ФЕДЕРАЛЬНОЕ АГЕНТСТВО

ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ

ПРЕДВАРИТЕЛЬНЫЙ НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

ПНСТ 301— 2018/ ИСО/МЭК 24767-1:2008

Информационные технологии

БЕЗОПАСНОСТЬ ДОМАШНЕЙ СЕТИ

Часть 1

Требования безопасности

(ISO/IEC 24767-1:2008, IDT)

Издание официальное

Москва
Стандартинформ
2018

gost.e-ecolog.ru

Предисловие

1 ПОДГОТОВЛЕН Федеральным государственным бюджетным образовательным учреждением высшего образования «Российский экономический университет им. Г.В. Плеханова» (ФГБОУ ВО «РЭУ им. Г.В. Плеханова») на основе собственного перевода на русский язык англоязычной версии международного 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 4 сентября 2018 г. № 38-пнст

4 Настоящий стандарт идентичен международному стандарту ИСО/МЭК 24767-1:2008 «Информационные технологии. Безопасность домашней сети. Часть 1. Требования безопасности» (ISO/IEC 24767-1:2008, «Information technology — Home network security — Part 1: Security requirements», IDT)

Правила применения настоящего стандарта и проведения его мониторинга установлены в ГОСТ Р 1.16—2011 (разделы 5 и 6).

Федеральное агентство по техническому регулированию и метрологии собирает сведения о практическом применении настоящего стандарта. Данные сведения, а также замечания и предложения по содержанию стандарта можно направить не позднее чем за 4 мес до истечения срока его действия разработчику настоящего стандарта по адресу: 117997 Москва, Стремянный переулок, д.36, ФГБОУ ВО «РЭУ им. Г.В. Плеханова» и в Федеральное агентство по техническому регулированию и метрологии по адресу:109074 Москва, Китайгородский проезд, д.7, стр.1.

*В случае отмены настоящего стандарта соответствующая информация будет опубликована в ежемесячном информационном указателе «Национальные стандарты» и также будет размещена на официальном сайте Федерального агентства по техническому регулированию и метрологии в сети Интернет (*gost.e-ecolog.ru

© Стандартинформ, оформление, 2018

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 Термины, определения и сокращения 1
2.1 Термины и определения 1
2.2 Сокращения 2
3 Соответствие 2
4 Требования безопасности внутренних домашних электронных систем и сетей 2
4.1 Общие положения 2
4.2 Безопасность домашней электронной системы 3
4.3 Вопросы, связанные с безопасностью домашних электронных сетей, не рассматриваемые в настоящем стандарте 6
5 Возникающие угрозы безопасности 7
5.1 Общие положения 7
5.2 Угрозы, связанные с постоянно активным подключением 7
5.3 Угрозы, связанные с линиями электропередач 7
5.4 Угрозы, связанные с беспроводной связью 8
5.5 Угрозы по причине сложности системы устройств 8
5.6 Множественные и разнообразные потребности пользователей 8
5.7 Разнообразные области применения 8
6 Модель обеспечения безопасности 9
6.1 Введение 9
6.2 Домашняя электронная система на один дом, управляемая владельцем (OSS) 9
6.3 Домашняя электронная система на один дом, управляемая третьей стороной (ESS) 9
6.4 Домашняя электронная система на несколько домов, управляемая третьей стороной (ESM) . . . 9
7 Анализ угроз 10
7.1 Общие положения 10
7.2 Несанкционированный доступ 10
7.3 Вредоносные программы и конфигурация домашней сети 11
7.4 Отказ в обслуживании 11
7.5 Непреднамеренное изменение данных в процессе передачи 12
7.6 Ошибки пользователей 12
7.7 Отказы системы 12
7.8 Провайдеры услуг, связанных с безопасностью 12
8 Требования безопасности 12
8.1 Общие положения 12
8.2 Контроль доступа 13
8.3 Аутентификация данных и сообщений 14
8.4 Контроль удаленного доступа 14
8.5 Защита средств связи 14
8.6 Межсетевые экраны 15
8.7 Защита от вирусов 15
8.8 Защита от атак типа «отказ в обслуживании» 15
8.9 Аудит 16
8.10 Восстановление 16
9 Требования к решениям по безопасности 16
9.1 Общие положения 16
9.2 Различные уровни служб безопасности для различных областей применения в доме 16
9.3 Удобство 17
Приложение А (справочное) Сравнение требований безопасности офисных ИТ-систем и домашней электронной системы 18
Библиография 19

Введение

ИСО (Международная организация по стандартизации) и МЭК (Международная электротехническая комиссия) образуют специализированную систему всемирной стандартизации. Государственные органы, являющиеся членами ИСО или МЭК, участвуют в разработке международных стандартов посредством технических комитетов. Участие в разработке стандарта в конкретной области может принять любой заинтересованный орган, являющийся членом ИСО или МЭК. Другие международные организации, правительственные и неправительственные, контактирующие с ИСО и МЭК, также принимают участие в работе.

В области информационных технологий ИСО и МЭК учредили Объединенный технический комитет ИСО/МЭК СТК 1. Проекты международных стандартов, подготовленные Объединенным техническим комитетом, рассылаются национальным комитетам на голосование. Публикация в качестве международного стандарта требует утверждения не менее чем 75% национальных комитетов, участвующих в голосовании.

Официальные решения или соглашения МЭК и ИСО по техническим вопросам выражают, насколько это возможно, международное согласованное мнение по относящимся к делу вопросам, так как каждый технический комитет имеет представителей от всех заинтересованных национальных комитетов — членов МЭК и ИСО.

Публикации МЭК, ИСО и ИСО/МЭК имеют форму рекомендаций для международного использования и принимаются национальными комитетами — членами МЭК и ИСО именно в таком понимании. Несмотря на все приложенные усилия для обеспечения точности технического содержания публикаций МЭК, ИСО и ИСО/МЭК, МЭК или ИСО не несут ответственности за то, каким образом они используются или за их неправильную трактовку конечным пользователем.

В целях обеспечения международной унификации (единой системы) национальные комитеты МЭК и ИСО обязуются обеспечить максимальную прозрачность применения международных стандартов МЭК, ИСО и ИСО/МЭК, насколько это позволяют государственные и региональные условия данной страны. Любое расхождение между публикациями ИСО/МЭК и соответствующими национальными или региональными стандартами должно быть четко обозначено в последних.

ИСО и МЭК не предусматривают процедуры маркировки и не несут ответственности за любое оборудование, заявленное на соответствие одному из стандартов ИСО/МЭК.

Все пользователи должны удостовериться в использовании последнего издания настоящей публикации.

МЭК или ИСО, их руководство, сотрудники, служащие или представители, включая отдельных экспертов и членов их технических комитетов, а также члены национальных комитетов МЭК или ИСО не несут ответственности за несчастные случаи, материальный ущерб или иной нанесенный ущерб, прямой или косвенный, или за затраты (включая судебные издержки), понесенные в связи с публикацией или вследствие использования настоящей публикации ИСО/МЭК или другой публикации МЭК, ИСО или ИСО/МЭК.

Особого внимания требует нормативная документация, цитируемая в настоящей публикации. Использование ссылочных документов необходимо для правильного применения настоящей публикации.

Обращается внимание на то, что некоторые элементы настоящего международного стандарта могут быть объектом патентных прав. ИСО и МЭК не несут ответственности за определение какого-либо или всех таких патентных прав.

Международный стандарт ИСО/МЭК 24767-1 был разработан Подкомитетом 25 «Взаимосвязь оборудования информационных технологий» Объединенного технического комитета ИСО/МЭК 1 «Информационные технологии».

Перечень всех имеющихся в настоящее время частей серии ISO/МЭК 24767 под общим названием «Информационные технологии. Безопасность домашней сети» представлен на сайте МЭК.

ПРЕДВАРИТЕЛЬНЫЙ НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

Информационные технологии

БЕЗОПАСНОСТЬ ДОМАШНЕЙ СЕТИ

Часть 1

Требования безопасности

Information technology. Home network security. Part 1. Security requirements

Срок действия — с 2019—02—01
до 2020—02—01

1 Область применения

Настоящий стандарт определяет требования к защите домашней сети от внутренних или внешних угроз. Стандарт служит основанием для разработки систем безопасности, защищающих внутреннюю среду от различных угроз.

Требования безопасности рассматриваются в настоящем стандарте относительно неформально. Несмотря на то, что многие вопросы, рассмотренные в настоящем стандарте, служат руководством по разработке систем безопасности как внутренней сети, так и сети Интернет, они носят характер неофициальных требований.

