Методы и проблемы оценивания угроз безопасности.

Стандарты информационной безопасности.

Обзор

1. Определение безопасной системы.
2. Угрозы безопасности.
3. Современные стандарты безопасности инфокоммуникационных сетей.

*Определение безопасной **системы***

Под информационной безопасностью понимается состояние защищенности информационной *системы*, включая собственно информацию и поддерживающую ее инфраструктуру. Информационная система находится в состоянии защищенности, если обеспечены ее *конфиденциальность, доступность и целостность*.

Конфиденциальность (confidentiality) — это гарантия того, что секретные данные будут доступны только тем пользователям, которым этот доступ разрешен; такие пользователи называются легальными, или авторизованными.

Доступность (availability) — это гарантия того, что авторизованные пользователи всегда получат доступ к данным.

Целостность (integrity) — это гарантия сохранности данными правильных значений, которая обеспечивается запретом неавторизованным пользователям каким-либо образом изменять, модифицировать, разрушать или создавать данные.

Требования безопасности могут меняться в зависимости от назначения информационной системы, характера используемых данных и типа возможных угроз. Трудно представить систему, для которой были бы не важны свойства целостности и доступности, но свойство конфиденциальности не всегда является обязательным. Например, если вы публикуете информацию в Интернете на веб-сервере и вашей целью является сделать ее доступной для самого широкого круга людей, конфиденциальность не требуется. Однако требования целостности и доступности остаются актуальными.

Действительно, если вы не предпримете специальных мер по обеспечению целостности системы, злоумышленник может изменить данные на вашем сервере и нанести этим ущерб вашему предприятию. Преступник может, например, внести изменения в помещенный на веб-сервере прайс-лист, что негативно отразится на конкурентоспособности вашего предприятия, и т.п.

*Определение безопасной **системы***

Не менее важным в данном примере является и обеспечение доступности данных. Затратив немалые средства на создание и поддержание сервера в Интернете, предприятие вправе рассчитывать на отдачу: увеличение числа клиентов, количества продаж и т. д. Однако существует вероятность того, что злоумышленник предпримет атаку, в результате которой помещенные на сервер данные станут недоступными для тех, кому они предназначались. Примером таких злонамеренных действий может служить «бомбардировка» сервера пакетами, каждый из которых в соответствии с логикой работы соответствующего протокола вызывает тайм-аут сервера, что, в конечном счете, делает его недоступным для всех остальных запросов.

Понятия конфиденциальности, доступности и целостности могут быть определены не только по отношению к информации, но и к другим ресурсам вычислительной сети, таким как внешние устройства или приложения. Так, свойство конфиденциальности по отношению, например, к устройству печати можно интерпретировать так, что доступ к устройству имеют те и только те пользователи, которым этот доступ разрешен, причем они могут выполнять только те операции с устройством, которые для них определены.

Свойство доступности устройства означает его готовность к работе всякий раз, когда в этом возникает необходимость. А свойство целостности может быть определено как свойство неизменности параметров данного устройства.

Легальность использования сетевых устройств важна не только постольку - поскольку она влияет на безопасность данных. Устройства могут предоставлять различные услуги (распечатка текстов, отправка факсов, доступ в Интернет, электронная почта и т. п.), незаконное потребление которых, наносящее материальный ущерб предприятию, также является нарушением безопасности системы.

Угрозы безопасности

Угроза — любое действие, которое может быть направлено на нарушение информационной безопасности системы.

Атака — реализованная угроза.

Риск — вероятностная оценка величины возможного ущерба, который может понести владелец информационного ресурса в результате успешно проведенной атаки.

Угрозы могут исходить как от легальных пользователей сети, так и от внешних злоумышленников. В последние два года в статистике нарушений безопасности зафиксирован резкий сдвиг от внешних к внутренним угрозам. Примерно 2/3 от общего числа всех наиболее серьезных инцидентов, связанных с безопасностью, составляют нарушения со стороны легальных пользователей сетей: сотрудников и клиентов предприятий, студентов, имеющих доступ к сети учебного заведения и др. Вместе с тем внутренние атаки обычно наносят меньший ущерб, чем внешние.

Угрозы со стороны легальных пользователей делятся на *умышленные* и *неумышленные*.

К *умышленным* угрозам относятся, например, мониторинг системы с целью получения персональных данных других сотрудников (идентификаторов, паролей) или конфигурационных параметров оборудования. Это может быть также злонамеренное получение доступа к конфиденциальным данным, хранящимся на серверах и рабочих станциях сети «родного» предприятия с целью их похищения, искажения или уничтожения; прямое «вредительство» — вывод из строя сетевого программного обеспечения и оборудования. Кроме того, к умышленным угрозам относится нарушение персоналом правил, регламентирующих работу пользователей в сети предприятия: посещение запрещенных веб-сайтов, вынос за пределы предприятия съемных носителей, небрежное хранение паролей и другие подобные нарушения режима.

Угрозы безопасности

Однако не меньший материальный ущерб предприятию может быть нанесен в результате *неумышленных* нарушений персонала — ошибок, приводящих к повреждению сетевых устройств, данных, программного обеспечения.

Угрозы внешних злоумышленников, называемых также *хакерами*, по определению являются умышленными и обычно квалифицируются как преступления. Среди внешних нарушителей безопасности встречаются люди, занимающиеся этой деятельностью профессионально или просто из хулиганских побуждений. Целью, которой руководствуются внешние злоумышленники, всегда является *нанесение вреда* предприятию. Это может быть, например, получение конфиденциальных данных, которые могут быть использованы для снятия денег с банковских счетов, или установление контроля над программно-аппаратными средствами сети для последующего их использования в атаках на сети других предприятий.

