьих сторон.

В следующих пунктах описаны угрозы безопасности и рекомендации по методам проектирования безопасности, а также меры и средства контроля и управления безопасности для уменьшения сопутствующих рисков, как только для внутреннего, так и для внутреннего и внешнего использования. Меры и средства контроля и управления безопасности применяются к управлению, передаче сигналов и трафику пользователя.

10.2 Угрозы безопасности

К угрозам безопасности, связанным с расширенным применением услуг для совместного использования, относятся:

- неавторизованный доступ, ведущий к раскрытию конфиденциальной информации:
  - злоупотребление совместным использованием инструментальных средств, чтобы незаконно воспользоваться материалами, охраняемыми авторским правом, получать конфиденциальные данные и навязывать пользователям нежелательную или пропагандистскую информацию,
  - нарушение непрозрачности посредством мониторинга использования шаблонов, спаминга и других идентичных атак;
- вирусные атаки и внедрение вредоносных программ:
  - распределение и выполнение вредоносных программ путем использования общих ресурсов;
- снижение доступности сети связи:
  - перегрузка сети с легитимным трафиком,
  - уязвимости эксплуатируемого протокола, используемые в услугах для совместного использования.

10.3 Методы проектирования безопасности и меры и средства контроля и управления

Методы проектирования информационной безопасности и меры и средства контроля и управления, относящиеся к расширенному применению услуг для совместного использования, приведены в таблице 6.

Таблица 6 — Меры и средства контроля и управления безопасности для расширенного применения услуг для совместного использования

Применяемые свойства безопасности для идентифицированных угроз	Реализуемые проекты и методы
Неавторизованный доступ, ведущий к раскрытию конфиденциальной информации	
- Управление доступом - Аутентификация - Конфиденциальность - Безопасность связи - Неотказуемость	- Доступ, основанный на ролях, для приложений, сетей и запоминающих устройств. - Назначение пользователей на разные роли с различными правами доступа для различных сетей VLAN. - Политики, основанные на ролях, касающиеся использования прав и доступа к ресурсам, таким как приложения, которые пользователь может запускать. - Списки управления доступом. - Строгая аутентификация и авторизация. - Сети VLAN для сетевой виртуализации. - IDSs, основанные на хосте. - Шифрование данных.
Вирусные атаки и введение вредоносной программы	
- Целостность	- Использование программ передачи изображения экранов, таких как терминальные серверы, чтобы свести к минимуму ввод в корпоративную среду данных и возможных вредоносных программ.

Окончание таблицы 6

Применяемые свойства безопасности для идентифицированных угроз	Реализуемые проекты и методы
Снижение доступности сети связи	
- Доступность	- Использование виртуальной архитектуры «сервер-хранилище данных» для повышения доступности и безопасности хранящихся данных. - Предотвращение извлечения информации путем использования программных инструментальных средств, чтобы предотвратить копирование/вставку информации, блокирование попытки записи на съемный носитель или печати. - Мониторинг программных средств для обнаружения нарушений политики — таких, как нарушения прав доступа к приложениям и другим сетевым ресурсам.

11 Сегментация сети

11.1 Исходные данные

Этот сценарий следует рассматривать организациям, которые хотят разделить свою внутреннюю сеть на несколько доменов, согласующихся с организационной структурой.

Сегментация сетей является методом, который может быть использован для усиления мер и средств контроля и управления в отношении системы и доступа к приложениям. Сегментация сети может быть использована для группирования определенных видов деятельности, приложений или систем таким образом, что доступ будет возможен только для тех, кто имеет доступ к сегменту сети. Таким образом, меры и средства контроля и управления сетевого доступа дополняют другие меры и средства контроля и управления доступа к конечным точкам и обеспечивают дополнительный уровень защиты в глубину. Например, сегментация сети может быть использована для:

- отделения административных возможностей и возможностей технического обслуживания от операций доступа пользователей к приложениям бизнеса;
- отделения критически важных приложений от других приложений;
- разделения баз данных большинства пользователей.

Для стран с многонациональными организациями большое влияние на требования информационной безопасности оказывает специальное законодательство. Фактическое выполнение организацией обязанностей по сегментации сети в соответствии с национальными границами может быть эффективным подходом для охвата требований информационной безопасности различных стран. Например, законодательство той или иной страны может потребовать специальной защиты клиента/данных клиента, и не позволит передачу таких данных другой стране. Обычно это требует дополнительных мер и средств контроля и управления информационной безопасности, чтобы гарантировать соответствие такому законодательству.

В пунктах ниже описаны угрозы безопасности и рекомендации по методам проектирования безопасности, а также по мерам и средствам контроля и управления безопасности, как только для внутреннего, так и для внутреннего и внешнего использования, для уменьшения рисков безопасности.

11.2 Угрозы безопасности

К угрозам безопасности, связанным с сегментацией сети, при выполнении в организациях соответствующих национальных требований других стран относятся:

- ответственность за несоблюдение законодательства;
- утечка данных:
  - нарушение конфиденциальности, например, когда данные заказчика/клиента доступны из стран, из которых они не должны быть доступны,
  - нарушение требований конфиденциальности конкретной страны,
  - риски, связанные с репутацией, влекут за собой неудовлетворение ожиданий заказчика/клиента в отношении конфиденциальности или непрозрачности.

11.3 Методы проектирования безопасности и меры и средства контроля и управления

Методы проектирования информационной безопасности и меры и средства контроля и управления, относящиеся к сегментации сети при выполнении в организациях соответствующих требований конкретной страны, приведены в таблице 7.

Таблица 7 — Меры и средства контроля и управления безопасности для сегментации сети

Применяемые свойства безопасности для идентифицированных угроз	Реализуемые проекты и методы
Ответственность за несоблюдение нормативов	
- Непрозрачность - Конфиденциальность	Политики и осведомленность пользователей: - нормы права (неприкосновенность личной жизни); - допустимые методы шифрования; - хранение данных, законы о передаче; - законы, касающиеся правомерного перехвата информации
Утечка данных	
- Управление доступом - Аутентификация - Целостность	- Шлюзы безопасности. - Прокси-программы прикладного уровня. - Шифрование данных

12 Сетевая поддержка работы на дому или в малых предприятиях

12.1 Исходные данные

Этот сценарий должны рассматривать организации, которым необходимо предоставить доступ к внутренним ресурсам для своих сотрудников, работающих на дому или в малых предприятиях.