К внутренней (домашней) сети подключены различные устройства (см. рисунок 1). Устройства «сети бытовых приборов», «развлекательные аудио-/видео-» устройства и устройства для работы с «информационными приложениями» имеют различные функции и рабочие характеристики. Настоящий стандарт содержит средства для анализа рисков по каждому подключенному к сети устройству и определения требований безопасности для каждого устройства.

2 Термины, определения и сокращения

2.1 Термины и определения

В настоящем стандарте применены следующие термины и определения:

2.1.1 **бытовая электроника** (brown goods): Аудио-/видеоустройства, которые в основном используются в развлекательных целях, например телевизор или DVD-рекордер.

2.1.2 **конфиденциальность** (confidentiality): Свойство, обеспечивающее недоступность и неразглашение информации неуполномоченным лицам, организациям или процессам.

2.1.3 **аутентификация данных** (data authentication): Служба, используемая для обеспечения корректной верификации заявленного источника данных.

2.1.4 **целостность данных** (data integrity): Свойство, подтверждающее, что данные не были изменены или уничтожены неразрешенным образом.

2.1.5 **аутентификация пользователя** (user authentication): Сервис для обеспечения корректной проверки идентификационной информации, представленной участником коммуникации, при том что служба авторизации обеспечивает доступ идентифицированного и авторизованного пользователя к конкретному устройству или приложению домашней сети.

2.1.6 **бытовая техника** (white goods): Устройства, применяемые в повседневном обиходе, например кондиционер, холодильник и т.д.

Издание официальное

2.2 Сокращения

В настоящем стандарте использованы следующие сокращения:

Аудио/видео — аудиоустройства/визуальные устройства;

CD — (Compact Disc) компакт-диск;

DDoS — (Distributed Denial of Service) распределенная атака типа «отказ в обслуживании»;

DoS — (Denial of Service) отказ в обслуживании;

DRM — (Digital Rights Management) управление цифровыми правами;

DTV — (Digital TeleVision) цифровое телевидение;

DVD — (Digital Versatile Disc) компакт-диск / формата DVD;

ESM — (Externally Supported Multiple homes HES) домашняя электронная система на несколько домов, управляемая третьей стороной;

ESS — (Externally Supported Single home HES) домашняя электронная система на один дом, управляемая третьей стороной;

HES — (Home Electronic System) домашняя электронная система;

ICT — (Information and Communication Technology) информационно-коммуникационные технологии (ИКТ);

IP — (Internet Protocol) интернет-протокол;

IPSec — (IP Security protocol) протокол безопасности интернет-протокола;

IPv4 — (Internet Protocol version 4) интернет-протокол, версия 4;

IPv6 — (Internet Protocol version 6) интернет-протокол, версия 6;

IT — (Information Technology) информационные технологии (ИТ);

MPEG — (Moving Picture Expert Group) стандартный способ упаковки полнометражных видеозаписей;

OSS — (Owner supported single home HES) домашняя электронная система на один дом, управляемая владельцем;

PPC — (Pocket Personal Computer) карманный персональный компьютер (КПК);

PC — (Personal Computer) персональный компьютер (ПК);

TCP — (Transmission Control Protocol) протокол управления передачей;

TLS — (Transport Layer Security) протокол безопасности транспортного уровня;

URL — (Uniform Resource Locator) система унифицированных адресов ресурсов;

VCR — (Video Cassette Recorder) кассетный видеомагнитофон;

VoIP — (Voice over Internet Protocol) голосовая связь по интернет-протоколу.

3 Соответствие

В настоящем стандарте содержатся методические указания без каких-либо требований соответствия.

4 Требования безопасности внутренних домашних электронных систем и сетей

4.1 Общие положения

С быстрым развитием Интернета и связанных с ним сетевых технологий появилась возможность установки связи между компьютерами в офисах и домах с внешним миром, что обеспечивает доступ ко множеству ресурсов. Сегодня технологии, которые стали основой этого успеха, достигли наших домов и обеспечивают возможность подключения приборов так же, как и персональных компьютеров. Таким образом, они не только позволяют пользователям отслеживать и контролировать свои бытовые приборы, находясь как внутри, так и вне дома, но и создавать новые сервисы и возможности, например удаленное управление бытовой техникой и ее обслуживание. Это означает, что обычная компьютерная среда дома преобразуется во внутреннюю домашнюю сеть, объединяющую множество устройств, безопасность которых также будет необходимо обеспечить.

Необходимо, чтобы жильцы, пользователи и владельцы как дома, так и системы, доверяли домашней электронной системе. Цель безопасности домашней электронной системы — обеспечение доверия к системе. Поскольку многие компоненты домашней электронной системы находятся в работе непрерывно, 24 часа в день, и автоматически обмениваются информацией с внешним миром, информационная безопасность необходима для обеспечения конфиденциальности, целостности и доступности данных и системы. Надлежащим образом реализованное решение по безопасности подразумевает, например, что доступ к системе и сохраненным, поступающим и исходящим данным получают только авторизованные пользователи и процессы, и что пользоваться системой и вносить в нее изменения могут только авторизованные пользователи.

Требования безопасности для сети HES могут быть описаны несколькими способами. Этот стандарт ограничен ИТ-безопасностью сети HES. Тем не менее, безопасность информационных технологий должна выходить за рамки самой системы, поскольку дом должен функционировать, хотя и с ограниченными возможностями, в случае отказа ИТ-системы. Интеллектуальные функции, которые обычно поддерживаются сетью HES, могут выполняться также при разрыве связей системы. В таких случаях можно понять, что существуют требования безопасности, которые не могут быть частью самой системы, но при этом система не должна запрещать реализацию резервных решений.

Существует ряд лиц, заинтересованных в вопросах безопасности. Домашней электронной системе должны доверять не только жители и владельцы, но и провайдеры услуг и контента. Последние должны быть уверены, что предлагаемые ими услуги и контент используются только разрешенным способом. Однако одной из основ безопасности системы является то, что отвечать за нее должен конкретный администратор службы безопасности. Очевидно, что такая ответственность должна быть возложена на жителей (владельцев системы). Не имеет значения, занимается ли этим администратор лично или отдает на аутсорсинг. В любом случае ответственность несет администратор системы безопасности. Вопрос доверия провайдеров услуг и контента к домашней электронной системе и их уверенности в том, что пользователи применяют их услуги и контент надлежащим образом, определяется договорными обязательствами между сторонами. В договоре, например, могут быть перечислены функции, компоненты или процессы, которые должна поддерживать домашняя электронная система.

Архитектура домашней электронной системы различна для разных видов домов. Для любой модели может существовать свой определенный набор требований безопасности. Ниже приведено описание трех различных моделей домашних электронных систем с различными наборами требований безопасности.

Очевидно, что некоторые требования безопасности более важны, чем остальные. Таким образом, понятно, что поддержка некоторых мер противодействия будет опциональной. Кроме того, меры противодействия могут различаться по качеству и стоимости. Также для управления и поддержания таких мер противодействия могут потребоваться различные навыки. В данном стандарте сделана попытка разъяснить мотивы перечисленных требований безопасности и тем самым позволить разработчикам домашней электронной системы определить, какие функции безопасности должна поддерживать конкретная домашняя система, а также, с учетом требований по качеству и усилий по обеспечению управления и обслуживания, какой механизм следует выбрать для таких функций.

Требования безопасности внутренней сети зависят от определения безопасности и «дома», а также от того, что понимается под «сетью» в этом доме. Если сеть — это просто канал, соединяющий отдельный ПК с принтером или кабельным модемом, то для обеспечения безопасности домашней сети достаточно обеспечить безопасность этого канала и оборудования, которое он соединяет.

Однако если в доме находятся десятки, если не сотни, объединенных в сеть устройств, при этом некоторые из них относятся к домохозяйству в целом, а некоторые принадлежат находящимся в доме людям, понадобится предусмотреть более сложные меры безопасности.

4.2 Безопасность домашней электронной системы

4.2.1 Определение домашней электронной системы и безопасности системы

Домашнюю электронную систему и сеть можно определить как набор элементов, которые обрабатывают, передают и хранят информацию, а также управляют ею, обеспечивая связь и интеграцию множества компьютерных устройств, а также устройств управления, контроля и связи, находящихся в доме.

Кроме того, домашние электронные системы и сети обеспечивают взаимосвязь развлекательных и информационных устройств, а также приборов связи и безопасности, и имеющейся в доме быто-

вой техники. Такие устройства и приборы будут обмениваться информацией, ими можно управлять и контролировать их, находясь в доме, либо удаленно. Соответственно, для всех внутренних домашних сетей потребуются определенные механизмы безопасности, защищающие их повседневную работу.