Угрозы безопасности

Как правило, атака предваряется сбором информации о системе (mapping), которая помогает не только эффективно спланировать атаку, но и скрыть все следы проникновения в систему. К полезной для хакера информации относятся типы операционных систем и приложений, развернутых в сети, IP-адреса, номера портов клиентских частей приложений, имена и пароли пользователей. Часть информации такого рода может быть получена путем простого общения с персоналом (это называют социальным инжинирингом), а часть — с помощью тех или иных программ. Например, определить IP-адреса можно с помощью утилиты ping, задавая в качестве цели адреса из некоторого множества возможных адресов.

Если при очередном запуске программы ping пришел ответ, значит, произошло совпадение заданного адреса с адресом узла в атакуемой сети.

Для подготовки и проведения атак могут использоваться либо специально разработанные для этих целей программные средства, либо легальные программы «мирного» назначения. Так, последний пример показывает, как легальная программа ping, которая создавалась в качестве инструмента диагностики сети, может быть применена для подготовки атаки. При проведении атак злоумышленнику важно не только добиться своей цели, заключающейся в причинении ущерба атакуемому объекту, но и уничтожить все следы своего участия в этом. Одним из основных приемов, используемых злоумышленниками для «заметания следов», является подмена содержимого пакетов (spoofing). В частности, для сокрытия места нахождения источника вредительских пакетов (например, при атаке отказа в обслуживании) злоумышленник изменяет значение поля адреса отправителя в заголовках пакетов. Поскольку адрес отправителя генерируется автоматически системным программным обеспечением, злоумышленник вносит изменения в соответствующие программные модули так, чтобы они давали ему возможность отправлять со своего компьютера пакеты с любыми IP-адресами.

Современные стандарты ИБ инфокоммуникационных сетей

Ниже в таблице представлен список базовых официальных документов по протоколам и алгоритмам безопасности Securing IP networks.

Тип документа	Документы
IPsec	**RFC 2401** - Security Architecture for the Internet Protocol **RFC 4301** - Security Architecture for the Internet Protocol
ESP	**RFC 2406** - IP Encapsulating Security Payload (ESP) – (Изоляция секретной информации в сети IP) **RFC 4303** - IP Encapsulating Security Payload (ESP)
AH	**RFC 2402** - IP Authentication Header (Идентификация заголовка IP протокола) **RFC 4302** - IP Authentication Header

Алгоритмы аутентификации	**RFC 2104** - HMAC: Keyed Hashing for Message Authentication, 1997 (Хеширование инф. блоков аутентиф. ключами) **RFC 2403** - The use of HMAC-MD5-96 within ASP and AH, Nov 1998 **RFC 2404** - The use of HMAC-SHA-1-96 within ASP and AH, Nov 1998 **RFC 3566** - The AES-XCBC-MAC-96 Algorithm and its Use With IPsec, Sep 2003 NIST, FIPS-180-2 Secure Hash Standard (SHA-1, SHA-2, SHA-384, SHA-512), Aug 2002 **RFC4231** - Identifiers and Test Vectors for HMAC-SHA-224, HMAC-SHA-256, HMAC-SHA-384 and HMAC-SHA-512, Dec 2005 **RFC4494** - The AES-CMAC-96 Algorithm and Its Use With IPsec, Jun 2006

RFC (Request for Comments – предлагается к обсуждению)

Современные стандарты ИБ инфокоммуникационных сетей

Шифры	**RFC 2405** - The ESP DES-CBC Cipher Algorithm With Explicit IV (алгоритм кодирования с открытым ключем IV) **RFC 2410** - The Null Encryption Algorithm and Its Use With Ipsec (алгоритм шифрования нулей и его использование в IPsec) **RFC 2451** - The ESP CBC-Mode Cipher Algorithms (3DES) (алгоритмы режимов кодирования в ESP CBC) **RFC 3602** - The AES CBC-Cipher Algorithm and Its Use With IPsec **RFC 3686** - Using Advanced Encryption Standard (AES) Counter Mode With IPsec Encapsulating Security Payload (ESP) NIST, FIPS PUB 197, Advanced Encryption Standard (AES), Nov 2001 NISA, Special Publication 800-38A, Recommendation for Block Cipher Modes of Operation, Dec 2001 **RFC 4309** - Using Advanced Encryption Standard (AES) CCM Mode With IPsec Encapsulating Security Payload (ESP), Dec 2005 **RFC 4106** - The Use of Galois/Counter Mode (GCM) in IPsec Encapsulating Security Payload (ESP), Jun 2005 **RFC 4543** - The Use of Galois Message Authentication Code (GMAC) in IPsec ESP and AH, May 2006 NIST, The Galois/Counter Mode of Operation (GCM), May 2005 csrc.nist.gov/CryptoToolkit/Modes/pro posedmodes/gcm/gcm-revised-spec.pdf NIST FIPS 186-2, Digital Signature Standard, Jan 2000 fips186-2/csrc.nist.gov/publication/fips/fips186-2-change1.pdf ANSI X9.31 - RSA Digital Signature NIST FIPS 186-2, Digital Signature Standard, Jan 2000 csrc.nist.gov/publication/fips/fips186-2/fips186-2-change1.pdf ANSI X9.31 - RSA Digital Signature ANSI X9.62 - ECDSA, Elliptic Curve Digital Signature Algorithm

