МЕЖДУНАРОДНЫЙ СОЮЗ ЭЛЕКТРОСВЯЗИ

МСЭ-Т X.1205

СЕКТОР СТАНДАРТИЗАЦИИ
ЭЛЕКТРОСВЯЗИ МСЭ

(04/2008)

СЕРИЯ X: СЕТИ ПЕРЕДАЧИ ДАННЫХ,
ВЗАИМОСВЯЗЬ ОТКРЫТЫХ СИСТЕМ
И БЕЗОПАСНОСТЬ

Безопасность электросвязи

Обзор кибербезопасности

Рекомендация МСЭ-Т X.1205

РЕКОМЕНДАЦИИ МСЭ-Т СЕРИИ X

СЕТИ ПЕРЕДАЧИ ДАННЫХ, ВЗАИМОСВЯЗЬ ОТКРЫТЫХ СИСТЕМ И БЕЗОПАСНОСТЬ

СЕТИ ПЕРЕДАЧИ ДАННЫХ ОБЩЕГО ПОЛЬЗОВАНИЯ	
Службы и услуги	X.1–X.19
Интерфейсы	X.20–X.49
Передача, сигнализация и коммутация	X.50–X.89
Сетевые аспекты	X.90–X.149
Техническое обслуживание	X.150–X.179
Административные предписания	X.180–X.199
ВЗАИМОСВЯЗЬ ОТКРЫТЫХ СИСТЕМ	
Модель и обозначение	X.200–X.209
Определения служб	X.210–X.219
Спецификации протоколов с установлением соединений	X.220–X.229
Спецификации протоколов без установления соединений	X.230–X.239
Проформы PICS	X.240–X.259
Идентификация протоколов	X.260–X.269
Протоколы обеспечения безопасности	X.270–X.279
Управляемые объекты уровня	X.280–X.289
Испытание на соответствие	X.290–X.299
ВЗАИМОДЕЙСТВИЕ МЕЖДУ СЕТЯМИ	
Общие положения	X.300–X.349
Спутниковые системы передачи данных	X.350–X.369
Сети, основанные на протоколе Интернет	X.370–X.379
СИСТЕМЫ ОБРАБОТКИ СООБЩЕНИЙ	X.400–X.499
СПРАВОЧНИК	X.500–X.599
ОРГАНИЗАЦИЯ СЕТИ ВОС И СИСТЕМНЫЕ АСПЕКТЫ	
Организация сети	X.600–X.629
Эффективность	X.630–X.639
Качество обслуживания	X.640–X.649
Наименование, адресация и регистрация	X.650–X.679
Абстрактно-синтаксическая нотация 1 (ASN.1)	X.680–X.699
УПРАВЛЕНИЕ В ВОС	
Структура и архитектура управления системами	X.700–X.709
Служба и протокол связи для общего управления	X.710–X.719
Структура управляющей информации	X.720–X.729
Функции общего управления и функции ODMA	X.730–X.799
БЕЗОПАСНОСТЬ	X.800–X.849
ПРИЛОЖЕНИЯ ВОС	
Фиксация, параллельность и восстановление	X.850–X.859
Обработка транзакций	X.860–X.879
Удаленные операции	X.880–X.889
Общие приложения ASN.1	X.890–X.899
ОТКРЫТАЯ РАСПРЕДЕЛЕННАЯ ОБРАБОТКА	X.900–X.999
БЕЗОПАСНОСТЬ ЭЛЕКТРОСВЯЗИ	**X.1000**–

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

Рекомендация МСЭ-Т X.1205

Обзор кибербезопасности

Резюме

В Рекомендации МСЭ-Т X.1205 дано определение кибербезопасности. Также в данной Рекомендации предоставлена систематика угроз безопасности с точки зрения организации. И в ней представлены угрозы кибербезопасности и уязвимости, включая самые распространенные профессиональные инструментальные средства хакеров. Угрозы обсуждаются на различных уровнях сетевой иерархии.

Обсуждаются различные технологии кибербезопасности, которые можно применить для устранения этих угроз, включая: маршрутизаторы, брандмауэры, антивирусную защиту, системы обнаружения вторжения, системы защиты от вторжения, безопасную компьютерную обработку данных, аудит и мониторинг. Обсуждаются принципы защиты сетей, такие как защита в глубину, управление доступом применительно к кибербезопасности. Обсуждаются технологии и стратегии управления рисками, включая значимость профессионального обучения и образования, связанные с вопросом защиты сетей. Также обсуждаются примеры защиты различных сетей на основе обсуждаемых технологий.