Безопасность сети и информации можно понимать как способность сети или информационной системы на определенном уровне противостоять случайным событиям или злонамеренным действиям. Такие события или действия могут поставить под угрозу доступность, аутентичность, подлинность и конфиденциальность сохраненных или переданных данных, а также связанных с ними сервисов, предлагаемых через такие сети и системы.

Инциденты информационной безопасности можно объединить в следующие группы:

- электронное сообщение может быть перехвачено, данные могут быть скопированы или изменены. Это может стать причиной ущерба, причиненного как путем нарушения права личности на конфиденциальность, так и путем злоупотребления перехваченными данными;

- несанкционированный доступ к компьютеру и внутренним компьютерным сетям обычно выполняется со злым умыслом на копирование, изменение или уничтожение данных и может распространяться на автоматическое оборудование и системы, находящиеся в доме;

- вредоносные атаки в сети Интернет стали вполне обычным явлением, а в будущем более уязвимой может также стать телефонная сеть;

- вредоносное программное обеспечение, такое как вирусы, может выводить из строя компьютеры, удалять или изменять данные, либо перепрограммировать бытовую технику. Некоторые атаки вирусов были весьма разрушительными и дорогостоящими;

- искажение информации о физических или юридических лицах может стать причиной значительного ущерба, например клиенты могут скачать вредоносное программное обеспечение с веб-сайта, маскирующегося под доверенный источник, могут быть расторгнуты контракты, а конфиденциальная информация может быть направлена ненадлежащим получателям;

- многие инциденты информационной безопасности связаны с непредусмотренными и непреднамеренными событиями, например стихийными бедствиями (наводнениями, штормами и землетрясениями), отказами аппаратного или программного обеспечения, а также с человеческим фактором.

Помимо таких инцидентов существуют другие связанные с безопасностью вопросы, также важные для дома, например надежность системы. Защита, в том числе физическая, не входит в понятие информационной безопасности. Защита связана с предотвращением нанесения вреда людям или зданиям. Физическая защита подразумевает защиту дома, аппаратного обеспечения домашней электронной системы при помощи соответствующих дверных и оконных замков. Такие вопросы, несмотря на их важность для дома, не рассматриваются в настоящем стандарте.

Поскольку абсолютную надежность или безопасность домашней электронной системы невозможно обеспечить, необходимо исходить из того, что может произойти отказ всей системы или ее части. Такую потерю работоспособности системы следует учитывать. Соответственно необходимо разработать процессы восстановления, чтобы иметь возможность вновь перезапускать эти компоненты данных и системы, обработать соответствующие части данных и системы, а также возможно поддерживать отказоустойчивые технологии и процедуры.

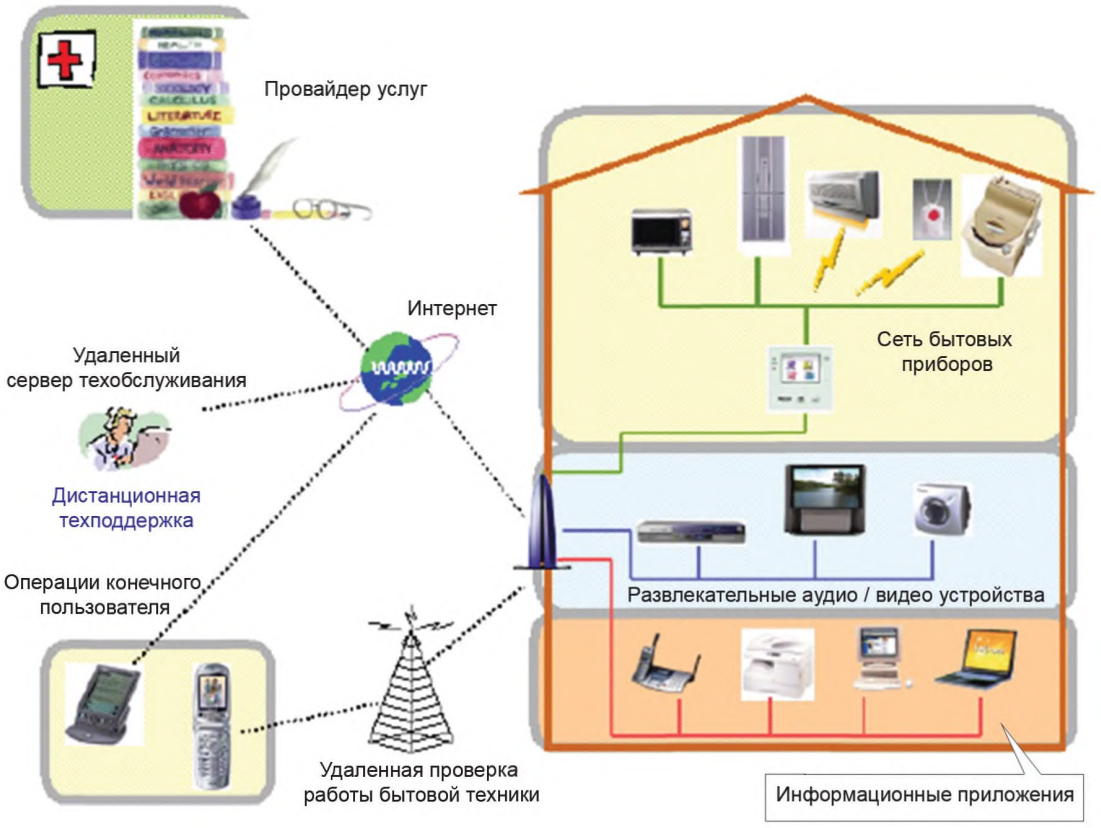
Решение для аварийной ситуации очевидно не входит в объем домашней электронной системы, однако она должна допускать наличие таких решений.

Требования безопасности внутренних сетей связаны не только с сетью HES, они также необходимы для внешней среды, которая может оказывать значительное влияние на все сервисы, от операций, которые совершают жильцы дома, и удаленной поддержки поставщиков, до приложений — разнообразных служб. При взаимодействии внутренних сетей с внешним миром вопросы безопасности внутренних сетей окажутся аналогичными тем, с которыми сталкиваются отделы информационно-коммуникационных технологий (ИКТ) компаний. И большинство из них подробно рассмотрены (см., например, серию ИСО/МЭК 18028) в приложении А.

Однако все же существует ряд различий между приложениями для домашнего и корпоративного применения, инфраструктурой внутренней домашней сети и корпоративными сетями, потребностями жильцов дома и работников предприятия. Соответственно необходимо в первую очередь представить некоторые существующие модели внутренних сетей и проиллюстрировать некоторые области их применения, а затем рассмотреть эти модели с точки зрения возможных угроз внутренним сетям и наконец подробно сформулировать требования безопасности.

На рисунке 1 представлена концептуальная модель внутренней сети. Дом соединен с внешним миром с помощью интернет-шлюза. В доме находятся разнообразные устройства, возможно подпадающие под некоторые категории, показанные на рисунке 1.

И наконец при тщательном изучении возможностей внутренних сетей становится ясно, что требования безопасности можно разделить на две части: защита от внешних угроз и защита от внутренних угроз. На рисунке 2 показаны различные требования к обеспечению безопасности для различных видов внутренней среды.



Сеть бытовых приборов: Может включать в себя стиральную машину, кондиционер и электрическую рисоварку, может поддерживать операции по включению/выключению как изнутри, так и извне.

Аудио-/видеосеть: Может включать в себя телевизоры, DVD-проигрыватели и другую аудио-/ видеотехнику, может поддерживать подключение к сети Интернет через ТВ (обеспечивающее сервисы, отличные от предлагаемых при подключении ПК).

Различные составные системы домашних кинотеатров, которые могут совместно использовать те же аудио-/видеоресурсы, что и аудио-/видеотехника и ПК.