Современные стандарты ИБ инфокоммуникационных сетей

IKE и IKEv2	**RFC 2407** - The Internet IP Security Domain of Interpretation for ISAKMP, Nov 1998 **RFC 2408** - Internet Security Association and Key Management Protocol (ISAKMP), Nov 1998 **RFC 2409** - The Internet Key Exchange (IKE), Nov 1998 **RFC 4109** - Algorithms for Internet Key Exchange version 1 (IKEv1), May 2005 **RFC 4306** - Internet Key Exchange (IKEv2) Protocol, Dec 2005 **RFC 4434** - The AES-XCBC-PRF-128 Algorithm for the Internet Key Exchange Protocol (IKE), Feb 2006
NAT	**RFC 3022** - Traditional IP Network Address Translator (Traditional NAT), Jan 2001 **RFC 3715** - IPsec-Network Address Translation (NAT) Compatibility Requirements, Mar 2004 **RFC 3948** - VDP Encapsulation of IPsec ESP Packets, Jan 2005
SRTP	**RFC 3711** - The Secure Real-time Transport Protocol (SRTP), Mar 2004
Алгоритм Диффи-Хелмана	**RFC 2539** - Storage of Diffie-Hellman Keys in the Domain Name System (DNS), Mar 1999 **RFC 2631** - Diffie-Hellman Key Agreement Method, Jun 1999 **RFC 3526** - More Modular Exponential (MODP) Diffie-Hellman groups for Internet Key Exchange (IKE), May 2003 **RFC 5144** (Jan 2008), 4754, 4753 and 4492

Современные стандарты ИБ инфокоммуникационных сетей

Применительно к средствам защиты от НСД определены **семь классов** защищенности (1-7) *средств вычислительной техники* (СВТ) и **девять классов** (1А,1Б,1В,1Г,1Д,2А,2Б,3А,3Б) *автоматизированных систем* (АС). Для СВТ самым низким является седьмой класс, а для АС - 3Б.

Например, сертифицированная система защиты от НСД "КОБРА" соответствует требованиям 4-ого класса защищенности (для СВТ), реализует идентификацию и разграничение полномочий пользователей и криптографическое закрытие информации, фиксирует искажения эталонного состояния рабочей среды ПК (вызванные вирусами, ошибками пользователей, техническими сбоями и т.д.) и автоматически восстанавливает основные компоненты операционной среды терминала.

Подсистема разграничения полномочий защищает информацию на уровне логических дисков. Пользователь получает доступ к определенным дискам A,B,C,...,Z. Все абоненты разделены на 4 категории:

- суперпользователь (доступны все действия в системе);
- администратор (доступны все действия в системе, за исключением изменения имени, статуса и полномочий суперпользователя, ввода или исключения его из списка пользователей);
- программисты (может изменять личный пароль);
- коллега (имеет право на доступ к ресурсам, установленным ему суперпользователем).

Помимо санкционирования и разграничения доступа к логическим дискам, администратор устанавливает каждому пользователю полномочия доступа к последовательному и параллельному портам. Если последовательный порт закрыт, то невозможна передача информации с одного компьютера на другой. При отсутствии доступа к параллельному порту, невозможен вывод на принтер.

Современные стандарты ИБ инфокоммуникационных сетей

Защита данных в компьютерных сетях становится одной из самых открытых проблем в современных информационно-вычислительных системах. На сегодняшний день сформулировано три базовых принципа информационной безопасности, задачей которой является обеспечение:

- *целостности данных* - защита от сбоев, ведущих к потере информации или ее уничтожения;
- *конфиденциальности информации*;
- *доступности информации* для авторизованных пользователей.

Рассматривая проблемы, связанные с защитой данных в сети, возникает вопрос о классификации сбоев и несанкционированности доступа, что ведет к потере или нежелательному изменению данных. Это могут быть сбои оборудования (кабельной системы, дисковых систем, серверов, рабочих станций и т.д.), потери информации (из-за инфицирования компьютерными вирусами, неправильного хранения архивных данных, нарушений прав доступа к данным), некорректная работа пользователей и обслуживающего персонала. Перечисленные нарушения работы в сети вызвали необходимость создания различных видов защиты информации. Условно их можно разделить на три класса:

- средства физической защиты;
- программные средства (антивирусные программы, системы разграничения полномочий, программные средства контроля доступа);
- административные меры защиты (доступ в помещения, разработка стратегий безопасности фирмы и т.д.).

.

Современные стандарты ИБ инфокоммуникационных сетей

Одним из средств физической защиты являются системы архивирования и дублирования информации. В локальных сетях, где установлены один-два сервера, чаще всего система устанавливается непосредственно в свободные слоты серверов. В крупных корпоративных сетях предпочтение отдается выделенному специализированному архивационному серверу, который автоматически архивирует информацию с жестких дисков серверов и рабочих станций в определенное время, установленное администратором сети, выдавая отчет о проведенном резервном копировании. Наиболее распространенными моделями архивированных серверов являются Storage Express System корпорации Intel ARCserve for Windows.

Для борьбы с компьютерными вирусами наиболее часто применяются антивирусные программы, реже - аппаратные средства защиты. Однако, в последнее время наблюдается тенденция к сочетанию программных и аппаратных методов защиты. Среди аппаратных устройств используются специальные антивирусные платы, вставленные в стандартные слоты расширения компьютера. Корпорация Intel предложила перспективную технологию защиты от вирусов в сетях, суть которой заключается в сканировании систем компьютеров еще до их загрузки. Кроме антивирусных программ, проблема защиты информации в компьютерных сетях решается введением контроля доступа и разграничением полномочий пользователя. Для этого используются встроенные средства сетевых операционных систем, крупнейшим производителем которых является корпорация Novell. В системе, например, NetWare, кроме стандартных средств ограничения доступа (смена паролей, разграничение полномочий), предусмотрена возможность кодирования данных по принципу "открытого ключа" с формированием электронной подписи для передаваемых по сети пакетов.