Работа на дому или в малых предприятиях часто требует расширения внутренней сети организации до местонахождения дома или малого предприятия. Затраты на расширение сети до местонахождения дома или малого предприятия являются важным вопросом, поскольку реализация, отражающая соотношение затраты/выгоды, как правило, не должна требовать высоких затрат. Это означает ограничение стоимости мер и средств контроля и управления безопасности, которые используются для обеспечения такого расширения сети и обычно препятствуют использованию существующих межсетевых мер и средств контроля и управления безопасности, используемых для подсоединения наибольшего количества сегментов Интранет.

Для многих сценариев работы на дому или в малых предприятиях инфраструктура может быть использована как для целей бизнеса, так и для личных целей — что может привести к дополнительным рискам информационной безопасности.

В пунктах ниже описаны угрозы безопасности и рекомендации по разрабатываемым методам, касающимся безопасности, а также мерам и средствам контроля и управления безопасности для уменьшения сопутствующих рисков, как только для внутреннего, так и для внутреннего и внешнего использования.

12.2 Угрозы безопасности

К угрозам безопасности, связанным с сетевой поддержкой работы на дому или в малых предприятиях, относятся:

- неавторизованный доступ:
  - слабые настройки конфигурирования в отношении сетевого оборудования доступа, например, сетевых маршрутизаторов SOHO[1)],

[1)] Маршрутизатор SOHO (Small Office/Home Office) — Маршрутизатор, применяемый в офисе малого предприятия или для работы на дому.

- использование разделенного туннелирования,
- отсутствие или слабые физические меры и средства контроля и управления безопасности,
- продолжительное отображение на экране монитора окна в отношении подключения к сети с возможностями, обусловленными атрибутом «всегда включено»,
- использование учетных записей гостя и настроек по умолчанию;
- вирусные атаки и введение вредоносных программ:
- оборудование, включая компьютеры, используемые в домашней сети или в сети малых предприятий и работающие с недостаточными мерами и средствами контроля и управления безопасности, например, отсутствует или слабая защита от вредоносных программ и т. д.,
- проблемы, созданные смешиванием частных и бизнес-сред, например, индивидуального использования протоколов с присущими им высокими рисками, таких как одноранговые протоколы совместного использования файлов,
- исправления недостаточности,
- после заражения доступность сети может серьезно пострадать в результате распространения вирусов, ведущих к перегрузке сети;
- несанкционированное разглашение конфиденциальной информации:
- отсутствие шифрования данных, хранящихся в системах и передающихся через сети домашнего или малого бизнеса,
- злоупотребление возможностями доступа, такими как беспроводной доступ в Интернет через домашние сети или сети малых предприятий,
- недостаточное обучение конечных пользователей передовым практикам осведомленности и безопасности,
- недостоверность предположений касательно защиты Интранета, так как сетевые шлюзы, используемые при работе на дому или в малых предприятиях, не обеспечивают такой же уровень защиты, как шлюзы, использующиеся для соединения филиалов организации.

12.3 Методы проектирования безопасности и меры и средства контроля и управления

Методы проектирования информационной безопасности и меры и средства контроля и управления, относящиеся к сетевой поддержке при работе на дому или в малых предприятиях, приведены в таблице 8.

Таблица 8 — Меры и средства контроля и управления безопасности при использовании сети для сценариев работы на дому или в малых предприятиях

Применяемые свойства безопасности для идентифицированных угроз	Реализуемые проекты и методы
Несанкционированный доступ	
- Управление доступом - Аутентификация - Безопасность связи	- Отключение сетевых интерфейсов и услуг, которые не используются. - Установление межсетевого экрана хоста — пропуск или отключение всех входящих извне соединений. - Проектирование и методы защиты раздельного туннелирования. - В системах не должны использоваться пароли, состоящие из пробелов, нулей, или пароли по умолчанию. - Строгие пароли должны быть обязательными для всех пользователей. Анонимный/гостевой доступ не должен быть разрешен. - Технические проверки соответствия для обеспечения уверенности в надлежащей конфигурации и настройках всего чувствительного оборудования безопасности, например, маршрутизатора или точек доступа к беспроводной сети. - Безопасные технологии VPN в компонентах сетевого доступа, такие как маршрутизаторы сетевого доступа.

Окончание таблицы 8

Применяемые свойства безопасности для идентифицированных угроз	Реализуемые проекты и методы
Вирусные атаки и введение вредоносной программы	
- Целостность - Доступность	- Поддержка текущих версий программных средств и уровней обновления. - Обеспечение уверенности в том, что антивирусные обновления устанавливаются автоматически, или пользователи предупреждены о том, что обновления доступны. - Использование хостовой системы обнаружения вторжений (HIDS — Host-based Intrusion Detection System), по крайней мере, для обнаружения целостности базы данных/программного средства (если применимо). - Сканирование файлов и всех хранимых данных на наличие вирусов и троянов, а также других видов вредоносных программ. - Резервное копирование данных конфигурации и файлов для реагирования на инциденты и восстановления.
Несанкционированное раскрытие конфиденциальной информации	
- Конфиденциальность - Непрозрачность	- Осведомленность и обучение пользователей лучшим практикам по безопасности. - Шифрование хранимых и передаваемых данных.

13 Мобильная связь

13.1 Исходные данные

Этот сценарий должны рассматривать организации, разрешающие сотрудникам использование мобильных устройств.

Этот сценарий сосредоточен на безопасных деловых отношениях предприятий, использующих и развертывающих мобильные устройства и приложения. Хотя основным фактором для быстрого развития новых возможностей мобильных устройств, таких как смартфоны или персональные информационные устройства (PDA — personal data assistants), является потребительский рынок, они также используются в среде бизнеса. Часто такие устройства являются личной собственностью, и используются, как для целей бизнеса, так и в личных целях. Иногда устройства могут быть предоставлены компанией и применены для личного использования. Таким образом, ориентированным на профессиональную деятельность устройствам необходимо иметь функции, введенные для потребительского рынка, поскольку продавцы хотят получить настолько выгодный бизнес, насколько он возможен в условиях конкуренции.

Устройства мобильной связи позволяют удаленным пользователям координировать персональные базы данных, а также обеспечивать доступ к услугам сети, таким как беспроводная электронная почта, просмотр веб-страниц, а также доступ к Интернету. Когда человек использует одни и те же устройства для частных и для деловых целей, возникает тенденция обхода политик или игнорирование их использования, таким образом, на предприятие привносятся значительные риски информационной безопасности.

В пунктах ниже описываются угрозы безопасности и даются рекомендации по методам проектирования безопасности, а также приводятся меры и средства контроля и управления, как только для внутреннего, так и для внутреннего и внешнего использования, для уменьшения соответствующих рисков.