Сеть ИТ-оборудования: Может включать в себя домашние серверы, принтеры, ПК, ноутбуки, КПК, мобильные телефоны, VoIP-серверы и переносные телефоны и поддерживать распечатку с экрана цифрового ТВ на принтер, подключенный к ПК, поиск данных приложений, сохраненных на ПК, КПК или мобильных телефонах, аудио-/видеосвязь на основе VoIP

Рисунок 1 — Концептуальная модель внутренних домашних сетей

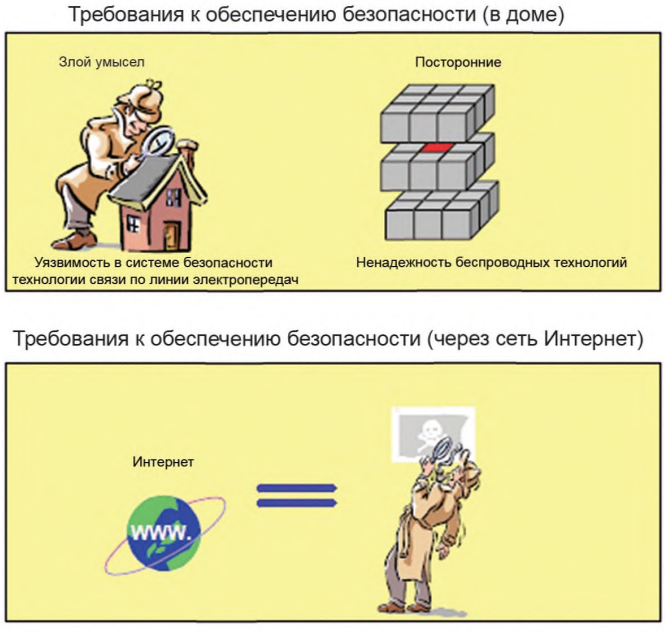


Рисунок 2 — Различные требования к обеспечению безопасности для разнообразных видов внутренней среды

Внутри дома проблемы безопасности могут быть связаны с ненадежными техническими средствами информационных сетей, такими как беспроводная связь или линии электропередач, и контролем доступа для различных пользователей/сценариев пользования. За пределами дома проблемы безопасности будут практически такими же, как и уязвимости в системе безопасности в сети Интернет.

4.3 Вопросы, связанные с безопасностью домашних электронных сетей, не рассматриваемые в настоящем стандарте

4.3.1 Управление цифровыми правами

Управление цифровыми правами (DRM) связано с проблемой незаконного копирования и распространения цифровых материалов, защищенных авторским правом. Типичными примерами являются компьютерное программное обеспечение, музыка и фильмы. Их можно передавать по сети или на носителе, например на CD.

Провайдеры контента заинтересованы, чтобы владелец (житель) дома не осуществлял незаконное копирование контента. Поскольку это является угрозой для провайдера контента, а не для владельца/жителя дома, данный вопрос не рассматривается в настоящем стандарте.

4.3.2 Родительский контроль

Во многих домах, где есть дети, у родителей может возникнуть потребность в защите своих детей от доступа к данным, которые могут причинить им вред, таким как фильмы со сценами насилия или порнографические материалы. Такую защиту можно обеспечить с помощью средств контроля доступа. Существуют различные формы такой защиты. Одна из них — запрещение доступа к нежелательным провайдерам услуг. Другая — разрешение доступа только к избранным разрешенным провайдерам. Кроме того, данные могут иметь метку о том, что они не подходят для детей, тем самым, на основании такой информации запускается механизм контроля доступа. Последний метод работоспособен только при наличии соответствующей метки данных и при условии, что эта метка распознается методом контроля доступа. Однако ни один из этих аспектов невозможно гарантировать.

4.3.3 Снижение криминогенности продукции и услуг

Криминогенными называют продукцию и услуги, которые с определенной вероятностью могут стать объектом или орудием преступления. В настоящее время эта область не регулируется стандартами, однако следует отметить, что в будущем могут появиться технические требования к домашней

электронной системе, направленные на снижение криминогенности как изделий, установленных в домах, так и услуг.

4.3.4 Вопросы пользования

Существует ряд общих указаний по пользованию системой. Всем пользователям домашней электронной системы будут полезны общие указания о том, как работать с системой (например, делать покупки через интернет-магазины), и о том, как поддерживать и обновлять систему, чтобы избежать уязвимостей, например вирусов, «червей» и т.д.

4.3.5 Вопросы, связанные с провайдерами услуг

У провайдеров услуг существуют требования безопасности, направленные на то, чтобы пользователи и владельцы домашних электронных систем доверяли данным, которые получают от них. Это верно в отношении всех типов провайдеров услуг, например тех, кто предоставляет данные для пользователей (например, аудио-/видеосервисы), тех, кто предоставляет услуги для дома (например, контроль охранной сигнализации), и тех, кто предоставляет сервисы для домашней электронной системы (например, обновления для программного обеспечения и встроенного ПО). Все провайдеры таких услуг должны гарантировать пользователям и владельцам системы, что поступающие данные можно принимать и что такие данные поступают из доверенного источника и защищены в процессе передачи как от нарушения конфиденциальности, так и от внесения изменений со злым умыслом.

4.3.6 Вопросы, связанные с аварийными ситуациями

В любой сложной электронной системе, имеющей программное обеспечение, возможны проблемы, например отказ оборудования, ошибки в программном обеспечении, человеческие ошибки, грозовой разряд, затопление или намеренное повреждение. Поэтому важно предусмотреть технологии и процедуры на случай аварийной ситуации для защиты ответственных элементов дома. Например, дверные замки, управляемые домашней электронной системой, должны быть оборудованы аварийным механизмом, с тем чтобы жильцы в любом случае могли открыть и закрыть двери.

4.3.7 Вопросы, связанные с аутсорсингом

Существует вопрос поддержания безопасности домашней электронной системы в случаях, когда поддержка обработки информации выполняется сторонней организацией. В договоре должны быть по крайней мере рассмотрены риски, средства контроля защиты и соответствующие процедуры. [4] содержит примеры вопросов, которые могут быть урегулированы в подобном договоре.

5 Возникающие угрозы безопасности

5.1 Общие положения

Угрозы внутренним сетям в основном возникают по причине сложности системы устройств, от различных типов физических носителей и разнообразных используемых протоколов связи. Некоторые угрозы безопасности, возникающие при использовании некоторых наиболее известных структур внутренних сетей, перечислены ниже.

5.2 Угрозы, связанные с постоянно активным подключением

Постоянно активное широкополосное соединение делает доступ в Интернет быстрым и легким. К сожалению, оно также обеспечивает широкую возможность проникновения интернет-угроз, таких как хакерские атаки и вирусы, в ваш дом, офис или бизнес.

Бытовые устройства с постоянно активным подключением особенно уязвимы для атак, поскольку они находятся в режиме онлайн 24 часа в сутки и постоянно подключены к сети Интернет с одного и того же IP-адреса.

5.3 Угрозы, связанные с линиями электропередач

Вопросы обеспечения безопасности данных возникают для домов, которые используют одни и те же линии электропередач, в особенности на участках старой застройки. Большинство соседних домов подключены к одной и той же подсети линий электропередач, подключенной в свою очередь к одному распределительному трансформатору. Передаваемые по линии передач команды из одного дома могут достигать устройств в другом доме, находящемся по соседству, и мешать управлению данными устройствами.

5.4 Угрозы, связанные с беспроводной связью

Беспроводные сети подвержены множеству новых угроз безопасности, которых не существовало для традиционных проводных сетей. По своей природе беспроводные сети уязвимы для различных атак, таких как пассивный перехват информации, активное вмешательство, утечка секретной информации, искажение данных, имитация и отказ в обслуживании. Пользователю-злоумышленнику больше нет необходимости получать физический доступ к сетевой среде. Он просто может находиться в диапазоне передачи транслирующего узла, чтобы перехватить передаваемые пользователем сообщения.

5.5 Угрозы по причине сложности системы устройств

В число устройств, которые потенциально может объединять внутренняя домашняя сеть, входят бытовая техника, бытовая электроника, оборудование связи, компьютерное оборудование, системы освещения, системы технического обслуживания дома, системы сигнализации и мониторинга и так далее. Некоторые из них, например бытовая техника и системы освещения, отличаются ограниченностью ресурсов и не могут обеспечить сложные вычисления. Однако некоторые информационные или аудио-/видеоустройства поддерживают различные приложения, и им необходима большая надежность системы безопасности для защиты данных. Функции безопасности для таких устройств строятся на других принципах.

5.6 Множественные и разнообразные потребности пользователей

Говоря о потребностях пользователей, необходимо признать, что каждый из них индивидуален и имеет особые потребности, исходя из образа жизни, экономического положения, образования и так далее. Различные типы домов предполагают различные требования безопасности: проблемы безопасности семьи из двух человек существенно отличаются от проблем семьи, где есть дети-подростки.

Большинство подростков стремятся к определенной степени независимости. Это может предполагать владение личными устройствами, подключенными к сети, и, вероятно, приглашение в дом друзей. Что если подростки не захотят показывать своим родителям, что записано на их DVD-дисках? Что если их друзья захотят подключить свои устройства к внутренней сети?

С другой стороны, родители могут захотеть установить определенные ограничения для своих детей. Например, родители могут захотеть сделать так, чтобы дети не имели доступа к телепрограммам в рабочие дни после 19:00, либо запретить детям младше 12 лет просмотр фильмов категории R.