Однако, такая система защиты **слабомощна**, т.к. уровень доступа и возможность входа в систему определяются паролем, который легко подсмотреть или подобрать.

Для исключения неавторизованного проникновения в компьютерную сеть используется комбинированный подход - пароль + идентификация пользователя по персональному "ключу". "Ключ" представляет собой пластиковую карту (магнитная или со встроенной микросхемой - смарт-карта) или различные устройства для идентификации личности по биометрической информации - по радужной оболочке глаза, отпечаткам пальцев, размерам кисти руки и т.д. Серверы и сетевые рабочие станции, оснащенные устройствами чтения смарт-карт и специальным программным обеспечением, значительно повышают степень защиты от несанкционированного доступа.

Смарт-карты управления доступом позволяют реализовать такие функции, как контроль входа, доступ к устройствам ПК, к программам, файлам и командам. Одним из удачных примеров создания комплексного решения для контроля доступа в открытых системах, основанного как на программных, так и на аппаратных средствах защиты, стала система Kerberos, в основу которой входят три компонента:

- база данных, которая содержит информацию по всем сетевым ресурсам, пользователям, паролям, информационным ключам и т.д.;
- авторизационный сервер (authentication server), задачей которого является обработка запросов пользователей на предоставление того или иного вида сетевых услуг. Получая запрос, он обращается к базе данных и определяет полномочия пользователя на совершение определенной операции. Пароли пользователей по сети не передаются, тем самым, повышая степень защиты информации;
- Ticket-granting server (сервер выдачи разрешений) получает от авторизационного сервера "пропуск" с именем пользователя и его сетевым адресом, временем запроса, а также уникальный "ключ". Пакет, содержащий "пропуск", передается также в зашифрованном виде.

Сервер выдачи разрешений после получения и расшифровки "пропуска" проверяет запрос, сравнивает "ключи" и при тождественности дает "добро" на использование сетевой аппаратуры или программ.

По мере расширения деятельности предприятий, роста численности абонентов и появления новых филиалов, возникает необходимость организации доступа удаленных пользователей (групп пользователей) к вычислительным или информационным ресурсам к центрам компаний. Для организации удаленного доступа чаще всего используются кабельные линии и радиоканалы. В связи с этим защита информации, передаваемой по каналам удаленного доступа, требует особого подхода. В мостах и маршрутизаторах удаленного доступа применяется сегментация пакетов - их разделение и передача параллельно по двум линиям, - что делает невозможным "перехват" данных при незаконном подключении "хакера" к одной из линий. Используемая при передаче данных процедура сжатия передаваемых пакетов гарантирует невозможность расшифровки "перехваченных" данных. Мосты и маршрутизаторы удаленного доступа могут быть запрограммированы таким образом, что удаленным пользователям не все ресурсы центра компании могут быть доступны.

Современные стандарты ИБ инфокоммуникационных сетей

В настоящее время разработаны специальные устройства контроля доступа к вычислительным сетям по коммутируемым линиям. Примером может служить, разработанный фирмой AT&T модуль Remote Port Securiti Device (PRSD), состоящий из двух блоков размером с обычный модем: RPSD Lock (замок), устанавливаемый в центральном офисе, и RPSD Key (ключ), подключаемый к модему удаленного пользователя. RPSD Key и Lock позволяют устанавливать несколько уровней защиты и контроля доступа:

- шифрование данных, передаваемых по линии при помощи генерируемых цифровых ключей;
- контроль доступа с учетом дня недели или времени суток.

Прямое отношение к теме безопасности имеет стратегия создания резервных копий и восстановления баз данных. Обычно эти операции выполняются в нерабочее время в пакетном режиме. В большинстве СУБД резервное копирование и восстановление данных разрешаются только пользователям с широкими полномочиями (права доступа на уровне системного администратора, либо владельца БД), указывать столь ответственные пароли непосредственно в файлах пакетной обработки нежелательно. Чтобы не хранить пароль в явном виде, рекомендуется написать простенькую прикладную программу, которая сама бы вызывала утилиты копирования/восстановления. В таком случае системный пароль должен быть "зашит" в код указанного приложения. Недостатком данного метода является то, что всякий раз при смене пароля эту программу следует перекомпилировать.

Современные стандарты ИБ инфокоммуникационных сетей

В Российской федерации информационная безопасность инфокоммуникационных сетей регламентируется ФЗ РФ №126-ФЗ от 7.07.2003 «О связи» и Государственным стандартом *ГОСТ Р 52448-2005 Защита информации. Обеспечение безопасности сетей электросвязи. Общие положения*.

ФЕДЕРАЛЬНОЕ АГЕНТСТВО
ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

ГОСТ Р 52448— 2005

Защита информации

ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ СЕТЕЙ ЭЛЕКТРОСВЯЗИ

Общие положения

В настоящем стандарте использованы нормативные ссылки на следующие стандарты:

ГОСТ Р ИСО/МЭК 15408-2—2002 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 2. Функциональные требования безопасности

ГОСТ Р ИСО/МЭК 15408-3—2002 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 3. Требования доверия к безопасности

ГОСТ Р 51275—99 Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения

1 Область применения

Настоящий стандарт предназначен для применения расположенными на территории Российской Федерации организациями, предприятиями и другими субъектами хозяйственной деятельности независимо от их организационно-правовой формы и формы собственности, которые связаны с созданием и эксплуатацией сетей электросвязи, являющимися составными компонентами сети связи общего пользования единой сети электросвязи Российской Федерации. Основными функциями сетей электросвязи являются прием, обработка, хранение, передача и предоставление требуемой информации пользователям и органам государственного управления для ее последующего применения. Сети электросвязи предназначены для оказания услуг связи любому пользователю путем предоставления открытых информационных ресурсов и информации, не содержащей сведений, составляющих государственную тайну, или информации, доступ к которой ограничен в соответствии с законодательством Российской Федерации.