Источник

Рекомендация МСЭ-Т X.1205 была утверждена 18 апреля 2008 года 17-й Исследовательской комиссией МСЭ-Т (2005–2008 гг.) в соответствии с процедурой, изложенной в Резолюции 1 ВАСЭ.

ПРЕДИСЛОВИЕ

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

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

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

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

ПРИМЕЧАНИЕ

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

Соблюдение положений данной Рекомендации носит добровольный характер. Однако в Рекомендации могут содержаться определенные обязательные положения (например, для обеспечения возможности взаимодействия или применимости), и соблюдение положений данной Рекомендации достигается в случае выполнения всех этих обязательных положений. Для выражения необходимости выполнения требований используется синтаксис долженствования и соответствующие слова (такие, как "должен" и т. п.), а также их отрицательные эквиваленты. Использование этих слов не предполагает, что соблюдение положений данной Рекомендации является обязательным для какой-либо из сторон.

ПРАВА ИНТЕЛЛЕКТУАЛЬНОЙ СОБСТВЕННОСТИ

МСЭ обращает внимание на вероятность того, что практическое применение или реализация этой Рекомендации может включать использование заявленного права интеллектуальной собственности. МСЭ не занимает какую бы то ни было позицию относительно подтверждения, обоснованности или применимости заявленных прав интеллектуальной собственности, независимо от того, отстаиваются ли они членами МСЭ или другими сторонами вне процесса подготовки Рекомендации.

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

СОДЕРЖАНИЕ

Рекомендация МСЭ-Т X.1205

Обзор кибербезопасности

1 Сфера применения

В пункте 7 данной Рекомендации раскрывается определение кибербезопасности. В Рекомендации представляется классификация угроз безопасности с точки зрения организации.

ПРИМЕЧАНИЕ. – Использование в настоящей Рекомендации термина "идентичность" не указывает на его абсолютное значение. В частности, он не означает какого-либо подтверждения правильности.

В пункте 7 обсуждается природа среды кибербезопасности предприятия, риски кибербезопасности и сквозная безопасность связи. В пункте 8 обсуждаются возможные методы защиты сетей, включая: управление политикой замкнутого шлейфа, управление унифицированным доступом. В пункте 8 также обсуждаются технологии безопасных передач в сети, безопасность на разную глубину, организация защиты плоскости управления, уровневая безопасность и живучесть сети даже в момент попытки нарушения защиты.

В Дополнении I рассматривается систематика угроз безопасности, средства хакеров, создающие угрозы электронной торговле и безопасности.

В Дополнении II приводится обзор технологий областей кибербезопасности, включая: криптографию, технологии контроля доступа, методы защиты по периметру, антивирусную и системную целостность, методы аудита, мониторинга и управления.

В Дополнении III предоставлены примеры безопасности сетей. В эти примеры включены: организация защиты удаленного доступа, организация безопасности IP-телефонии, организация безопасности клиентов VoIP, организация безопасности удаленного офиса и организация безопасности WLAN.

2 Справочные документы

Нижеследующие Рекомендации МСЭ-Т и другие ссылки содержат пункты, на которые имеются ссылки в тексте этих Рекомендаций. Во время опубликования все перечисленные издания были в силе. Все Рекомендации и другие ссылки могут пересматриваться: все пользователи настоящих Рекомендаций должны использовать возможность применения наиболее современного издания Рекомендаций и других ссылок приведенных ниже. Список действующих в настоящее время Рекомендаций МСЭ-Т регулярно публикуется. Ссылка на документ, приведенный в настоящей Рекомендации, не придает ему как отдельному документу статуса рекомендации.

[ITU-T X.800] ITU-T Recommendation X.800 (1991), *Information processing systems Open Systems Interconnection Basic Reference Model Part 2: Security Architecture.*

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

[ITU-T X.811] Рекомендация МСЭ-Т X.811 (1995 г.), *Структуры безопасности для открытых систем: структура аутентификации*.

[ITU-T X.812] Рекомендация МСЭ-Т X.812 (1995 г.), *Структуры безопасности для открытых систем: структура управления доступом*.

[IETF RFC 1918] IETF RFC 1918 (1996), *Address Allocation for Private Internets* <http://www.ietf.org/rfc/rfc1918.txt?number=1918>.

[IETF RFC 2396] IETF RFC 2396 (1998), *Uniform Resource Identifiers (URI): Generic Syntax* <http://www.ietf.org/rfc/rfc2396.txt?number=2396>.