Если в доме проживает один человек, все находящиеся в доме устройства принадлежат ему, поэтому требований в части контроля доступа может не быть. Однако домовладелец, тем не менее, может пожелать делегировать ряд полномочий провайдерам услуг для целей обслуживания, и тогда встает задача обеспечения безопасности сети от доступа извне.

5.7 Разнообразные области применения

Области применения внутренних сетей можно условно разделить на следующие категории:

a) домашняя автоматизация (управления домом, безопасности и контроля дома);

b) развлечения;

c) информация и связь.

Требования безопасности для таких разных областей применения могут отличаться.

В отношении домашней автоматики производители бытовой техники включают в свою продукцию сетевой интерфейс, с тем чтобы провайдеры услуг с разрешения владельцев дома могли удаленно контролировать состояние оборудования и расходных материалов. Кроме того, необходимо принять меры к тому, чтобы управляющие команды поступали только с согласованных, надежных источников.

В отношении развлечений пользователи всегда стремятся подключить свои домашние развлекательные устройства совместно, чтобы распределять цифровой контент и аудио и совместно пользоваться им в пределах всего дома.

Однако удобство подключения порождает проблемы с контролем доступа. Кроме того, владельцы устройств могут пожелать, чтобы авторизованные пользователи могли иметь доступ только к определенному контенту.

В отношении информации и связи защита конфиденциальности приобрела большую важность, чем другие вопросы, поскольку связь может быть предназначена для передачи определенной финансовой отчетности, информации о банковских счетах и кредитных картах, а также личной информации.

6 Модель обеспечения безопасности

6.1 Введение

Создание сложной домашней электронной системы, отличающейся надежностью, и управление ею таким образом, чтобы она оставалась надежной и безопасной, — весьма непростая задача. Такая задача зависит от методов обеспечения выполнения политики безопасности, которые, в свою очередь, зависят от применения методик безопасности, таких как контроль доступа, защита целостности передаваемой информации и т.д. В части безопасности домашней электронной системы можно выделить три совершенно различных сценария или модели. Неудивительно, что все они сходны с различными формами предприятий. Однако угрозам и требованиям безопасности в доме зачастую придают меньшее значение, чем на предприятии. В данном стандарте представлены следующие три модели:

- домашняя электронная система на один дом, управляемая владельцем (OSS);
- домашняя электронная система на один дом, управляемая третьей стороной (ESS);
- домашняя электронная система на несколько домов, управляемая третьей стороной (ESM).

6.2 Домашняя электронная система на один дом, управляемая владельцем (OSS)

Первая и наиболее простая модель включает в себя отдельную компоненту — собственно домашнюю электронную систему (включающую в себя один системный блок или более), которая полностью управляется владельцем или жильцом дома. Это примерно соответствует индивидуальному пользованию компьютерной системой с подключением к сети Интернет с сегодняшней точки зрения. Для такой архитектуры также характерны многие угрозы, которым подвергается подобная компьютерная система, и ее уязвимости.

Однако большинство владельцев (жильцов) в целом незнакомы с компьютерной безопасностью, и им были бы полезны методические указания в виде контрольных списков требований по безопасности. Более эффективным может стать привлечение профессиональной поддержки безопасности домашней электронной системы. Это предполагает следующий вариант модели.

6.3 Домашняя электронная система на один дом, управляемая третьей стороной (ESS)

Второй сценарий также рассчитан на одиночные дома. Однако ответственность за домашнюю электронную систему и, в частности, за ее безопасность и надежность, возлагается не на владельца (жильца), а на профессионального провайдера ИТ-услуг. Весьма похожим образом организовано большинство небольших предприятий, масштабы которых не позволяют им иметь собственный ИТ-отдел. Провайдер услуг может обеспечить выбор надлежащих решений в области безопасности, корректную установку и обслуживание. Преимущество такой схемы в том, что за безопасность и надежность, формирование и поддержание которых отнимает много усилий и времени, отвечают профессионалы.

Однако можно сделать еще один шаг и передать поддержание, эксплуатацию домашней электронной системы и работу с ней профессиональному провайдеру услуг. Это предполагает третью модель.

6.4 Домашняя электронная система на несколько домов, управляемая третьей стороной (ESM)

В третьей модели провайдер услуг обслуживает несколько домов. Такие дома могут находиться в отдалении друг от друга. Однако также это может быть многоквартирный дом либо группа таунхаусов, где квартиры в доме или таунхаусы на участке обслуживаются локальным отделом. Одно из крупнейших отличий между первыми двумя моделями и этой состоит в том, что в первых двух входящая и исходящая связь с домом является прямой, а в данной модели связь осуществляется через ESM.

В таком сценарии владелец (жильцы) дома играют ту же роль, что и работодатель или отдел в крупной организации, имеющей профессиональный ИТ-отдел. Это решение будет наиболее удобным и надежным для большинства владельцев и жильцов домов. Если бы такая архитектура была самой распространенной, ее успех наверняка зависел бы от ежемесячных затрат на такие услуги. Такие затраты могли бы быть уравновешены, если бы страховые компании снижали премии для клиентов, которые пользуются подобными услугами.

7 Анализ угроз

7.1 Общие положения

В анализе угроз рассматривается возможный ущерб, причиняемый владельцу (жильцу) дома от действий, связанных с домашней электронной системой, внутренней сетью или любыми элементами информации в системе.

Угрозы домашней системе и сетям аналогичны угрозам, которые создаются для корпоративной системы и сетей. Однако различные угрозы отличаются по значимости для конфигурации и приложений не производственной, а домашней сети. Например, если отказ от выполнения (отрицание того, что сделка состоялась) очевидно является значительной проблемой для банка или брокерской фирмы, то для дома, где сделка скорее всего носит частный и непроизводственный характер, это менее серьезно. И наоборот, предприятиям не имеет смысла скрывать, в какое время дня их сети наиболее загружены, тогда как частные пользователи вполне могут пожелать скрыть трафик, который показывает, дома ли они.

Домашние пользователи могут чувствовать себя менее уязвимыми, поскольку их сетевые устройства отличаются от выполняющих ответственные функции корпоративных систем, содержащих жизненно важную для компании информацию, и вероятность атак против них не очень высока. Однако такая точка зрения устарела. Устройства, подключенные ко внутренней сети, могут быть не конечными объектами для хакерских атак, а отправной точкой для атак на другие устройства, являющиеся целью злоумышленников.

Поскольку, как правило, невозможно определить причину непосредственно во время атаки, домашние пользователи должны достаточно полно представлять себе угрозы и знать, какие решения существуют.

Выявлены следующие виды угроз для домашних систем и сетей.

7.2 Несанкционированный доступ

Очевидно, что для домашних пользователей важно, для чего и какие действия санкционированы, и доступ к какой информации на каждом из устройств предоставлен. Например, в случае с кассетным видеомагнитофоном и его контроллером доступ к видеомагнитофону предоставлен только контроллеру, соответствующему видеомагнитофону. Другими словами, контроллер, которым владеет или пользуется человек, не являющийся членом семьи, например гость, сосед или пользователь с доступом через Интернет, не получит доступа к видеомагнитофону, принадлежащему конкретной семье. Таким образом, существует потребность в защите домашней электронной системы от неавторизованных пользователей и от событий, которые инициированы неавторизованными системами в доме и (или) вне его.

Неавторизованный нарушитель может, например являться автоматической системой, запрограммированной на поиск уязвимых сообщений, или лицом, которое перехватило или, иначе, нарушило целостность канала связи.

Доступ может быть пассивным или активным. Пассивный перехват — это подслушивание, фактически, чтение чужого трафика. Активный перехват может подразумевать изменение содержания сообщения, удаление или изменение части сообщения, или изменение его протокольной управляющей информации, в частности заголовка (в том числе адреса получателя или отправителя).

Наиболее опасен активный (локальный или удаленный) нарушитель, который может манипулировать домашней электронной системой, установить троянскую программу или предоставить услуги от имени владельца (жителя) дома. Троянская программа может предоставить неавторизованным пользователям и процессам доступ к данным и системе, тем самым нарушив конфиденциальность и подлинность данных, а также, возможно, их доступность и работоспособность системы.

Одна из форм неавторизованного доступа — когда активный нарушитель (самозванец) притворяется полномочным пользователем, например владельцем дома. Это называется подменой. Самозванец также может притвориться провайдером услуг, имеющим договор с владельцем дома.

Еще один метод, которым самозванец может предстать перед домашней системой авторизованным пользователем, — это перехватить подлинное сообщение и переслать его позже. Это называется атакой повторного воспроизведения. Например, если самозванец может перехватить сообщение для системы охранной сигнализации дома с командой на отключение, воспроизведение именно этого сообщения позднее может привести к нежелательному результату.