13.2 Угрозы безопасности

Угрозами безопасности, связанными с мобильными устройствами связи являются:

- несанкционированный доступ к информации, хранящейся на мобильных устройствах, вследствие:
  - слабого управления доступом или недостаточной защиты конфиденциальной информации,
  - недостаточной информированности и неадекватных паролей,

- слабой конфигурации,
- хакерских атак с использованием мошеннических устройств,
- отсутствия осведомленности конечных пользователей о требованиях обеспечения информационной безопасности, например, при смешивании частной информации и информации бизнеса;
- несанкционированное разглашение местоположения конфиденциальных данных и информации, вследствие:
- услуг, связанных с определением местоположения, которые могут раскрывать несанкционированным третьим лицам информацию о положении пользователя, что затрагивает неприкосновенность частной жизни,
- подслушивания,
- вовлечения неадекватно защищенных третьих лиц в процесс передачи информации,
- использования открытого текста или недостаточно защищенных протоколов передачи,
- неправильных процедур утилизации;
- несанкционированная модификация/удаление хранимой информации (включая программное средство), вследствие:
- ввода вредоносных программ путем установления программного средства, полученного от неавторизованного источника,
- использования уязвимостей в базовой операционной системе;
- спам, приводящий к:
- повышенной плате за обслуживание,
- возможности фишинг-атак,
- атакам «отказ в обслуживании»;
- кража или случайная потеря, приводящая к:
- потере чувствительных данных всякий раз, когда данные, хранящиеся на устройстве, не отображаются, или резервное копирование выполняется в другом месте,
- проблемам конфиденциальности, когда конфиденциальные данные, хранящиеся на устройстве, не защищены должным образом,
- бесконтрольному резервному копированию данных.

13.3 Методы проектирования безопасности и меры и средства контроля и управления

Методы проектирования информационной безопасности и меры и средства контроля и управления, относящиеся к устройствам персональной мобильной связи, приведены в таблице 9.

Таблица 9 — Меры и средства контроля и управления безопасности для сценария мобильной связи

Применяемые свойства безопасности для идентифицированных угроз	Реализуемые проекты и методы
Несанкционированный доступ к информации, хранящейся на мобильных устройствах	
- Управление доступом - Аутентификация - Неотказуемость	- Осведомленность пользователя о физическом контроле. - Избегание стандартных конфигураций. - Строгая аутентификация. - Включение опций регистрации. - Блокировка таймера неактивности. - Межсетевые экраны. - Формирование политики безопасности в отношении паролей и использования в бизнесе (ограничение использования в личных целях устройств, принадлежащих предприятию).

Окончание таблицы 9

Применяемые свойства безопасности для идентифицированных угроз	Реализуемые проекты и методы
Несанкционированное разглашение конфиденциальных данных и информации, касающейся размещения	
- Конфиденциальность - Аутентификация - Безопасность связи - Непрозрачность	- Шифрование хранимых и передаваемых (беспроводным способом) данных. - Защита паролей. - Избегать услуг третьей стороны, которые требуют свободного доступа к тексту передаваемых данных или, а если это невыполнимо, то требовать обеспечения уверенности в том, что конфиденциальность обрабатываемых данных такая, как требуется. - Обеспечение уверенности в безопасных процедурах синхронизации. - Для удаленного доступа использовать соединения через безопасную VPN. - Надлежащие процедуры утилизации носителей для удаления чувствительных данных. - Согласие пользователя на определение его местоположения.
Несанкционированная модификация/удаление хранимой информации (включая программное средство)	
- Конфиденциальность - Доступность - Целостность	- Отключение неиспользуемых беспроводных интерфейсов, услуг и приложений. - Своевременное проведение исправлений операционной системы. - Надлежащие процедуры утилизации для удаления конфиденциальных данных. - Обеспечение уверенности в том, что антивирусные обновления устанавливаются автоматически, или пользователи предупреждены о том, что обновления доступны. - Загрузка программного средства, полученного только от предприятий, имеющих право на распространение программного средства (во избежание установки нелицензионного программного средства). - Цифровые подписи для проверки источника загружаемого программного средства.
Спам	
- Управление доступом	- Фильтрация информации. - Повышение осведомленности пользователей.
Кража или случайная потеря	
- Конфиденциальность - Аутентификация	- Удаленное управление активами (устройства отключения/блокировки). - Периодическое безопасное резервное копирование. - Централизованный менеджмент в отношении отслеживания активов и соблюдения политики.

14 Сетевая поддержка мобильных пользователей

14.1 Исходные данные

Этот сценарий должны рассматривать организации, разрешающие сотрудникам перемещаться для получения доступа к ресурсам организации.

Решения и предложения в этой области часто сосредоточены на функциональности и ориентированы в первую очередь на потребительский рынок. С точки зрения информационной безопасности предлагаемые уровни функциональности привносят новые риски, например, влияя на информационную безопасность или опровергая предположения относительно нее. Например, предположение о поддержке хорошо контролируемого и (внешне) защищаемого Интранета может быть подвергнуто сомнению по существу, если доступ к Интранету для мобильного пользователя не обеспечивается соответствующими мерами и средствами контроля и управления.

В пунктах ниже описываются угрозы безопасности и даются рекомендации по методам проектирования безопасности, а также приводятся меры и средства контроля и управления для уменьшения соответствующих рисков, как только для внутреннего, так и для внутреннего и внешнего использования.

14.2 Угрозы безопасности

Угрозами безопасности, связанными с сетевой поддержкой мобильных пользователей, являются:

- несанкционированный доступ:
  - неправильное использование технической поддержки мобильных пользователей сети для получения несанкционированного доступа к Интранету организации;
  - компрометация шлюзов безопасности, используемых на границе сети Интранет;
  - несанкционированный доступ к данным, хранящимся на устройствах мобильного пользователя;
- снижение доступности сети связи:
  - проблемы доступности, возникающие, когда пользовательские ожидания относительно сетевой поддержки не могут быть выполнены, например, когда это зависит от доступности провайдеров услуг Интернет.

14.3 Методы проектирования безопасности и меры и средства контроля и управления

Методы проектирования информационной безопасности и меры и средства контроля и управления, относящиеся к сетевой поддержке мобильных пользователей, приведены в таблице 10.