3 Определения

3.1 Термины, определенные где-либо

В настоящей Рекомендации используются следующие термины, определенные где-либо:

3.1.1 В данной Рекомендации используются следующие термины, определенные в [ITU-T X.800]:

a) санкционирование;

b) архитектура безопасности;

c) политика безопасности;

d) пользователь.

3.1.2 В данной Рекомендации используются следующие термины, определенные в [ITU-T X.805]:

a) аспект безопасности;

b) служба безопасности.

3.1.3 В данной Рекомендации используются следующие термины, определенные в [ITU-T X.811]:

a) аутентификация;

b) принцип.

3.1.4 В данной Рекомендации используются следующие термины, определенные в [ITU-T X.812]:

a) информация контроля доступа;

b) доступ;

c) контроль доступа;

d) пользователь.

3.1.5 В данной Рекомендации используются следующие термины, определенные в [IETF RFC 2396:

a) универсальный идентификатор ресурса (URI);

b) ссылка URI.

3.2 Термины, определенные в настоящей Рекомендации

В настоящей Рекомендации определены следующие термины:

3.2.1 точка доступа: Беспроводной концентратор IEEE 802.11, особый вид станции (STA), функционирующий как точка доступа.

3.2.2 базовый набор услуг (BSS): Зона покрытия, обслуживаемая одной точкой доступа (AP).

3.2.3 криптографический алгоритм: Криптографический алгоритм является средством, с помощью которого данные изменяются и маскируются в зашифрованном виде.

3.2.4 киберсреда: Включает пользователей, сети, устройства, все программное обеспечение, процессы, сохраненную или транзитную информацию, приложения, услуги и системы, которые могут быть прямо или косвенно соединены с сетями.

3.2.5 кибербезопасность: Кибербезопасность – это набор средств, стратегии, принципы обеспечения безопасности, гарантии безопасности, руководящие принципы, подходы к управлению рисками, действия, профессиональная подготовка, практический опыт, страхование и технологии, которые могут быть использованы для защиты киберсреды, ресурсов организации и пользователя. Ресурсы организации и пользователя включают подсоединенные компьютерные устройства, персонал, инфраструктуру, приложения, услуги, системы электросвязи и всю совокупность переданной и/или сохраненной информации в киберсреде. Кибербезопасность состоит в попытке достижения и сохранения свойств безопасности у ресурсов организации или пользователя, направленных против соответствующих угроз безопасности в киберсреде. Общие задачи обеспечения безопасности включают следующее:

- доступность;
- целостность, которая может включать аутентичность и неотказуемость;
- конфиденциальность.

3.2.6 система распределения: Нестандартная среда для присоединения наборов BSS внутри Расширенного набора услуг (ESS).

3.2.7 расширяемый протокол аутентификации: Это расширение протокола сквозного соединения (PPP), предоставляющее обеспечение для дополнительных методов аутентификации, является частью спецификации [b-IEEE 802.1X].

3.2.8 расширенный набор услуг: Отдельная беспроводная локальная сеть (LAN) с наборами BSS внутри отдельной подсети Интернет протокола (IP).

3.2.9 брандмауэр: Система или комбинация систем, которая принудительно устанавливает границу между двумя или более сетями. Шлюз, ограничивающий доступ между сетями в соответствии с местной политикой безопасности.

3.2.10 внешний агент: Маршрутизатор посещаемой/главной сети, который обслуживает подвижный узел во время посещения главной сети. Этот внешний агент обрабатывает туннелирование и доставку между подвижным узлом и другими устройствами, и между подвижной домашней сетью и главной сетью.

3.2.11 приманка: Программа компьютерного обеспечения, которая эмулирует сеть таким образом, чтобы привлечь (а возможно и запутать) злоумышленников и проследить их действия. Выходной сигнал этих систем может использоваться для того, чтобы сделать выводы по поводу намерений злоумышленников и для сбора доказательств.

3.2.12 домашний агент: Маршрутизатор, который обслуживает подвижный узел во время посещения других сетей, поддерживающий текущую местную информацию на этом подвижный узле.

3.2.13 горячие точки: Общественные места, в которых пользователи подвижного хоста IEEE 802.11 подключаются к интернет.

3.2.14 мобильность IP: Механизм, активирующий более прозрачную подключаемость для подвижных узлов, которые "посещают" различные подсети IP во время перемещения. Это механизм для мобильного управления подвижными узлами как в коммутируемых, так и в беспроводных сетях.