Пассивный нарушитель, способный только считывать данные, также может представлять собой угрозу. Данные могут носить конфиденциальный характер либо они могут указывать на то, что дома

никого нет. Первая категория может содержать персональные данные, а примером второй могут служить настройки системы отопления, которые могут быть весьма информативными для потенциального взломщика. Подобные угрозы существуют для всех трех моделей. Поэтому важно обеспечить доступ к домашней электронной системе и ее данным только для авторизованных пользователей и сделать так, чтобы сторонним системам было непросто получить подобные данные от домашней электронной системы.

Даже если при коммуникации задействованы службы обеспечения подлинности и конфиденциальности, пассивный нарушитель может узнать многое о внутренней сети, отслеживая отправителей и получателей информации, и время каждого сообщения. Это называется анализом трафика.

Угроза нарушения конфиденциальности выше для двух последних моделей (ESS и ESM), поскольку они предполагают наличие авторизованного доступа к системе не только у жителей, но и у сторонних организаций, занятых поддержкой домашней электронной системы. Рекомендуется ограничивать такие организации только обязанностями по обслуживанию домашней электронной системы и не давать им доступа к важной конфиденциальной информации. Эта проблема не технического характера, она связана с доверительными взаимоотношениями между провайдерами услуг и их клиентами.

7.3 Вредоносные программы и конфигурация домашней сети

Вредоносные программы могут, например, проникнуть в домашнюю электронную систему через коммуникационный канал или измененная им конфигурация сети может загрузить зараженное программное обеспечение из дома. Наиболее очевидные примеры вредоносного программного обеспечения — вирусы, проникающие в домашнюю электронную систему. Вирус может разрушить данные и программное обеспечение и привести систему в неработоспособное состояние. Это угрозы подлинности программного обеспечения и информации о конфигурации на устройствах доступа и устройствах, подключенных к домашней сети.

Троянская программа — несанкционированное программное обеспечение, проникающее в дом или в устройство доступа внутри подлинного сообщения. Проникнув в дом, троянская программа может оказаться в процессоре любого устройства, подключенного к сети. Например, троянская программа может находиться внутри перехваченного транспортного потока MPEG в виде конфиденциальных данных и быть записана в процессоре цифрового телевизора. Затем она может воспользоваться ресурсами процессора телевизора и цифровой домашней сети, чтобы поставить под угрозу безопасность внутренней сети.

О «червях» и вирусах достаточно много пишут и в технических, и в популярных изданиях. «Червь» — это программа, которая может самовоспроизводиться и рассылать свои копии от одного компьютера к другому по сети. При проникновении «червь» может активироваться и вновь самовоспроизводиться и распространяться. Кроме того, «червь» обычно выполняет некоторые нежелательные функции. «Червь», который проник во внутреннюю сеть, может распространиться по ней на множество устройств; если «червь» выполнит вредоносные функции, например сотрет постоянную память устройства, владелец дома может обнаружить, что множество устройств, от цифрового телевизора до тостера, вышли из строя.

Вирус — это код, встроенный в программу, который встраивает свои копии в одну программу или более, а также выполняет несанкционированные функции на главном компьютере. В отличие от «червя», вирус не будет активно распространяться на процессоры, подключенные к внутренней сети, т. е. он повредит единичное устройство. Однако устройства, работа которых критична для внутренней сети, могут начать работать непредсказуемым и нежелательным образом.

Некоторые атаки могут поставить под угрозу конфигурацию домашней сети, изменяя информацию, связанную с безопасностью. Три примера такой информации — адреса внешних серверов, доверенные открытые ключи и пароли, используемые в процессе авторизации, а также фильтры нежелательного трафика на интерфейсе доступа.

7.4 Отказ в обслуживании

Отказ в обслуживании нарушает работоспособность системы. В случае некоторых установок неработоспособное состояние вызывает незначительные неудобства, и требуется лишь повторить попытку позднее. В других случаях это может стать серьезной угрозой дому, например в случае отключения системы сигнализации.

Атаки типа «отказ в обслуживании» реализуются посредством лавинной маршрутизации бесполезного трафика на сеть доступа и препятствования поступления подлинных сообщений во внутреннюю сеть. Входящие сообщения также могут вызвать попытки ответа со стороны внутренней сети, привязывая ресурсы к устройству доступа, что негативно отражается на исходящем трафике. Внутренняя сеть может пострадать от атаки типа «отказ в обслуживании» или действий невольного участника. Если компьютер, подключенный к внутренней сети, находится под угрозой, атакующая сторона может воспользоваться им для лавинной рассылки пакетов без ведома владельца дома. Это называется распределенной атакой типа «отказ в обслуживании» (DDoS).

7.5 Непреднамеренное изменение данных в процессе передачи

Может случиться так, что информация случайно подвергается изменению или повторно воспроизводится в процессе передачи, таким образом сообщение интерпретируется неверно. Незначительные изменения отдельных бит данных можно исправить с помощью кода с коррекцией стандартной ошибки, но для реального обеспечения целостности и защиты подлинности данных в процессе их передачи необходимы криптографические технологии.

7.6 Ошибки пользователей

Существует риск, что авторизованный пользователь допустит ошибку и может активировать ненадлежащие услуги либо дать ошибочные параметры в команде. Такие ошибки, как правило, имеют меньшее значение, если жилец находится дома, по сравнению с ситуацией его отсутствия. Один из способов свести к минимуму такие ошибки — это предоставить пользователю устройство с простым пользовательским интерфейсом, который несложен в использовании и осуществляет проверку вводимых значений. Еще одна контрмера — ограничить набор команд, которые можно активировать, находясь вне дома.

7.7 Отказы системы

Отказы домашней электронной системы неизбежны. Они могут быть связаны с нарушением безопасности либо с нестабильностью системы, отключением питания, грозовым разрядом и многими другими причинами. В результате часть данных или все данные пропадают, и система перестает работать. Таким образом, существует потребность в процессе восстановления, а возможно, в технологиях и процедурах на случай аварийной ситуации.

7.8 Провайдеры услуг, связанных с безопасностью

Наконец, необходимо отметить, что провайдерам услуг, связанных с безопасностью, которые в основном используют третий вариант модели домашней электронной сети (ESM), необходимо реализовать целый пакет сложных мер безопасности. Они аналогичны тем, которые принимают множество организаций, обладающих конфиденциальной информацией, и должны быть активны 24 часа в сутки семь дней в неделю. Однако такие требования не описаны в настоящем стандарте.

8 Требования безопасности

8.1 Общие положения

Владелец/жилец дома может создать свои доверительные отношения с помощью различных устройств и процедур. Доверие к домашней электронной системе в целом подразумевает комбинацию технических контрмер (например, межсетевая защита, антивирусное программное обеспечение и т.д.), процедурные меры (такие как обновление программного обеспечения, мероприятия по резервному копированию и восстановлению, обучение и информирование по вопросам безопасности), а также различные прочие меры, например, такие как страхование. Сюда включаются следующие методические указания и процедуры, например по установке, конфигурации, обслуживанию, обновлению и использованию системы.

Многие механизмы и сервисы, связанные с безопасностью, разработанные против потенциальных угроз в деловой среде, могут не подходить для домашних сетей из-за ограниченности ИТ-возможностей, например датчиков и бытовой техники.

Ниже приводится набор угроз безопасности различной степени серьезности для защиты домашней электронной системы, от которых существуют решения, повышающие доверие к ней. Таблица 1 содержит сводную информацию о ряде механизмов защиты от угроз, перечисленных в разделе 7.