Таблица 10 — Меры и средства контроля и управления сетевой поддержки мобильных пользователей

Применяемые свойства безопасности для идентифицированных угроз	Реализуемые проекты и методы
Несанкционированный доступ	
- Управление доступом - Аутентификация - Безопасность связи - Конфиденциальность	- Усовершенствованные методы аутентификации (аутентификация на основе сертификатов, двухфакторной аутентификации или аутентификации вызов-ответ). - Специализированные услуги для мобильных пользователей, основанные на протоколах TLS/SSLv3 защищенных веб-интерфейсов. - Использование методов безопасных виртуальных частных сетей в сочетании с соответствующими шлюзами безопасности на клиентских системах (например, персональные брандмауэры): - реализации уровней 2/3, например, IPSec; - уровня приложений VPN, например, основанного на TLS. - Шифрование хранимых данных пользователя.
Снижение доступности сети связи	
- Доступность	- Привлечение общеизвестных провайдеров услуг и использование соглашения об уровне услуг для надежности и производительности.

15 Услуги аутсорсинга

15.1 Исходные данные

Этот сценарий должны рассматривать организации, использующие услуги аутсорсинга.

Организации используют услуги аутсорсинга, поскольку они рассматриваются в качестве жизнеспособной стратегии бизнеса, но это вносит организационные и оперативные сложности, особенно для обеспечения качества и безопасности услуг аутсорсинга.

Такое расширение сфер действия предприятия наследует дополнительные риски в связи с зависимостью от поставщика услуг. Например, поставщикам или продавцам услуг может потребоваться прямой доступ к активам внутри организации для поддержки и (или) исходя из управления инцидентами, тем самым подвергая критические активы рискам безопасности. Наряду с тем, что для многих

вспомогательных услуг требуются постоянные права доступа к поддерживаемой инфраструктуре, для других, возможно, необходим лишь временный доступ. Часто услуги поддержки нуждаются в высокопривилегированных правах доступа для выполнения своих задач.

Независимо от типа сценария аутсорсинга рассмотрение безопасности и надзора являются обязательными для всех таких договорных отношений. Общее представление о соответствующих угрозах и проблемах приведено в настоящем документе. Более подробные сведения об обеспечении безопасности услуг аутсорсинга можно найти в ИСО/МЭК 27036.

В пунктах ниже описываются угрозы безопасности и даются рекомендации по методам проектирования безопасности, а также приводятся меры и средства контроля и управления для уменьшения соответствующих рисков, как только для внутреннего, так и для внутреннего и внешнего использования.

15.2 Угрозы безопасности

Угрозами безопасности, связанными с услугами аутсорсинга, являются:

- несанкционированный доступ к другим внутренним системам (когда поставщик получает доступ к внутренним системам для удаленной поддержки и технического обслуживания):
  - злоупотребление удаленными портами обслуживания,
  - злоупотребление правами администратора;
- несанкционированное раскрытие поставщиком услуг конфиденциальных данных:
  - пренебрежение правами интеллектуальной собственности,
  - отсутствие разделения многокомпонентных сред клиентов,
  - отсутствие лучших практик по обеспечению информационной безопасности (например, широко распространено совместное использование паролей),
  - неправильное обращение с носителями информации,
  - использование небезопасных методов передачи информации;
- внедрение вредоносных программ (в среду разработки программного средства):
  - недостаточная безопасность при разработке программного средства и процедур выпуска программного средства,
  - небезопасная передача файлов и данных,
  - небезопасные практики совместного использования режима онлайн;
- ответственность за несоблюдение законодательства:
  - отсутствие понимания норм и законов конкретной страны об ответственности, если поставщик услуг находится в другой стране,
  - недостаточные правовые требования к конфиденциальности и защите данных, применяемые в стране, где находится поставщик; это может оказать существенное неблагоприятное воздействие на конфиденциальность данных и защиту требований, предъявляемых к покупателю.

15.3 Методы проектирования безопасности и меры и средства контроля и управления

Методы проектирования информационной безопасности и меры и средства контроля и управления, относящиеся к услугам аутсорсинга, приведены в таблице 11.

Таблица 11 — Меры и средства контроля и управления безопасности для услуг аутсорсинга

Применяемые свойства безопасности для идентифицированных угроз	Реализуемые проекты и методы (реализацию может взять на себя аутсорсинговая организация или внешнее предприятие в зависимости от утвержденного задания)
Несанкционированный доступ к внутренним системам	
- Управление доступом - Аутентификация - Неотказуемость	- Строгое назначение персональных идентификаторов пользователя. - Строгая аутентификация (например, двухфакторная аутентификация) для регистрации входа суперпользователя/администратора. - Местный консольный порт или рабочий порт, защищенный идентификатором и паролем пользователя (в случае, если поставщиком услуг запрещен удаленный доступ). - Всеобъемлющая регистрация действий, связанных с доступом, и анализ журналов регистрации.

Окончание таблицы 11

Применяемые свойства безопасности для идентифицированных угроз	Реализуемые проекты и методы (реализацию может взять на себя аутсорсинговая организация или внешнее предприятие в зависимости от утвержденного задания)
Несанкционированное раскрытие конфиденциальных данных	
- Конфиденциальность	- Лучшие практики, касающиеся защиты данных клиента шифрованием. - Осведомленность и обучение безопасности. - Средства и процедуры мониторинга и аудита. - Договорная политика безопасности и директивы в отношении процедур.
Внедрение вредоносных программ	
- Целостность	- Безопасные приемы программирования. - Процессы менеджмента изменений. - Обеспечение уверенности в том, что антивирусные обновления устанавливаются автоматически, или пользователи предупреждены о том, что обновления доступны.
Ответственность за несоблюдение законодательства	
- Конфиденциальность - Непрозрачность	- Осведомленность о местном законодательстве. - Использование совместимого программного средства для шифрования. - Механизмы непрозрачности (IPSec VPN).

Приложение А
(справочное)

Пример политики использования объединенной сети

А.1 Общий обзор

Намерения InfoSec[1)] в отношении публикации «Политики приемлемого использования» — не налагать ограничений, которые являются несоответствующими для <Наименование компании>[2)] с устойчивой культурой открытости, доверия и целостности. InfoSec выполняет обязательства по защите сотрудников, партнеров <Наименование компании> и самой компании от незаконных или вредных действий отдельных лиц, выполняемых осознанно или неосознанно.

Связанные с Интернет/Интранет/Экстранет системы, включающие компьютерное оборудование, программное обеспечение, операционные системы, хранящуюся информацию, сетевые ресурсы, обеспечивающие электронную почту, просмотр страниц Интернет и FTP, но не ограничивающиеся этим, являются достоянием <Наименование компании>. Эти системы должны быть использованы для коммерческих целей, должны служить интересам компании, клиентов и заказчиков в процессе обычной работы. Для получения более подробной информации, пожалуйста, рассмотрите «Кадровые политики».