4 Сокращения

В настоящей Рекомендации используются следующие сокращения и акронимы:

3DES	Triple Data Encryption Standard	Тройной DES, стандарт шифрования данных
AAA	Authentication, Authorization and Accounting	Аутентификация, санкционирование и учет
ACL	Access Control List	Перечень контроля доступа
AES	Advanced Encryption Standard	Улучшенный стандарт шифрования
AP	Access Point	Точка доступа
ASP	Application Service Provider	Поставщик программно-аппаратных ресурсов
BSS	Basic Service Set	Базовый набор услуг
CA	Certification Authority	Сертификационные органы
CMP	Certificate Management Protocol	Протокол управления сертификатом
COPS	Common Open Policy Service	Общая открытая служба политики
CRL	Certificate Revocation List	Список аннулированных сертификатов
DISA	Direct Inward System Access	Доступ к добавочной линии путем прямого установления входящего соединения
DNS	Domain Name System	Доменная система имен
EAP	Extensible Authentication Protocol	Расширяемый протокол аутентификации
EMS	Element Management System	Система управления элементами
ESS	Extended Service Set	Расширенный набор услуг

ESSID	Extended Service Set Identifier		Идентификатор расширенного набора услуг
FTP	File Transfer Protocol		Протокол передачи файлов
HMAC	Hash function based MACs		Хешированный код аутентификации сообщения
HTTP	Hypertext Transport Protocol		Протокол передачи гипертекста
IDS	Intrusion Detection System		Система обнаружения проникновений
IKE	Internet Key Exchange		Обмен ключами интернет
IP	Internet Protocol		Протокол Интернет
IPSec	Internet Protocol Security		Протокол IPSec
ISP	Internet Service Provider		Поставщик услуг интернета
L2TP	Layer 2 Tunneling Protocol		Сетевой протокол туннелирования канального уровня
LAN	Local Area Network		Локальная сеть
MAC	Message Authentication Code		Код аутентификации сообщения
MD5	Message Digest algorithm 5		Односторонняя хэш-функция MD5
MIC	Message Integrity Check		Проверка целостности сообщения
MIME	Multipurpose Internet Mail Extensions		Многоцелевые расширения почты в интернете
MPLS	Multiprotocol Label Switching		Многопротокольная коммутация на основе признаков
MU	Mobile Unit		Модуль для подвижной связи
NAT	Network Address Translation		Протокол NAT (Трансляция сетевых адресов)
NGN	Next Generation Network	СПП	Сеть последующего поколения
NIC	Network Interface Card		Сетевая интерфейсная плата
NOC	Network Operations Center		Центр управления сетью
OAM&P	Operations, Administration, Maintenance & Provisioning		Эксплуатация, администрирование, сопровождение и предоставление услуг
OCSP	Online Certificate Status Protocol		Онлайновый протокол состояния сертификата
OC	Operating System		Операционная система
OSI	Open Systems Interconnection		Взаимодействие открытых систем
PDP	Policy Decision Point		Сервер политики, пункт выбора политики
PEAP	Protected EAP protocol		Защищенный расширяемый протокол аутентификации (EAP)
PEP	Policy Enforcement Point		Клиент сервера политики, пункт принудительного применения политики
PGP	Pretty Good Privacy		Программа шифрования PGP
PKI	Public Key Infrastructure		Инфраструктура открытого ключа
PKIX	Public Key Infrastructure X.509		Инфраструктура открытых ключей X.509
PoP	Proof of Possession		Доказательство права владения
PPP	Point-to-Point Protocol		Протокол передачи из пункта в пункт
PSTN	Public Switched Telephone Network	КТСОП	Коммутируемая телефонная сеть общего пользования
RADIUS	Remote Authentication Dial-in User Service		Служба удаленной аутентификации пользователей по коммутируемым линиям

RSA	Rivest Shamir Adleman public key algorithm	Алгоритм асимметричного шифрования с открытыми ключами Райвеста-Шамира-Адлемана
SHA1	Secure Hash Algorithm 1	Алгоритм безопасного хеширования версии 1, алгоритм SHA-1
SIP	Session Initiation Protocol	Протокол инициации сеанса
SMTP	Simple Mail Transfer Protocol	Простой протокол пересылки почты
SNMP	Simple Network Management Protocol	Простой протокол управления сетью
SP	Service Provider	Поставщик услуг
SSH	Secure Shell	Безопасная оболочка
SSID	Service set identification	Идентификация набора услуг
SSO	Single Sign On	Единственная подпись
TKIP	Temporal Key Integrity Protocol	Временный протокол целостности ключа
TLS	Transport Layer Security Protocol	Протокол безопасности транспортного уровня
UE	User Equipment	Оборудование пользователя
URI	Uniform Resource Identifier	Унифицированный идентификатор ресурса
UTC	Coordinated Universal Time	Всеобщее скоординированное время
VAR	Value-Added Reseller	Фирма-посредник, вносящая добавленную стоимость
VLAN	Virtual LAN	Виртуальная LAN
VoIP	Voice over IP	Передача голоса по протоколу Интернет
VPLS	Virtual Private LAN Service	Услуга виртуальной LAN
VPN	Virtual Private Network	Виртуальная частная сеть
VPWS	Virtual Private Wire Service	Виртуальное частное телеграфное агентство
WAN	Wide Area Network	Территориально-распределенная сеть
WEP	Wired Equivalent Privacy	Протокол шифрования в беспроводной связи, протокол WEP
WLAN	Wireless LAN	Беспроводная LAN
WPA	Wi-Fi Protected Access	Защищенный доступ Wi-Fi
XML	eXtensible Markup Language	Расширяемый язык разметки, язык XML