Настоящий стандарт определяет терминологию, цели, задачи, принципы и основные положения обеспечения безопасности сетей электросвязи.

Положениями настоящего стандарта рекомендуется руководствоваться при:

- развитии и совершенствовании правового, организационного, экономического и научно-технического обеспечения безопасности сетей электросвязи;
- разработке проектов, программ, нормативных документов и методических рекомендаций по обеспечению безопасности сетей электросвязи и контролю их состояния;
- формировании и реализации политики безопасности операторами связи.

ВН – воздействие нарушителя;
ИТ – информационная технология;
СОБ – система обеспечения безопасности;
НСД (В) – несанкционированный доступ (воздействие).

5 Основные положения по обеспечению безопасности сетей электросвязи

5.1 Сети электросвязи являются средой переноса сообщений любого рода в виде электрических сигналов. Сообщения содержат информацию пользователя, которая может быть открытой, закодированной, зашифрованной или скремблированной (что для сети электросвязи является неопределяющим), и служебную информацию (например, адрес получателя). Сеть электросвязи должна обеспечить целостность передаваемых сообщений и своевременность их доставки адресату.

Открытость сетей электросвязи не должна означать полную доступность ко всем ее информационным ресурсам и отсутствие контроля их использования. В сети электросвязи должна быть обеспечена защита собственной, служебной информации, предназначенной для управления работой сети или служб сети.

К информационным ресурсам сетей электросвязи, требующим защиты со стороны оператора связи, могут быть отнесены:

- сведения об абонентах, базы данных;
- информация управления;
- данные, содержащие информацию пользователей (обеспечение доступности и целостности);
- программное обеспечение систем управления сетями электросвязи;
- сведения о прохождении, параметрах, загрузке (использовании) линий связи магистральных сетей;
- обобщенные сведения о местах дислокации узлов связи и установленном сетевом оборудовании;
- сведения, раскрывающие структуру используемых механизмов обеспечения безопасности сети электросвязи.

Современные стандарты ИБ инфокоммуникационных сетей

5.2 Необходимость рассмотрения проблем обеспечения безопасности сетей электросвязи обусловлена:

- динамикой развития сетей электросвязи и их интеграцией с глобальными сетями связи, в том числе с Интернет;
- совершенствованием применяемых ИТ;
- ростом числа пользователей услугами связи и расширением спектра предоставления услуг связи;
- увеличением объемов хранимой и передаваемой информации;
- территориальной рассредоточенностью сложных информационно-телекоммуникационных структур;
- недостаточностью в сетях электросвязи необходимых механизмов обеспечения безопасности.

Эти проблемы существенно повышают уязвимость сетей, способствуют появлению новых угроз безопасности и определяют необходимость комплексного решения задач по обеспечению безопасности сетей электросвязи путем:

- организации эффективного, безопасного управления и взаимодействия сетей;
- поддержания гарантированных качественных характеристик процессов обработки информации в сетях электросвязи (качества обслуживания) в условиях возможных ВН на инфокоммуникационную структуру сетей электросвязи;
- создания в сетях электросвязи надежных и защищенных каналов по пропуску определенных категорий трафика, из совокупности которого могут быть извлечены сведения, способные нанести ущерб безопасности Российской Федерации;
- противодействия проявлению терроризма на сетях электросвязи, в том числе экстремистским действиям.

5.3 Основными целями обеспечения безопасности сетей электросвязи являются:

- достижение устойчивого функционирования и успешного выполнения заданных функций сетью электросвязи, в условиях возможного ВН, способного привести к нарушению конфиденциальности, целостности, доступности или подотчетности;
- обеспечение доступности услуг связи, особенно услуг экстренного обслуживания в чрезвычайных ситуациях, в том числе и в случае террористических актов.

5.4 Основными задачами обеспечения безопасности сетей электросвязи являются:

- своевременное выявление, оценка и прогнозирование источников угроз безопасности, причин и условий, способствующих нанесению ущерба, нарушению нормального функционирования и развития сетей электросвязи на всех уровнях иерархии единой сети электросвязи России (международном, междугороднем, зоновом, местном, на уровне пользования услугами связи и т. д.);
- выявление и устранение уязвимостей в средствах связи и сетях электросвязи;
- предотвращение, обнаружение угроз безопасности, пресечение их реализации и своевременная ликвидация последствий возможных ВН, в том числе и террористических действий;
- организация системы пропуска приоритетного трафика по сети электросвязи в случае чрезвычайных ситуаций, организация бесперебойной работы международной аварийной службы;
- совершенствование и стандартизация применяемых мер обеспечения безопасности сетей электросвязи.

5.5 Оператор связи при осуществлении процесса управления функционированием сети электросвязи должен минимизировать возможные негативные ВН для обеспечения выполнения основных целей организации связи, в том числе и бизнес-процессов. Это достигается путем интегрирования в систему управления функционированием сети электросвязи процесса управления рисками.

На каждой стадии жизненного цикла сетей электросвязи (проектирование, строительство, реконструкция, развитие и эксплуатация) должна осуществляться деятельность по поддержанию управления рисками, основой которой являются процессы идентификации и оценки рисков.