Эффективная безопасность является результатом совместных усилий при участии и поддержке каждого сотрудника <Наименование компании> и филиалов, имеющих дело с информацией и (или) информационными системами. В обязанность каждого пользователя компьютера входит знание этих рекомендаций, и осуществление своей деятельности в соответствии с ними.

А.2 Цель

Цель политики заключается в определении приемлемого использования компьютерной техники в <Наименование компании>. Этот перечень правил выпускается, чтобы защитить работника и <Наименование компании>. Нецелевое использование компьютерной техники подвергает <Наименование компании> рискам, включающим риски вирусных атак, риски компрометации сетевых систем и услуг и риски юридических проблем.

А.3 Область применения

Настоящая политика распространяется на сотрудников, подрядчиков, консультантов, временных и других работников <Наименование компании>, в том числе на персонал, связанный с третьими сторонами. Эта политика распространяется на все оборудование, которое находится в собственности или арендуется <Наименование компании>.

А.4 Политика

А.4.1 Общее использование и собственность

1) Хотя администрация сети <Наименование компании> желает обеспечить приемлемый уровень непрозрачности, пользователи должны быть осведомлены о том, что данные, которые они создают на корпоративных системах, являются собственностью <Наименование компании>. В связи с необходимостью защиты сети <Наименование компании> менеджмент не может гарантировать конфиденциальности информации, хранящейся на любых сетевых устройствах, принадлежащих <Наименование компании>.

2) Сотрудники несут ответственность за осуществление правильного решения, касающегося обоснованности персонального использования. Отдельные подразделения несут ответственность за создание рекомендаций, касающихся персонального использования систем Интернет/Интранет/Экстранет. При отсутствии политик, сотрудники должны руководствоваться ведомственными политиками в личных целях, и если возникают какие-либо неопределенности, сотрудники должны проконсультироваться со своим руководителем или менеджером.

3) InfoSec рекомендует, чтобы любая информация, которую пользователи считают чувствительной или уязвимой, была зашифрована. Для получения руководящих указаний, касающихся классификации информации, см. «Политику чувствительной информации», разработанную InfoSec. Для получения руководящих указаний по шифрованию электронной почты и документов обратитесь к «Инициативе осведомленности», разработанной InfoSec.

4) В целях безопасности и технического обслуживания сетей, уполномоченные лица в пределах <Наименование компании> могут контролировать оборудование, системы и сетевой трафик в любое время согласно «Политике аудита», разработанной InfoSec.

5) <Наименование компании> сохраняет за собой право на проведение аудита сетей и систем на регулярной основе в целях обеспечения соблюдения этой политики.

[1)] Служба информационной безопасности.

[2)] Здесь должно указываться наименование конкретной компании, к которой применима рассматриваемая политика.

А.4.2 Безопасность и служебная информация

1) Интерфейс пользователя для информации, содержащейся в системах, связанных с Интернет/Интранет/Экстранет, которая должна быть классифицирована в качестве конфиденциальной или не конфиденциальной, как определено в рекомендациях по корпоративной конфиденциальности, более подробные сведения о которой можно найти в «Кадровой политике». Примеры конфиденциальной информации включают, но не ограничиваются: секреты компании, корпоративные стратегии, чувствительную информацию о конкурентах, торговые секреты, спецификации, списки клиентов и данные исследований. Сотрудники должны принять все необходимые меры для предотвращения несанкционированного доступа к этой информации.

2) Хранить пароли в секрете и не разделять учетные записи. Авторизованные пользователи несут ответственность за сохранность своих паролей и учетных записей. Пароли системного уровня должны изменяться ежеквартально, пароли уровня пользователя следует изменять каждые шесть месяцев.

3) Все персональные компьютеры, ноутбуки и рабочие станции должны быть обеспечены защищенной паролем заставкой с автоматической активацией, установленной на 10 минут или меньше, или отключением регистрации (комбинация клавиш «control-alt-delete» для пользователей Win2K[1)]), когда хост будет необслуживаемым.

4) Использование шифрования информации в соответствии с «Политикой приемлемого использования шифрования», разработанной InfoSec.

5) Поскольку информация, содержащаяся на портативных компьютерах особенно уязвима, ей должно быть уделено особое внимание. Защита ноутбука осуществляется в соответствии с «Информацией по безопасности для ноутбука».

6) Почтовые сообщения сотрудников из адреса электронной почты <Наименование компании> для сетевых телеконференций должны содержать оговорку о том, что выражено строго индивидуальное мнение, и оно не обязательно совпадает с позицией <Наименование компании>, кроме почтовых сообщений, участвующих в процессе бизнеса.

7) Все хосты, используемые служащими для подключения к Интернет/Интранет/Экстранет <Наименование компании> и принадлежащие сотруднику или <Наименование компании>, должны непрерывно сканироваться антивирусной программой с действующей (актуальной) базой данных вирусов, если не переопределены ведомственные или групповые политики.

8) Сотрудники должны соблюдать осторожность при открытии вложений электронной почты, полученных от неизвестных отправителей, которые могут содержать вирусы, бомбы электронной почты, или код Троянского коня.

А.4.3 Недопустимое использование

Перечисленные ниже виды деятельности строго запрещены. Служащие могут быть освобождены от этих ограничений в ходе выполнения своих законных обязанностей (например, системам управления персоналом может потребоваться отключение сетевого доступа к хосту, если этот хост нарушает производство услуг).

Ни при каких обстоятельствах сотруднику <Наименование компании> не разрешается выполнение какой-либо деятельности, являющейся незаконной в соответствии с местным, государственным, федеральным или международным правом, пока используются ресурсы, принадлежащие <Наименование компании>.

Перечни ниже, не являются исчерпывающими, а пытаются обеспечить базу для деятельностей, которые попадают в категорию недопустимого использования.