5 Соглашения

В настоящей Рекомендации оборудование пользователя (UE) понимается в широком смысле и охватывает все виды устройств, модулей (аппаратных или программных) – подвижных и/или стационарных, персональных компьютеров (ПК), терминалов (с мультимедийными возможностями), телефонов и пр., которые находятся в помещениях пользователя и часто не управляются оператором или поставщиком услуг.

6 Введение

Использование сетей для соединения неоднородных систем информационных технологий (IT) может привести к повышению производительности для организаций и к новым возможностям, которые активируются системами, объединенными в сеть. В настоящее время сравнительно легко можно получать информацию, общаться, наблюдать и управлять системами IT на значительных расстояниях. По существу, современные сети играют ключевую роль во многих инфраструктурах государственной важности: электронной торговли, передаче данных и голоса, коммунальных услуг, финансовой, здравоохранения, транспорта и обороны.

Возможность сетевого соединения и повсеместный доступ является центральным вопросом для современных систем IT. Однако широкий доступ и слабая связь взаимосвязанных систем IT может стать первичным источником широко распространенной уязвимости. Для систем, объединенных в сеть, возрастают угрозы, такие как: взлом типа "отказ в обслуживании", кража финансовых и личных сведений, сбои в работе сети, нарушение речевой связи и дистанционной передачи данных.

Сетевые протоколы, которыми пользуются сегодня, были разработаны в обстановке доверия. Большинство новых инвестиций и разработок посвящены построению новой функциональности, но не безопасности этой функциональности.

Угрозы для кибербезопасности быстро возрастают. Вирусы, черви, Троянские кони, попытки нарушения защиты типа имитации соединения, кража идентичности[1], спам и кибератаки находятся на подъеме. Необходимо понимание кибербезопасности для построения фундамента тех знаний, которые помогут обезопасить сети завтрашнего дня.

Корпорациям и государственным учреждениям рекомендуется рассматривать безопасность, как процесс или способ обдумывания возможностей защиты систем, сетей, приложений и ресурсов. Основной мыслью является наличие неотъемлемых рисков в соединенных системах. Однако безопасность не должна быть препятствием для бизнеса. Задача состоит в безопасном предоставлении необходимых услуг.

В современном деловом окружении концепция периметра исчезает. Границы между внутренними и внешними сетями становятся более размытыми. Приложения выполняются на верхнем уровне сетей, с использованием уровневого подхода. Предполагается, что между этими уровнями обеспечена безопасность. Уровневый подход к проблеме безопасности дает организациям возможность создания множества уровней защиты, направленных против угроз.

7 Кибербезопасность

Организации должны разработать всесторонний план для удовлетворения своих нужд по безопасности. Организации должны рассматривать безопасность, как процесс или способ обдумывания возможностей защиты систем, сетей, приложений и ресурсов.

7.1 Что такое кибербезопасность?

В данной Рекомендации термин кибербезопасность определяется в пункте 3.2.5:

Технологии кибербезопасности могут использоваться для гарантирования готовности систем, целостности, аутентичности, конфиденциальности и строгого выполнения обязательств. Технологии кибербезопасности могут использоваться для гарантий соблюдения личной тайны пользователя. Технологии кибербезопасности могут использоваться для установления достоверности пользователя.

Технологии, такие как беспроводные сети и передача голоса по протоколу Интернет (VoIP), расширяют область влияния и масштаб интернет. В связи с этим, киберсреда включают пользователей, интернет, компьютерные устройства, которые подключены к нему, все приложения, услуги и системы, которые могут напрямую или опосредованно подключаться к интернету, и среду сетей последующих поколений (СПП), доступных для общего и частного применения. Таким образом, при использовании технологии VoIP, настольный телефон является частью киберсреды. Однако даже изолированные устройства также могут являться частью киберсреды, если они могут пользоваться информацией совместно с компьютерными устройствами, подключаемыми с помощью сменных носителей.