Таблица 1 — Угрозы безопасности и соответствующие меры защиты

Угрозы	Меры защиты
Активный перехват: добавление сообщений, изменение данных	Аутентификация данных, целостность данных
Открытие файлов и приложений	Управление, программное обеспечение
Установка нового программного обеспечения	Управление, программное обеспечение
Обновление программного обеспечения в режиме онлайн	Аутентификация
Обновление программного обеспечения в локальном режиме	Управление, программное обеспечение
Отказ в обслуживании	Межсетевая защита, контроль доступа, входные фильтры
Несанкционированное прослушивание	Службы сохранения конфиденциальности информации
Подмена	Аутентификация пользователя/устройства (часть процедуры контроля доступа)
Удаленный доступ	Контроль доступа
Повторное воспроизведение	Функция антиповтора, аутентификация с защитой от повторного воспроизведения
Отказ от выполнения	Криптография открытого ключа
Отказ системы	Восстановление, мероприятия на случай аварийной ситуации, отказоустойчивость
Анализ трафика	«Холостое заполнение» сообщений
Несанкционированный доступ к передаваемым данным	Службы сохранения конфиденциальности информации
Несанкционированный доступ к данным в системе	Контроль доступа
Несанкционированный доступ к системе	Контроль доступа
Ошибка пользователя	Пользовательский интерфейс, контроль удаленного доступа
Вирус, «червь», троянская программа:	
Открытие файлов и приложений	Управление, программное обеспечение
Установка нового программного обеспечения	Управление, программное обеспечение
Обновление программного обеспечения в режиме онлайн	Аутентификация
Обновление программного обеспечения в локальном режиме	Управление, программное обеспечение

8.2 Контроль доступа

Несанкционированный доступ к домашней электронной системе и ее сервисам является наиболее серьезной угрозой, как было показано в разделе 7. Защитой от этой угрозы служит хороший механизм контроля доступа. Рационально давать разный уровень прав доступа разным людям. Для первой модели (OSS) важно отличать пользователя, действующего как администратор системы, от того же лица в роли обычного пользователя. Целесообразным является предоставление нескольких уровней

прав доступа. Есть несколько функций, которые могут быть разрешены всем, но к некоторым другим функциям доступ должен быть ограничен, например для детей. Также разумно, находясь вне дома, налагать большие ограничения на права доступа по сравнению с периодом времени, когда вы находитесь в доме (см. удаленный доступ и контроль ниже).

Во-первых, необходима запись и регистрация авторизованных пользователей. Важно тщательно вести работу с зарегистрированными и авторизованными пользователями. Например, рационально немедленно отзывать права доступа у пользователей, если изменился их стереотип поведения, например права гостя, приходящего в дом, должны быть отозваны, если гость уходит раньше запланированного изначально времени.

Во-вторых, надлежащая аутентификация пользователя, т. е. проверка подлинности пользователя, является обязательным условием работы системы контроля доступа. Только после успешной верификации личности авторизованного пользователя домашней электронной системой такому пользователю могут быть предоставлены корректные права доступа к запрошенному ресурсу. Однако первым шагом является требование регистрации авторизованных пользователей. В случае первой модели, описанной выше, это несложно сделать, но для двух других, и особенно для третьей архитектуры, важно, чтобы провайдер услуг корректно зарегистрировал владельца (жильцов) дома и пользователей.

Подмену можно предотвратить с помощью контроля доступа с надлежащей аутентификацией в сочетании со службой защиты целостности данных.

Однако аутентификация не может эффективно противостоять атакам повторного воспроизведения. Тем не менее, от атак повторного воспроизведения можно защититься с помощью параметров, переменных во времени и обеспечивающих уникальность и своевременность. Простой способ — это проверка на наличие повторных сообщений, что можно сделать, например, сопоставив поле временной метки или порядкового номера с ранее сохраненными сообщениями.

Кроме контроля физического и логического доступа в здание необходимо защищать чувствительные устройства домашней электронной системы. Например, если техобслуживание проводит представитель сторонней организации, разумно потребовать аутентификации, прежде чем предоставлять доступ в здание и к оборудованию. Также любые удаленные обновления и обслуживание требуют аутентификации.

8.3 Аутентификация данных и сообщений

Еще одной задачей является надлежащая аутентификация сообщений от устройства, запрашивающего услуги, в том случае, когда сообщения в любом направлении (от пользователя к дому или от дома к пользователю) требуют аутентификацию. Требование аутентификации сообщений от пользователя к дому является очевидным, поскольку существуют сообщения, которые активируют определенные действия внутри дома. Однако разумно, чтобы ответные сообщения от дома к пользователю тоже проходили аутентификацию во избежание ситуации, когда нарушитель вводит ложное подтверждение или подтвержденное сообщение, тогда как подлинное сообщение не поступило. Также уведомления и ответы от дома, подлинность которых проверена, могут, в конечном итоге, содержать информацию о состоянии, например, температуры в доме или о том, включена ли система сигнализации.

8.4 Контроль удаленного доступа

Зачастую житель желает получить доступ к домашней электронной системе, находясь вне дома. Поэтому необходимо предоставить доступ к системе извне. Для этого необходимы механизмы аутентификации, описанные выше. В отличие от деловой среды, где пользователь обычно имеет доступ только к ИТ-среде и соответственно получает обычные права доступа, домашняя среда поддерживает дистанционное управление многими устройствами в доме. Это может предъявлять иные требования к контролю доступа, с меньшим количеством прав доступа при удаленном подключении, с тем чтобы ограничить количество операций и параметров, которые можно использовать. Поскольку непреднамеренные действия сложнее зафиксировать, находясь вне дома, во избежание ошибок необходимо особое внимание к пользовательскому интерфейсу устройства, используемого для удаленного доступа.

8.5 Защита средств связи

В целом для пользователя нежелательно, чтобы какой-либо пассивный нарушитель узнал содержание сообщения.

Это касается не только тела сообщения (которое содержит команду, подлежащую исполнению), но также и полей заголовка, которые могут раскрыть информацию об устройстве. Например, поле заголовка [To:] будет содержать URL адресата, который также может указывать на тип устройства и его местонахождение. Возможно, пользователь не желает, чтобы кто-либо знал, есть ли в доме телевизор и тем более в какой именно комнате он расположен.

В домашней среде существует четыре вида связи. Проводная связь в доме, беспроводная в доме, а также проводная и беспроводная из дома и в дом. Все они возможны за исключением данных, передаваемых по кабелю в пределах дома, нуждаются в защите конфиденциальности и подлинности, с тем чтобы только авторизованные пользователи получали доступ к данным и чтобы была возможность выявить несанкционированные изменения. Требования безопасности проводных средств связи в отдельном доме зависят от используемого кабеля. Если существует возможность распознавания связи вне дома, то необходимость в защите конфиденциальности есть. Кроме того, если стороннее лицо может изменять или вносить данные в систему, также необходима защита целостности информации.

Защиту от анализа трафика можно обеспечить путем создания ложного трафика, скрывающего полезные сообщения.

Защиту данных в процессе передачи осуществляют службы защиты конфиденциальности, целостности и секретности и службы аутентификации адресата. Важно, чтобы такие решения были основаны на международных признанных стандартах, чтобы обеспечить возможность взаимодействия с внешним миром.

8.6 Межсетевые экраны

Если у пользователей в доме возникает потребность в защите своих устройств и данных от вторжения извне, им необходимо использовать межсетевой экран. Межсетевой экран обычно располагается между локальной сетью и сетью Интернет. Дополнительные межсетевые экраны могут применяться для разделения локальной сети на несколько доменов безопасности для защиты отдельных устройств. Это может использоваться для контроля входящего и исходящего трафика в сети.

Основная цель применения межсетевых экранов — предотвращение хакерских атак на сеть извне. Ответы системы на отказы в обслуживании должны быть рассчитаны на то, чтобы не позволить потенциальному взломщику извлечь полезную информацию о системе, например физические IP-адреса.

Межсетевой экран эффективен в случае использования протокола IPv4 и может быть не эффективен в случае использования недавно появившегося протокола IPv6.

8.7 Защита от вирусов

Вирус, «червь» или троянская программа в домашней электронной сети — большая проблема любого пользователя. Защита от них не является чисто техническим вопросом. Многое связано с поведением пользователей домашней электронной системы. Поэтому необходимо строго следовать политике, которая, например, предписывает осторожность при открытии вложений в электронные сообщения из незнакомых источников. Еще одну преграду вирусным атакам можно обеспечить с помощью механизма контроля доступа, с отказом в доступе любому лицу, которое не может пройти процесс аутентификации.

С технической точки зрения имеются различные методы выявления такого вредоносного программного обеспечения. Однако стандарта, который можно применить к защите от вирусов, не существует. Новые вирусы внедряются в сеть Интернет ежедневно, и многие компании трудятся над разработкой защиты от них. Вирус может попасть в систему через входящую связь, например через вложение в электронное сообщение, а также путем загрузки зараженного программного обеспечения в домашнюю электронную сеть. Предлагаемый подход подразумевает установку пакета антивирусного программного обеспечения от одного из производителей антивирусных программных средств и регулярное обновление этого пакета.

8.8 Защита от атак типа «отказ в обслуживании»

Существует два вида отказов в обслуживании. Один происходит, когда разрешенный пользователь домашней электронной системы пытается получить доступ к удаленному сервису и получает отказ. В подобном случае возможно, что сервис, к которому пытаются получить доступ, перегружен или подвергся атаке типа «отказ в обслуживании». Имеющиеся у разрешенного пользователя варианты весьма ограничены. В таком случае можно попробовать другой сервис или подождать, пока нагрузка трафика снизится либо сервис будет перезагружен.