А.4.3.1 Системная и сетевая деятельность

Следующие мероприятия, без исключений, являются строго запрещенными:

1) нарушения прав любого лица или компании, защищенных авторскими правами, коммерческой тайной, патентом или иной интеллектуальной собственностью, а также нарушения аналогичных законов или правил, включая, но не ограничиваясь, установки или распространения «пиратских» или других программных продуктов, которые не являются соответствующим образом лицензированными для использования <Наименование компании>;

2) строго запрещено несанкционированное копирование материалов, защищенных авторским правом, включая, но не ограничиваясь, оцифровку и распространение фотографий из журналов, книг или других источников, защищенных авторским правом, защищенной авторским правом музыки, а также установка любого программного средства, защищенного авторским правом, на которое <Наименование компании> или конечный пользователь не имеет активной лицензии;

3) незаконным является экспорт программного обеспечения, технической информации, программного обеспечения или технологии шифрования в нарушение международных или региональных законов о контроле над экспортом. Соответствующим представителям менеджмента следует проконсультироваться перед экспортом какого-либо рассматриваемого материала;

4) внедрение вредоносных программ в сеть или на сервер (например, вирусов, «червей», «Троянских коней», «бомб» электронной почты и т. д.);

5) раскрытие своего пароля учетной записи другим лицам или разрешение использовать свою учетную запись другими. Это касается членов семьи и других родственников, когда работа ведется на дому;

6) использование вычислительных активов <Наименование компании> для активного участия в приобретении или передаче материала, который нарушает законы о сексуальных домогательствах или о враждебном отношении на рабочем месте, находящиеся в местной юрисдикции пользователей;

[1)] Win2K — Операционная система MS Windows 2000.

7) оформление мошеннических предложений товаров, предметов или услуг, исходящих из какой-либо учетной записи <Наименование компании>;

8) оформление заявления о гарантии, прямой или косвенной, если это не является частью обычных рабочих обязанностей;

9) осуществление нарушений безопасности или сбоев в сетевой коммуникации. Нарушения безопасности включают, но не ограничивают, доступ к данным служащего, который не является предполагаемым получателем, регистрацию на сервере или учетную запись, явно не разрешенную для доступа сотрудника, если эти обязанности не входят в рамки обычных обязанностей. Для целей настоящего раздела термин «нарушение» включает, но не ограничивает, сниффинг[1)] сети, переполнение пакетами «запрос отклика», пакетный спуффинг[2)], отказ в обслуживании, и ложная маршрутная информация в злонамеренных целях;

10) сканирование портов или сканирование безопасности категорически запрещается без предварительного уведомления InfoSec ;

11) выполнение любых форм сетевого мониторинга, который будет перехватывать данные, не предназначенные для хоста служащего, если эта деятельность не является частью обычной работы сотрудника/его долгом;

12) обход аутентификации пользователей или защиты любого хоста, сети или учетной записи;

13) вмешательство в или отказ в услуге любому пользователю, за исключением вмешательства в работу хоста служащего (например, атака «отказ в обслуживании»);

14) использование любой программы/скрипта/команды или отправка сообщения любого рода, с намерением помешать или отключить терминальный сеанс пользователя, с помощью любых средств, локально или через Интернет/Интранет/Экстранет;

15) предоставление информации о сотрудниках или списков сотрудников <Наименование компании> сторонам за пределами <Наименование компании>.

А.4.3.2 Деятельность, связанная с коммуникацией и электронной почтой

1) Отправка незатребованных сообщений электронной почты, включая отправку «ненужных сообщений» или других материалов рекламного характера лицам, которые специально не запрашивают такие материалы (спам электронной почты).

2) Любая форма преследования по электронной почте, телефону или пейджинговой связи, будь то язык, частота или размер сообщений.

3) Несанкционированное использование или фальсификация данных, содержащихся в заголовке сообщений электронной почты.

4) Навязывание услуг по электронной почте для любых адресов электронной почты, отличающихся от тех, что зарегистрированы в учетной записи отправителя, с намерением надоедать или для сбора ответных сообщений.

5) Создание или пересылка «писем счастья», «схем Понци» или иных схем «пирамид» любого типа.

6) Использование навязываемых почтой, исходящей из сетей <Наименование компании> от других поставщиков услуг Интернет/Интранет/Экстранет от ее имени или в рекламных целях, любых услуг, выполняемых хостом <Наименование компании> или подключенным через сеть <Наименование компании>.

7) Рассылка по почте одинаковых или аналогичных сообщений, не связанных с бизнесом, многочисленным тематическим телеконференциям, проводимым в пользовательских сетях (спам телеконференций).

А.4.4 Ведение блогов

1) Ведение блогов сотрудниками, как при использовании имущества и систем <Наименование компании>, так и персональных компьютеров, находится также в соответствии с условиями и ограничениями, изложенными в этой политике. Ограниченное и нерегулярное использование систем <Наименование компании> для участия в блогах является приемлемым при условии, что это делается профессионально и ответственно, не нарушает политику <Наименование компании>, не наносит ущерба всем возможным интересам <Наименование компании> и не мешает обычным трудовым обязанностям работника. Ведение блогов из систем <Наименование компании> является также предметом мониторинга.

2) Политика конфиденциальной информации <Наименование компании> также распространяется на блоги. Таким образом, сотрудники не имеют права раскрывать какую-либо конфиденциальную или служебную информацию <Наименование компании>, коммерческие тайны или любой другой материал, охваченный политикой конфиденциальной информации <Наименование компании>, который затрагивался при ведении блога.

3) При ведении блога сотрудники не должны затрагивать ту информацию, которая может повредить или запятнать имидж, репутацию и (или) «неосязаемый капитал» <Наименование компании> и (или) любого из ее сотрудников. Сотрудникам также запрещается делать какие-либо дискриминационные, пренебрежительные, дискредитирующие или связанные с преследованием комментарии при ведении блога или ином участии в ведении каких-либо дел, запрещенных политикой недопущения дискриминации и борьбы с преследованием <Наименование компании>.

4) Сотрудники не могут приписывать личные заявления, мнения или убеждения в отношении <Наименование компании>, когда они участвуют в блогах. Если сотрудник выражает собственные убеждения и (или) мнения в

[1)] Сниффинг (SNIFFING) — Прослушивание сетевого трафика.

[2)] Спуффинг (SPOOFING) — Подмена пакетов.

блогах, то он не может прямо или косвенно представлять себя в качестве сотрудника или представителя <Наименование компании>. Сотрудники несут ответственность за все риски, связанные с ведением блогов.

5) Наряду с соблюдением всех законов, касающихся обработки и раскрытия информации, защищенной авторским правом, или экспорта контролируемых материалов, торговые марки, логотипы <Наименование компании> и любая другая интеллектуальная собственность <Наименование компании> не может и не должна использоваться в связи с любыми действиями по ведению блогов.

А.5 Принуждение к выполнению

Любой сотрудник, признанный виновным в нарушении этой политики, может быть подвергнут дисциплинарному взысканию, вплоть до увольнения.