В киберпространство входит программное обеспечение, которое работает в компьютерных устройствах, информация, которая сохраняется (и передается) в этих устройствах, или информация, которая создается этими устройствами. Оборудование и здания, в которых расположены эти устройства, также являются частью киберпространства. Такие элементы должны приниматься в расчет кибербезопасностью.

---

[1] Термин "кража идентичности" указывает только на несанкционированное использование набора идентификаторов и другой информации, которые в совокупности характеризуют идентичность конкретного пользователя. В отличие от обычного понимания кражи, когда намеченный предмет отнимается у жертвы, кража идентичности обычно предполагает получение или копирование подробных данных идентичности, так чтобы законный владелец даже не смог бы узнать о краже.

Кибербезопасность ставит своей целью организация безопасности киберсреды, системы, в которую могут входить акционеры, относящиеся ко многим общественным и частным организациям, использующим разнообразные компоненты и разные подходы к вопросу безопасности. По существу, полезно подумать о кибербезопасности в таком смысле:

– Совокупность политик и действий, которые должны быть предприняты для защиты соединенных сетей (включая компьютеры, устройства, аппаратные средства, хранящуюся информацию и передаваемую информацию) от несанкционированного доступа, изменения, кражи, разрушения и других угроз.

– Текущая оценка и мониторинг вышеуказанных политик и действий для гарантии непрерывного качества безопасности перед лицом изменяющейся природы угроз.

В [b-ITU-T Y.2201] приводятся требования к сетям СПП, которые могут использоваться для повышения их кибербезопасности. В этой работе предусматривается выполнение аутентификации с возможностью ее осуществления отдельно в отношении устройств и пользователей. Реализация в СПП многофакторной двухсторонней аутентификации с обеспечением санкционирования на каждом уровне обслуживания снижает риски нацеленных на пользователя попыток нарушения защиты.

7.2 Природа среды кибербезопасности предприятия

Организации должны разработать всесторонний план для удовлетворения нужд безопасности. Безопасность одного формата не может подходить для всех (см. [ITU-T X.805]). Безопасности нельзя добиться с помощью совокупности модулей, объединенных вместе. Организациям рекомендуется рассматривать безопасность, как процесс или способ обдумывания возможностей защиты систем, сетей, приложений и услуг, предоставляемых в сети.

Безопасность должна быть всесторонней во всех уровнях сетей. Принятие уровневого подхода к проблеме безопасности, который в союзе с сильным управлением политикой и обеспечением ее выполнения, предоставит профессионалам по безопасности выбор решения по этому вопросу, который будет модульным, гибким и расширяемым.

Безопасность трудно проверить, предсказать и реализовать. Безопасность не может подходить "на все случаи жизни". Требования к безопасности и рекомендуемая стратегия безопасности в каждой организации уникальна и различна. Например, какое-либо предприятие – оператор связи, оператор сети, поставщики услуг – обладает своим уникальным набором бизнес-требований и может создать свою сетевую среду, отвечающую этим требованиям.

Например, "закрытое предприятие" использует логические (например, ретрансляция кадров) или физические частные линии между узлами, удаленный доступ предоставляется избирательно для тех служащих, которым требуется доступ к интернет. Наличие всемирной сети достигается через информационный центр интернет с помощью поставщика услуг (который отвечает за установление безопасной среды). Организация также предоставляет обычный коммутируемый доступ для служащих, находящихся на удаленном расстоянии (например, работающих из гостиницы). Компания использует частную электронную почту (e-mail) среди тех служащих, у которых нет внешнего доступа. Также используются местные беспроводные сети LAN.

"Расширенное предприятие" или оператор связи, оператор сети или поставщик услуг благодаря различным бизнес-моделям могут обеспечивать доступ удаленным служащим и удаленным отделениям через сети IP VPN по интернету или предоставлять возможность осуществления недорогих высокоскоростных соединений, включая доступ в интернет общего назначения для всех сотрудников, например для взаимодействия внутренних систем электронной почты с остальным миром.

В случае бизнес-модели "открытого предприятия" партнеру, поставщику и потребителю может быть разрешено использовать интернет для получения доступа к информационному интернет-центру, управляемому предприятием, и даже получения избирательного доступа к внутренним базам данных и приложениям (например, как части системы управления цепочкой поставок). Внешние и внутренние пользователи получают доступ к сети предприятия из дома, из удаленных отделений или из других сетей, используя коммутируемые или подвижные устройства. По этой причине требование к безопасности для такого предприятия отличается от предъявляемых в отношении других предприятий.