Оценка риска при обеспечении безопасности сетей электросвязи должна производиться на основе анализа уязвимостей сетей электросвязи и угроз, способных реализовать эти уязвимости.

5.6 Угрозы могут способствовать причинению ущерба пользователям услугами связи, операторам и/или органам государственного управления.

За основу классификации угроз безопасности сетей электросвязи рекомендуется классификацию, установленную ГОСТ Р 51275, в соответствии с которой угрозы могут быть классифицированы:

- по природе возникновения: объективные (естественные) или субъективные (искусственные);
- по источнику возникновения: внешние или внутренние.

Источником угроз безопасности сетей электросвязи могут быть: субъект, материальный объект или физическое явление.

В процессе обеспечения безопасности сети электросвязи необходимо выявление всех возможных угроз инфокоммуникационной структуре сети.

Полное множество угроз безопасности не поддается формализации. Это связано с тем, что архитектура современных сетей электросвязи, используемые технологии обработки, хранения и передачи информации подвержены большому количеству объективных и субъективных дестабилизирующих воздействий. Но чем больше будет выявлено возможных угроз безопасности, тем точнее будет оценено состояние безопасности сети электросвязи.

К основным возможным угрозам безопасности сетей электросвязи могут быть отнесены следующие угрозы:

- уничтожение информации и/или других ресурсов;
- искажение или модификация информации;
- мошенничество;
- кража, утечка, потеря информации и/или других ресурсов;
- несанкционированный доступ;
- отказ в обслуживании.

5.7 В целях учета всех возможных сфер проявления угроз для каждой конкретной сети электросвязи необходимо разрабатывать модель угроз безопасности.

Модель угроз безопасности сети электросвязи представляет собой нормативный документ, которым должен руководствоваться заказчик при задании требований к безопасности сети, и разработчик, создающий эту сеть и службы обеспечения информационной безопасности сети при ее эксплуатации.

Модель угроз должна включать:

- описание ресурсов инфокоммуникационной структуры (объектов безопасности) сети электросвязи, требующих защиты;
- описание источников формирования дестабилизирующих воздействий и их потенциальных возможностей;
- стадии жизненного цикла сети электросвязи, в том числе определяющие ее технологический и эксплуатационный этапы;
- описание процесса возникновения угроз и путей их практической реализации.

В качестве приложения модель угроз безопасности должна содержать полный перечень угроз и базу данных о выявленных нарушениях безопасности сети электросвязи с описанием обстоятельств, связанных с обнаружением нарушений.

В соответствии с разработанной моделью угроз оценивается опасность угроз для каждой группы идентифицированных ресурсов инфокоммуникационной структуры сети электросвязи и услуг связи и определяются возможные меры обеспечения безопасности для противодействия каждой конкретной угрозе.

5.8 Угрозы безопасности сети электросвязи реализуются нарушителями безопасности через выявленные уязвимости инфокоммуникационной структуры сети, в которую они могут быть внесены на технологическом и/или эксплуатационном этапах ее жизненного цикла. Угрозы безопасности могут изменяться. Уязвимость может существовать на протяжении всего срока эксплуатации сети электросвязи или конкретного протокола, если она своевременно не устраняется разработчиком или по его представлению службами эксплуатации оператора связи.

5.9 Нарушителями безопасности сетей электросвязи могут быть:

- террористы и террористические организации;
- конкурирующие организации и структуры;
- спецслужбы иностранных государств и блоков государств;
- криминальные структуры;
- взломщики программных продуктов ИТ, использующихся в системах связи;
- бывшие сотрудники организаций связи;
- недобросовестные сотрудники и партнеры;
- пользователи услугами связи и др.

Основными мотивами нарушений безопасности сетей электросвязи могут быть:

- месть;
- достижение денежной выгоды, в том числе за счет продажи полученной информации;
- хулиганство и любопытство;
- профессиональное самоутверждение.

5.10 Для учета всех возможных ВН и определения его категории разрабатывается модель нарушителя безопасности сети электросвязи, под которой понимается абстрактное (формализованное или неформализованное) описание нарушителя политики безопасности.

Задача построения модели нарушителя безопасности сети электросвязи состоит в определении:

- штатных объектов и элементов сети, к которым возможен доступ;
- субъектов, допущенных к работе с оборудованием сети в период ее проектирования, разработки, развертывания и эксплуатации;
- перечня соответствия объектов доступа субъектам, которые могут быть потенциальными нарушителями.

При определении потенциального нарушителя и составлении его модели необходимо исходить из того, что нарушитель может быть как законным абонентом сети (принадлежать к персоналу, непосредственно работающему с абонентскими терминалами), так и посторонним лицом, пытающимся непосредственно или с помощью имеющихся у него технических и программных средств получить доступ к информационным ресурсам и инфраструктуре сети.

ВН, в основном, направлены на ухудшение качественных характеристик функционирования сетей электросвязи и могут осуществляться, как правило, путем поиска и использования эксплуатационных и технологических уязвимостей. ВН могут осуществляться:

- по каналам абонентского доступа, в том числе и беспроводным;
- по внутренним линиям связи;
- с рабочих мест систем управления и технического обслуживания;
- по недекларированным каналам доступа.

При этом могут использоваться как штатные, так и специальные средства связи.

5.12 Безопасность сети электросвязи характеризуется основными ее критериями:

- конфиденциальностью инфокоммуникационной структуры сети электросвязи;
- целостностью информации и услуг связи;
- доступностью информации и услуг связи;
- подотчетностью действий в сети.