Другой вариант — домашняя электронная система подвергается атаке типа «отказ в обслуживании». Защита от атак типа «отказ в обслуживании» в реальном времени практически невозможна. Фактически механизмы безопасности сами по себе не могут быть эффективны против атак типа «отказ в обслуживании», поскольку очень просто перегрузить любую защиту отправкой большого количества ложных сообщений. Тщательная разработка и реализация протокола и устройства доступа может уменьшить истощение ресурсов, тем самым лавинная маршрутизация связывает части внутренней сети или устройства доступа. Например, если устройство доступа распознает, что на него поступают запросы открыть одновременно 5000 TCP-подключений, оно может перейти в состояние тревоги, в котором оно игнорирует дополнительные поступающие запросы, которые не прошли надлежащую криптографическую аутентификацию, и отдает приоритет в своей выходной очереди сообщениям, исходящим из дома.

Чтобы внутренняя сеть не смогла непроизвольно стать участником распределенной атаки типа «отказ в обслуживании», необходимо принять меры к тому, чтобы избежать установки незаконного программного обеспечения. Устройства контроля доступа с реализованным входным фильтром, как указано в [12], предотвращает использование ложных IP-адресов. Однако это не работает, если нарушитель использует действительные сетевые адреса. Входные фильтры отслеживают источник атаки значительно легче, потому что источником трафика является адрес источника пакетов. Дополнительным преимуществом является то, что ответ жертвы возвращается атакующей системе, тем самым предотвращая дополнительный ущерб. Для осуществления фильтрования на входе устройство контроля доступа блокирует любые пакеты с адресом источника, не исходящим из домашней сети.

8.9 Аудит

Аудит — это механизм безопасности, который не реализует никакого защитного механизма, но обычно используется для контроля и проверки того, работают ли механизмы безопасности должным образом. При аудите регистрируются конфиденциальные операции, связанные с безопасностью. Необходимо решить, какие операции, связанные с безопасностью, подлежат регистрации. Если регистрируются все операции, связанные с безопасностью, в большом объеме сохраненных данных может оказаться затруднительно выявить любые непреднамеренные события. С другой стороны, если регистрируется очень малое количество конфиденциальных операций, взлом может быть не выявлен.

По крайней мере те операции, которые связаны с настройкой параметров безопасности, как, например, регистрация пользователей и все неуспешные попытки аутентификации, необходимо регистрировать. Даже данные об успешной аутентификации бывают полезны, поскольку помогают определить, кто пользовался системой в то или иное время.

8.10 Восстановление

В случае отказа системы необходимо иметь возможность ее перезапустить. Не имеет значения, вышла ли система из строя в результате взлома или из-за иного вида отказа. Наиболее подходящий способ подготовки к восстановлению — регулярное резервное копирование системы. Частота резервного копирования зависит от того, как часто в домашнюю электронную систему вносятся изменения.

9 Требования к решениям по безопасности

9.1 Общие положения

Требования, приведенные в данной статье, определяют форму и функциональные возможности решения по безопасности, а не тип защиты.

9.2 Различные уровни служб безопасности для различных областей применения в доме

Зачастую для различных видов деятельности принимают разные уровни безопасности. Например, управление температурой кондиционера в спальне из гостиной не требует безопасности того же уровня, как управление устройством в доме извне. В связи с различными факторами внутренних сетей практически невозможно разработать решение «под ключ» для создания служб безопасности, пригодных одновременно для различных моделей домашних сетей, разнообразных нужд пользователей и областей применения.

Таким образом, существует требование, чтобы решение по безопасности могло поддерживать несколько уровней безопасности в отдельном доме.

9.3 Удобство

В целом частные пользователи выбирают решения, которые не отличаются высокой ценой и не требуют обширных знаний для использования.

Поэтому выбранные решения должны по возможности соответствовать следующим требованиям:

a) низкая стоимость;

b) невысокая сложность;

c) простота в использовании (по возможности автоматическая работа).

Также для частных пользователей чрезвычайно важна надежность. Если процесс нуждается в обслуживании, не является простым в применении и быстрым в установке, маловероятно, что он будет внедрен. Пользователи не создают и не администрируют сложные системы. Это особенно важно для описанной выше модели безопасности OSS, но также и для ESS и, в меньшей степени, для модели ESM.

Приложение А
(справочное)

Сравнение требований безопасности офисных ИТ-систем и домашней электронной системы

Офисная ИТ-система представляет собой информационную систему, которая в отличие от домашней электронной системы, используется только для управления ИТ-устройствами, такими как принтеры и прочее. Внутренняя сеть и требования безопасности таким образом могут существенно различаться. Однако безопасность внешней сети имеет значительно больше сходств. Поскольку домашний офис является частью домашней электронной системы, эта система объединяет в себе все внешние требования, как офисная система. Кроме того, существует несколько других угроз для дома, которые необходимо учитывать.

Существуют следующие дополнительные требования по внешней информационной безопасности домашней электронной системы по сравнению с домашней и офисной ИТ-средой:

- как и некоторые офисы, умный дом подключен к сети 24 часа в сутки 7 дней в неделю;
- существуют требования не только удаленного доступа к системе, но и дистанционного управления устройствами в доме, например отоплением. Однако при дистанционном управлении устройствами им присваиваются права доступа, отличные от прав при управлении ими изнутри дома. Таким образом необходимо различать, осуществляется ли управление изнутри дома или дистанционно. Этого можно достичь, например, если позволить шлюзу направлять коммуникации на механизм контроля доступа, отличный от того, который используется при доступе к системе изнутри дома;
- оборудование, с которого осуществляется управление устройствами в доме, в частности при дистанционном управлении, должно быть сконструировано так, чтобы избежать ошибок. Соответственно существуют требования безопасности к пользовательскому интерфейсу устройства, с которого осуществляется дистанционное управление;
- на случай отказа системы должны быть предусмотрены решения для аварийных ситуаций, т. е. должна также существовать возможность управления устройствами, которые обычно управляются через домашнюю электронную систему, без этой системы. Примером могут служить дверные замки. Вышедшая из строя система не должна блокировать работу таких устройств.

Кроме того, домашняя электронная система должна быть отказоустойчивой. Это означает, что в случае отказа устройства должны прийти в состояние, которое не может нанести ущерб дому или жильцам. Это требование более всего касается устройств, которыми управляет система, а не самой системы.

Библиография

[1] ISO/IEC 10116, Information technology — Security techniques — Modes of operation for an nbit block cipher (Информационные технологии. Методы защиты. Режимы работы для алгоритма *n*-разрядного блочного шифра)

[2] ISO/IEC 18028 (all parts), Information technology — Security techniques — IT network Security ((все части) Информационные технологии. Методы защиты. Безопасность компьютерных сетей)

[3] ISO/IEC 18033-3, Information technology — Security techniques — Encryption algorithms —Part 3: Block ciphers (Информационные технологии. Методы защиты. Алгоритмы шифрования. Часть 3. Блочные шифры)

[4] ISO/IEC 27002, Information technology — Security techniques — Code of practice for information security management (Информационные технологии. Методы защиты. Практическое пособие по обеспечению безопасности информационных технологий)

[5] Письмо Еврокомиссии (2001) 298

[6] Сетевая и информационная безопасность: Предлагаемый подход к Европейской политике по обеспечению сетевой и информационной безопасности

[7] gost.e-ecolog.ru numero=298&ElementsPerPage=20&tri=cote&CL=en

[8] Фрайер А.О., Карлтон П., Кохер П.С. SSL-протокол, версия 3.0

[9] Диркс Т. и Аллен С. TLS-протокол, версия 1.0, RFC 2246, Техническая комиссия Интернета, январь 1999 г.

[10] Кент С., Аткинсон Р. Архитектура системы безопасности для межсетевого протокола, RFC 2401, Техническая комиссия Интернета, ноябрь 1998 г.

[11] NIST, FIPS PUB 197 «Симметричный алгоритм блочного шифрования (AES)», ноябрь 2001 г.

[12] RFC 2267 Входные фильтры сетей: Отражение атак типа «отказ в обслуживании» с использованием ложного IP-адреса источника

УДК 004.056:006.354 ОКС 35.110, 35.200, 35.240.99

Ключевые слова: защита прав потребителя, конкурентоспособность, безопасность работ и услуг

БЗ 8—2018/36

Редактор *Н.А. Аргунова*
Технический редактор *И.Е. Черепкова*
Корректор *Е.Д. Дульнева*
Компьютерная верстка *Л.А. Круговой*

Сдано в набор 06.09.2018. Подписано в печать 24.09.2018. Формат 60×84 1/8. Гарнитура Ариал.
Усл. печ. л. 2,79. Уч.-изд. л. 2,51.
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