Сводные данные о типах предприятий даны на рисунке 7-1.

Рисунок 7-1 – Общие типы предприятия

Для кибербезопасности требуется управление рисками. Этот процесс включает в себя задачу идентификации совокупного набора компонентов, которые нужно защитить. Для облегчения анализа рисков полезно рассматривать попытки нарушения защиты, как проблемы, принадлежащие к следующим категориям:

1) Нарушение защиты в виде прерывания обслуживания. Этот тип взлома отключает доступ пользователя к намеченным услугам временно или постоянно. Примерами являются: потеря доступа к сайту во всемирной сети, неспособность провести финансовую операцию или инициировать речевой вызов. Несколько типов взломов могут привести к нарушению обслуживания. Например, "отказ в обслуживании" (DoS), "распределённый отказ в обслуживании" (DDoS) или разрушение зданий, в которых размещается важная инфраструктура, может привести к препятствию для доступа пользователей к услуге.

2) Несанкционированный доступ к активам. Эти типы взломов включают в себя кражу или неправильное использование инфраструктуры. Взломы этого типа могут существенно повлиять на кибербезопасность, если они проводятся в большом масштабе.

3) Захват компонентов. Эти типы взломов включают в себя захват контроля над некоторыми устройствами, а затем использование их для запуска новых взломов, направленных против других компонентов киберсреды.

Любой элемент киберсреды может рассматриваться, как риск для безопасности, который в общем случае воспринимается, как комбинированная оценка угрозы. В анализ угрозы входит задача описания типа возможных взломов, потенциальные нападающие и их методы осуществления попытки нарушения защиты, и последствия, в случае успешных взломов. С другой стороны, уязвимость в данной Рекомендации относится к тем слабостям, которыми может воспользоваться нападающий. Оценка рисков вместе с анализом угрозы позволяют организации просчитать потенциальный риск для своей сети.

Попытки нарушения защиты могут исходить из киберсреды, такие как взломы посредством червей или других вредоносных программ, могут быть прямые попытки нарушения защиты важной инфраструктуры, такой как кабели электросвязи, или взломы, вызванные действиями доверенного хорошо осведомленного человека. Сочетание этих попыток нарушения защиты также возможно. Риски обычно характеризуются, как высокие, средние и низкие. Уровень риска изменяется среди разных компонентов киберсреды.

Кибербезопасность заключается в управлении рисками. Для управления рисками могут использоваться разные технологии. Например, разработка стратегии защиты, определяющая меры противодействия, которые могут быть предприняты при возможных попытках нарушения защиты. Обнаружение, в которое входит идентификация взлома в момент его развития и впоследствии. Формулировка отклика на попытку нарушения защиты, в которой определяется совокупность мер противодействия этой попытке для того, чтобы ее остановить или снизить ее влияние. Формулировка стратегии восстановления, которая дает возможность сети возобновить работу с известного состояния.

7.3 Угрозы кибербезопасности и методика их рассмотрения

Согласно Рекомендации МСЭ-Т X.800, в перечень угроз для системы передачи данных включены следующие:

a) уничтожение информации и/или других ресурсов;

b) искажение или изменение информации;

c) кража, перемещение или потеря информации и/или других ресурсов;

d) раскрытие информации; и

e) прерывание обслуживания.

В соответствии с [ITU-T X.800] угрозы могут классифицироваться, как случайные или преднамеренные, и они могут быть активными и пассивными. Случайными угрозами являются такие угрозы, которые возникают без предварительного умысла. Примерами реализованных случайных угроз являются: неправильное срабатывание системы, грубые просчеты в работе и ошибки в программном обеспечении. Преднамеренные угрозы могут классифицироваться от непредусмотренной экспертизы, использующей легкодоступные инструменты мониторинга, до сложных попыток нарушения защиты, использующих специальные системные знания. Преднамеренная угроза, если она реализована, может быть воспринята, как "попытка нарушения защиты". Пассивными угрозами являются такие, которые, если они реализованы, не приводят к какому-либо изменению информации, заключенной в системе(ах), и при которых не изменяется ни работа, ни состояние системы. Использование пассивного подслушивающего оборудования для наблюдения за информацией, передаваемой по подключенной линии, является реализацией пассивной угрозы. Активные угрозы для системы включают в себя изменение информации, содержащейся в системе, или изменения в состоянии или работе этой системы. Злонамеренное изменение таблиц маршрутизации системы несанкционированным пользователем, является примером активной угрозы. В Дополнении I предоставлено краткое резюме некоторых конкретных типов взломов.