5.12.1 Под конфиденциальностью инфокоммуникационной структуры сети электросвязи понимают свойство, позволяющее ограничить несанкционированный доступ к инфокоммуникационной структуре сети электросвязи и/или не раскрывать содержания информационных ресурсов сети неуполномоченным лицам, объектам или процессам.

Нарушение конфиденциальности — несанкционированное раскрытие информации управления, персональных данных пользователей и др.

5.12.2 Под целостностью информации и услуг связи понимают состояние сети электросвязи, при котором обеспечивается неизменность информации и доступность услуг связи для пользователей, независимо от преднамеренного или случайного несанкционированного ВН на инфокоммуникационную структуру сети, в том числе в чрезвычайных ситуациях.

Нарушение целостности — несанкционированная модификация или разрушение информационных ресурсов и инфраструктуры сети электросвязи.

5.12.3 Под доступностью информации и услуг понимается способность сети электросвязи обеспечить пользователям согласованные условия доступа к предоставляемым услугам связи и их получение, в том числе в условиях возможных ВН на инфокоммуникационную структуру сети электросвязи.

Нарушение доступности — нарушение доступа к использованию информации или услуг связи.

5.12.4 Под подотчетностью понимают свойство, которое обеспечивает однозначное отслеживание действий в сети любого объекта.

Нарушение подотчетности — отрицание действий в сети (например, участие в совершенном сеансе связи) или подделка (например, создание информации и претензии, которые якобы были получены от другого объекта или посланы другому объекту).

В таблице 2 показана взаимосвязь основных угроз и критериев безопасности сети электросвязи.

Таблица 2 — Отображение взаимосвязи основных угроз и критериев безопасности

Вид угрозы	Критерии безопасности			
	Конфиден-циальность	Целостность	Доступность	Подотчет-ность
Уничтожение информации и/или других ресурсов	—	+	+	+
Искажение или модификация информации	—	+	—	+
Мошенничество	+	+	+	+
Кража, утечка, потеря информации и/или других ресурсов	+	+	+	—
Несанкционированный доступ	+	+	+	+
Отказ в обслуживании	—	—	+	—

Примечание — Знак (+) означает возможное воздействие угрозы на критерий безопасности, знак (—) означает отсутствие угрозы критерию безопасности.

7 Основные мероприятия по обеспечению безопасности сетей электросвязи

7.1 Обеспечение безопасности сети электросвязи является обязанностью ее владельца. Ответственность владельца сети электросвязи за обеспечение ее безопасности не прекращается при делегировании им своих полномочий по данным функциям отдельным лицам (поставщикам услуг, администраторам, третьим лицам и т. д.).

Мероприятия по обеспечению безопасности сети электросвязи, проводимые оператором связи, не должны ухудшать качественных характеристик сети и снижать оперативность обработки информации.

Реализация обязательных требований к безопасности, установленных федеральными органами исполнительной власти в области связи, осуществляется силами и средствами владельца сети электросвязи с привлечением при необходимости специализированных организаций, имеющих лицензии на данный вид деятельности.

Дополнительные (повышенные) требования к безопасности (например, шифрование трафика пользователя) могут осуществляться оператором связи на договорной основе с пользователем.

Вопросы непосредственного обеспечения безопасности при присоединении одной сети электросвязи к другой и условия выполнения обязательных требований к безопасности, установленные федеральными органами исполнительной власти в области связи, при взаимодействии этих сетей оговариваются в заключаемых операторами связи договорах о присоединении сетей электросвязи.

При присоединении к сетям электросвязи иностранных государств и взаимодействии с глобальными информационно-телекоммуникационными сетями, в том числе и Интернет, обеспечение безопасности должно основываться на соблюдении международных правовых актов, регламентирующих безопасный пропуск трансграничного трафика. При этом должна быть обеспечена защита инфокоммуникационной структуры сетей электросвязи от НСД со стороны взаимодействующих сетей и гарантированное качество обслуживания в условиях возможных ВН трансграничного характера.

Современные стандарты ИБ инфокоммуникационных сетей

7.2 Обеспечение безопасности сетей электросвязи достигается:

а) защитой сетей электросвязи от НСД к ним и передаваемой посредством их информации;

б) противодействием техническим разведкам;

в) противодействием сетевым атакам и вирусам;

г) защитой средств связи и сооружений связи от НСВ, включая физическую защиту сооружений и линий связи;

д) разграничением доступа пользователей и субъектов инфокоммуникационной структуры сетей электросвязи к информационным ресурсам в соответствии с принятой политикой безопасности оператора связи;

е) использованием механизмов обеспечения безопасности;

ж) физической и инженерно-технической защитой объектов инфокоммуникационной структуры сетей электросвязи;

и) использованием организационных методов, включающих:

1) разработку и реализацию политики безопасности оператором связи;

2) организацию контроля состояния безопасности сети электросвязи;

3) определение порядка действий в чрезвычайных ситуациях и в условиях чрезвычайного положения;

4) определения порядка реагирования на инциденты безопасности;

5) разработку программ повышения информированности персонала сети электросвязи в вопросах понимания им проблем безопасности;

6) определение системы подготовки и повышения квалификации специалистов в области безопасности.

7.3 Пользователи услугами связи имеют право применять специальные механизмы обеспечения безопасности и средства защиты информации, разрешенные к применению на сетях электросвязи и сертифицированные в соответствии с действующим законодательством Российской Федерации.