А.6 Определения

Термин	**Определение**
Ведение блога (blogging)	Записи в блоге. Блог (сокращенно от weblog) является персональным интернет-журналом, который часто обновляется и предназначен для информирования широкой общественности.
Спам (spam)	Несанкционированные и (или) нежелательные массовые рассылки по электронной почте.

А.7 Статистика изменений

Приложение В
(справочное)

Каталог угроз

В.1 Ложное представление полномочий и прав

- Представление ложных полномочий, будто бы они верные, с намерением ввести в заблуждение.
- Представление другого пароля, ключа или сертификата (например, системного администратора).
- Несанкционированное приобретение и использование абонентом услуг, связанных с идентификационной информацией (например, идентификатор/пароль пользователя, сеансовые (криптографические) ключи). Ограничено для индивидуальных абонентов.
- Несанкционированное приобретение и использование административной информации по аутентификации (например, идентификатор пользователя/пароль).
- Атаки воспроизведения, включая сигнализацию.

В.2 Кража услуг

- Незаконный захват прибыли поставщика услуг с целью лишить поставщика услуг законного дохода.
- Обман поставщика услуг.
- Несанкционированное удаление или изменение платежной информации.
- Клонирование устройства.
- Обход систем условного доступа (CAS — conditional access systems).
- Избыточное дублирование/распространение информации, делающее возможными кражи услуг.

В.3 Вторжение в частную жизнь и прослушивание

- Отслеживание модели обращения для обнаружения идентификационных данных, принадлежности, наличия и использования.
- Захват трафика — несанкционированная запись трафика, включающая пакетную запись, пакетную регистрацию и отслеживание пакетов. Включает в себя управляющий и сигнальный трафик.
- Несанкционированный доступ к абонентскому потоку видео- или аудиоданных.
- Несанкционированный доступ к трафику OAM&P.
- Несанкционированный доступ к сигнальному трафику.
- Информационная «уборка урожая» — несанкционированное средство получения идентификационных данных, которое может являться результатом несанкционированного общения и кражи информации. Состоит из коллекции идентификаторов, которые могут быть представлены числами, цепочками символов, адресами URL и т. д.
- Реконструкции носителей данных — несанкционированный мониторинг, запись, хранение, реконструкция, осознание, трактовка, перевод, и (или) выделение признаков любой части видеосвязи, включая идентичность, наличие или состояние.
- Несанкционированное раскрытие возможностей абонентского обслуживания.
- Несанкционированное раскрытие предыдущих или текущего обращений или активности абонента (например, содержание предыстории просмотра абонентом телепередачи или контента[1] VoD[2], игровая деятельность в режиме онлайн и т. д.).
- Атаки воспроизведения в СМИ (повторное воспроизведение в СМИ захваченных форм информации, предназначенной для личного пользования, с целью извлечения незаконной прибыли или вторжения в частную жизнь).

В.4 Перехват и модификация

- Имитация переговоров и перехват — ввод, удаление, добавление, перемещение, замена или подстановка, а также иное изменение любой части передаваемой информации, которые меняют любую часть ее содержания и (или) идентичность, наличие или статус любой из ее частей. Включает в себя управляющий и сигнальный трафик.
- Несанкционированный доступ, изменение или удаление цифровой информации.
- Поток данных для похищения; вставки, изменения и удаления данных в потоке, проводимые несанкционированным способом.
- Любые виды спама.
- Несанкционированная передача материалов (по политическим или другим причинам).

---

[1] Контент — Содержательная часть данных документа. Может включать текст, изображения, видео, звук, сценарии (программы) или любой другой материал.

[2] VoD (video on demand) — Видео по запросу.

B.5 Лавинная маршрутизация трафика/пакетов

- Атака «отказ в обслуживании» на пользователей конечной точки, путем отправки большого количества достоверных пакетов, вызывая прерывания в оказании услуг, некоторые из которых заодно могут повлиять на элементы сети. Приложение перестает отвечать на запросы в результате перегрузки.
- Сценарии лавинной маршрутизации пакетов приводят элементы конечной точки сети или сервер к аварийному отказу, перезагрузке или исчерпывают все ресурсы.
- DoS — пропускная способность или потребление ресурса; большой объем трафика (например, для группы многоадресной рассылки).
- Потенциальное влияние тысяч абонентов (например, DSLAM[1)], серверов, поддерживающих тысячи абонентов).

B.6 Искаженные пакеты и сообщения

- Блокирующие конечные точки с недостоверными сообщениями — атака «отказ в обслуживании» на конечную точку (например, сервер) посредством отправления некоего количества недействительных сообщений, которые могут привести к аварийному отказу, перезагрузке или исчерпать все ресурсы.
- Искаженные сообщения протокола — отправка искаженных сообщений протокола (например, сообщений с переполнением или потерей значимости) на устройство, снижающих производительность устройства до такой степени, что оно не может обработать обычные сообщения.
- Искаженные сообщения, вызывающие переполнение буфера.
- Потенциальное влияние тысяч абонентов (например, серверы, поддерживающие тысячи абонентов).

B.7 Поддельные сообщения

- Атака «отказ в обслуживании», которая нарушает услугу посредством досрочного завершения сеанса связи.
- Спуффинг управляющих сообщений. Злоумышленный трафик управления — трафик, вводимый в систему связи, вызывая неисправности приложений и серверов или трафик, направляемый на ложные адреса назначения. Ложные управляющие сообщения используются для изменения структуры древовидных многоадресных схем распределения и нарушают необходимое распределение данных между узлами сети. DoS — широковещательная рассылка фиктивного сообщения, утверждающего, что существует высокий уровень потерь в канале или высокая перегруженность; причина этого приведет к снижению скорости передачи, затрагивающей других абонентов.
- Ложные сообщения конечного использования и ответные действия приложений или сервера.
- Изменение IP- и MAC-адресов, имитирующие MAC- и IP-адреса других пользователей для захвата потока данных.

B.8 Основная платформа DoS

- Уязвимости базовой операционной системы или встроенного программного средства, которые затрагивают приложение или услугу.
- «Выбрать и активизировать» — использует свободно доступную в Интернете информацию для скачивания.
- Атаки «отказ в обслуживании», снижающие производительность устройства. При эксплуатации эти уязвимости имеют возможность распространяться на тысячи устройств (например, клиентских устройств). Потенциальным результатом является перераспределение или поддержание тысяч устройств.