Взаимоотношения пользователей с операторами связи в сфере обеспечения безопасности сетей электросвязи должны строиться на основе следующих положений:

- только авторизованные пользователи должны иметь доступ к сетям электросвязи и использованию предоставляемых им услуг;
- авторизованные пользователи должны иметь доступ и оперировать только теми ресурсами, к которым они допущены;
- все пользователи должны быть ответственными за их собственные, и только их собственные, действия в сети электросвязи.

7.4 Оператор связи должен принимать меры, обеспечивающие:

- доступ правоохранительных органов, в предусмотренных законодательством Российской Федерации случаях, к информации конкретных пользователей;
- право на доступ пользователей услугами связи к информационным ресурсам в строгом соответствии с установленными правилами разграничения доступа;
- исключение несанкционированного доступа пользователей услугами связи к ресурсам сети и услугам связи;
- предоставление пользователям услугами связи дополнительных услуг по защите информации и процесса безопасной передачи сообщений на договорной основе;
- информирование пользователей о состоянии безопасности доступа к услугам связи.

8 Основные положения о структуре системы обеспечения безопасности сетей электросвязи

8.1 Система обеспечения безопасности (СОБ) сетей электросвязи ССОП является элементом системы информационной безопасности Российской Федерации и может быть отнесена к категории технологических систем связи.

Архитектура СОБ сетей электросвязи имеет многоуровневую иерархическую структуру, охватывающую магистральные транзитные, междугородние и зоновые (местные и внутризоновые) сети электросвязи, и состоит из взаимодействующих между собой служб обеспечения безопасности различных операторов связи, координируемых центральным органом СОБ, который может быть образован федеральным органом исполнительной власти в области связи.

8.2 Архитектура СОБ сети электросвязи может состоять из нескольких уровней безопасности, характеристика которых должна быть отражена в политике безопасности организации связи. В общем случае архитектура СОБ может содержать следующие уровни безопасности:

а) уровень управления безопасностью. На данном уровне осуществляется управление безопасностью сетей электросвязи, координируемое центральным органом СОБ;

б) организационно-административный уровень. Включает службы (отделы, подразделения, администраторов) безопасности, в зависимости от структуры организации связи. На данном уровне осуществляются:

1) взаимодействие с системой управления сетями электросвязи;

2) управление, координация и контроль проводимых организационных и технических мероприятий на всех нижележащих уровнях;

3) учет практического применения нормативной правовой базы (законов, стандартов, положений, должностных инструкций, планов по безопасности);

Современные стандарты ИБ инфокоммуникационных сетей

в) уровень безопасности инфокоммуникационной структуры. Содержит механизмы обеспечения безопасности и другие средства, обеспечивающие защиту процесса обработки и передачи информации в сети. На данном уровне осуществляются:

1) разграничение доступа к информационным ресурсам, сетевым объектам и системе управления сетью электросвязи,

2) защита от НСД, аутентификация и идентификация участников сетевого взаимодействия, включая удаленные объекты и администраторов (сетевых и безопасности),

3) контроль трафика (межсетевые экраны), средства обнаружения атак, средства регистрации и учета событий и ресурсов (аудит и мониторинг безопасности);

г) уровень безопасности услуг. На данном уровне осуществляется контроль качества обслуживания (предоставляемых услуг связи) в условиях возможных ВН и в чрезвычайных ситуациях, в том числе целостности циркулирующих в сети сообщений, содержащих данные пользователя и информацию управления;

д) уровень сетевой безопасности. Данный уровень поддерживает безопасность сетевых протоколов, которые обеспечивают:

1) передачи трафика из конца в конец,

2) транспортирование файлов,

3) поддержку фундаментальных приложений, передачу голоса в сети и электронную почту;

4) конфиденциальность передаваемой по каналам связи информации управления;

е) уровень физической безопасности. На данном уровне обеспечиваются:

1) физическая охрана помещений, в которых обрабатывается и хранится информация,

2) организация контроля доступа сотрудников и посетителей на территорию организации связи, в помещения со средствами связи, осуществляющими обработку информации, к технологическим системам управления, кабельным соединениям,

3) организация охранной сигнализации,

4) контроль вскрытия аппаратуры,

5) электро- и пожаробезопасность организации связи в целом.

8.4 Деятельность органов СОБ сети электросвязи подразумевает выполнение следующих мероприятий:

- подтверждение соответствия средств связи, паспортизацию организаций связи и аттестацию объектов и сетей электросвязи по требованиям безопасности;
- оценку состояния безопасности сети электросвязи, прогнозирование и обнаружение внутренних и внешних угроз безопасности;
- анализ информационных рисков, создание системы управления рисками и страхования информационных рисков;
- выявление уязвимостей в сетях электросвязи и осуществление комплекса адекватных и экономически обоснованных мер по их снижению;
- предотвращение либо обнаружение ВН, пресечение их реализации, локализацию и ликвидацию последствий этих дестабилизирующих воздействий на инфокоммуникационную структуру сети электросвязи;
- оповещение о нарушениях безопасности, реакцию на инциденты безопасности и восстановление нарушенного процесса функционирования сети электросвязи;
- адаптацию СОБ к изменяющимся условиям функционирования сети электросвязи;
- контроль качества обслуживания в условиях ВН;
- мониторинг СОБ и аудит событий безопасности;
- предупреждение, выявление и пресечение в сетях связи неправомочных действий пользователей услугами связи (нарушителей);
- противодействие распространению вредоносных программ (вирусов);
- организацию и проведение работ в области стандартизации безопасности сетей электросвязи с учетом рекомендаций и стандартов международных организаций по стандартизации;
- реализацию мер обеспечения безопасности сетей электросвязи, основой которых является применение соответствующих механизмов обеспечения безопасности.

Модель безопасности сети электросвязи