B.9 Компрометация установленного программного средства, служебных данных или конфигурации системы

- Ввод вредоносных программ, шпионских программ, руткитов[2)].
- Несанкционированное копирование, установка, изменение удаления файлов эксплуатируемого программного средства и конфигурации.
- Несанкционированное копирование, раскрытие информации, создание, изменение или удаление служебных данных (например, системных журналов, платежных реквизитов, ключей шифрования, контейнеров для хранения ключей расшифровки и т. п.).
- Атаки «распределенный отказ в обслуживании», использующие скомпрометированные устройства, приводящие к аварийному отказу услуги.
- Несанкционированное создание или изменение информации абонентской службы (например, проверка подлинности информации, сеансовых ключей).
- Несанкционированная или ненужная активация/деактивация логических (протоколов) портов.

B.10 Исчерпание ресурса

- Недостатки в программном или аппаратном средстве, которые приводят к истощению ресурсов памяти (например, буферов) в системе.

[1)] DSLAM (Digital Subscriber Line Access Multiplexer) — Мультиплексор доступа к цифровой абонентской линии.

[2)] Руткит (rootkit) — Программа или набор программ для сокрытия следов присутствия злоумышленника.

- Недостатки в программном или аппаратном средстве, которое потребляет наибольшее количество ресурсов центрального процессора в системе.
- Ошибки в оборудовании или программах, ограничивающие пропускную способность канала связи.
- Недостатки в программном или аппаратном средстве, создающие ненужные сообщения, снижающие пропускную способность.
- Например, множество циклов программ, циклов маршрутов.

B.11 Несанкционированное сетевое сканирование и тестовые сообщения

- Сканирование портов/эхо-тестирование. Атакующий может выполнить общедоступные программы сканирования хоста, который подсоединен к сети. Услуги хоста для устройств, контролирующих порт, будут реагировать, возможно, предоставляя информацию атакующему.
- Сканирование для поиска уязвимостей (например, nessus[1]), сетевое отображение (например, NMAP[2]). Атакующий может выполнить общедоступные программы на хосте, подключенном к сети, которая запрашивает конфигурацию устройства и топологию сети.
- Несанкционированный удаленный доступ к резидентным программам или функциям на устройстве (например, использование руткита для обеспечения тайны).

B.12 Компрометация данных приложения абонента

- Несанкционированное раскрытие, создание, изменение, копирование, удаление данных, созданных и (или) используемых приложений, доступных абоненту.
- Включает информацию, хранящуюся в сети поставщика услуг от имени абонентов (например, информационные ресурсы видео на цифровой видеозаписи).

B.13 Кража контента

- Захват цифрового сертификата для управления контентом и даже широковещательным/перераспределенным потоком других абонентов.
- Захват пакетов по домашней сети и подсети IP.
- Выход из аналоговых портов вывода на внешнее записывающее устройство.
- Выход из цифрового порта на внешнее записывающее устройство.
- Количество осуществленных воспроизведений превышает существующее ограничение на них.
- Доступ к незаконному контенту (например, пиратской информации).
- Обход систем условного доступа (CAS).
- Копирование информации с дискового запоминающего устройства на сервер или устройство конечного пользователя.

B.14 Доступ к нежелательному контенту

- Случайный доступ.
- Умышленный доступ.

B.15 Компрометация информации об абоненте

- Использование социальной инженерии для получения информации об абоненте.
- Несанкционированное раскрытие, создание, изменение, копирование или удаление информации об абоненте (например, адрес, номер телефона, число учетных записей, информация о кредитных картах, записи DNS/ENUM[3] и т. д.).
- Ограниченная ответственность отдельных абонентов.

B.16 Перехват сеанса связи и услуги маскировки имён

- Имитирование легитимного поставщика услуг. Захват цифрового сертификата от поставщика, чтобы изменить потоки и включить любую информацию по желанию.
- Имитация легитимного сетевого устройства, видео-сервера, игрового сервера, сервера DRM[4].
- Атака «Человек посредине».
- Перенаправление видеопотока к несанкционированному устройству.

---

[1] Nessus — Программа для автоматического поиска и обнаружения известных уязвимостей и брешей в защите информационных систем.

[2] NMAP — Утилита, предназначенная для сканирования IP-сетей с любым количеством объектов и определения состояния объектов сканируемой сети (портов и соответствующих им служб).

[3] ENUM (Electronic Number Mapping System) — Электронная система отображения номеров.

[4] DRM (Digital Rights Management) — Управления правами на цифровые материалы.

B.17 Несанкционированное управление

- Несанкционированное использование встроенного приложения по управлению или выполнение команд управления. Например, манипулирование с настройками модема для блокировки определенных услуг.
- Ложные/измененные сообщения протокола управления. Например, манипулирование с настройками модема для блокировки или разрешения определенных протоколов (например, SNMP).
- Изменение удаленных сообщений по управлению (например, MITM[1)]).
- Незаконные действия абонентов по самообеспечению. Например, реконфигурация стробирующего сигнала для удаления ограничения полосы пропускания с целью получения медленного соединения для других абонентов или увеличения пропускной способности для себя.
- Санкционированный агент управления, выполняющий несанкционированные действия.
- Несанкционированное управление содержимым, например, загрузка, удаление содержимого или изменение даты начала работы (даты, когда содержимое становится доступным для публичного просмотра).
- Несанкционированное управление абонентами, например, несанкционированное предоставление абоненту деятельности, включая повышение/понижение абонентских привилегий просмотра визуального отображения.

[1)] MITM (man-in-the-middle) — Атака методом перехвата сообщений и подмены ключей.

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 27000:2009	IDT	ГОСТ Р ИСО/МЭК 27000—2012 «Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Общий обзор и терминология»
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»
Примечание — В настоящей таблице использовано следующее условное обозначение степени соответствия стандартов: - IDT — идентичные стандарты.		

УДК 006.034: 004.056: 004.057.2 ОКС 35.040

Ключевые слова: информационная технология, безопасность сети, мера и средство контроля и управления, сетевой сценарий, риск сетевой безопасности, угроза безопасности, метод проектирования безопасности

Редактор *Н.С. Рагузина*
Технический редактор *В.Н. Прусакова*
Корректор *Е.Ю. Мирофанова*
Компьютерная верстка *Е.А. Кондрашовой*

Сдано в набор 18.01.2019. Подписано в печать 30.01.2019. Формат 60×84⅛. Гарнитура Ариал.
Усл. печ. л. 4,18. Уч.-изд. л. 3,35.

Подготовлено на основе электронной версии, предоставленной разработчиком стандарта

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

gost.e-ecolog.ru