Угрозы безопасности, перечисленные в Рекомендации МСЭ-Т X.800 применяются также и к киберсреде. Функции безопасности, указанные в [ITU-T X.800], обычно увеличивают стоимость системы и она может стать более сложной в использовании. Таким образом, до начала разработки системы безопасности, нужно идентифицировать конкретные угрозы, против которых понадобится защита. Этот анализ известен, как оценка угроз. Система уязвима во многих отношениях, но только некоторые слабости можно использовать, из-за того, что у нападающего не много возможностей, или из-за того, что результат не оправдывает приложенных усилий и риск обнаружения. Хотя подробности оценки угроз выходят за пределы данной Рекомендации, в общем плане в них включены:

Угрозы ресурсам, поэтому первым шагом является перечисление требующих защиты ресурсов. На следующем шаге оценки проводится анализ угроз, а затем анализ уязвимости (включая оценку воздействия), меры противодействия и механизмы обеспечения безопасности:

a) идентификация уязвимых мест системы;

b) анализ вероятности угроз, нацеленных на использование этих уязвимых мест;

c) оценка последствий, если каждая угроза будет успешно выполнена;

d) оценка стоимости каждой попытки нарушения защиты;

e) расчет стоимости потенциальных мер противодействия; и

f) выбор механизмов безопасности, которые оправданы (возможно с помощью использования анализа стоимостной выгоды).

В некоторых случаях не технические меры, такие как страховое покрытие, могут быть экономически эффективной альтернативой техническим мерам безопасности. Вообще, идеальная техническая безопасность невозможна. Таким образом, нужно поставить целью удорожание попытки нарушения защиты до достаточно высокого значения, чтобы снизить риск до приемлемых уровней.

7.4 Сквозная безопасность связи

В [ITU-T X.805] определена структура безопасности сети для рассмотрения сквозной безопасности связи. [ITU-T X.805] применима к различным типам сетей, в которых есть проблема сквозной безопасности связи. Эта архитектура не зависит от базовой технологии сети.

Архитектура безопасности предназначена для решения глобальной сложной задачи безопасности поставщиков услуг, предприятий и потребителей; она применима для беспроводной, оптической и проводной линии сетей конвергенции, сетей передачи речи и данных. Архитектура предназначена для безопасности, затрагивающей вопросы управления, контроля и использования сетевой инфраструктуры, услуг и приложений. [ITU-T X.805] обеспечивает возможность активно действующего обнаружения уязвимых мест в безопасности и смягчения связанных с ними последствий в отношении известных угроз. Архитектура безопасности логически разделяет сложный набор функций, связанных со сквозной безопасностью связи, на отдельные архитектурные компоненты. Это разделение дает возможность систематического подхода к сквозной безопасности связи, который может использоваться для планирования новых решения по безопасности, а также для оценки безопасности существующих сетей.

В [ITU-T X.805] фактором безопасности является совокупность мер безопасности, разработанных для определенного аспекта безопасности сетей. В [ITU-T X.805] определяется восемь факторов, которые защищают от всех основных угроз безопасности. Эти факторы не ограничиваются сетями, а также распространяются на приложения и информацию конечного пользователя. Эти факторы безопасности применимы для поставщиков услуг или предприятий, предлагающих услуги безопасности своим потребителям. Факторами безопасности являются:

1) контроль доступа;
2) аутентификация;
3) неотказуемость;
4) конфиденциальность данных;
5) безопасность связи;
6) целостность данных;
7) готовность; и
8) секретность.

Для того чтобы обеспечить решение вопроса сквозной безопасности связи факторы безопасности должны применяться к иерархии сетевого оборудования и группировкам средств, которые рассматриваются, как уровни безопасности. Обращаются к трем следующим уровням:

1) уровень безопасности инфраструктуры;
2) уровень безопасности услуг; и
3) уровень безопасности приложений.

Уровни безопасности устанавливают, где в продуктах и решениях принимается во внимание обеспечение безопасности путем предоставления последовательной структуры безопасности сетей. Например, сначала обращаются к уязвимым местам с точки зрения безопасности для уровня инфраструктуры, затем для уровня услуг и для уровня приложений. На рисунке 7.4-1 изображено, каким образом факторы безопасности применяются к уровням безопасности для того, чтобы уменьшить количество уязвимых мест, присутствующих в каждом уровне.

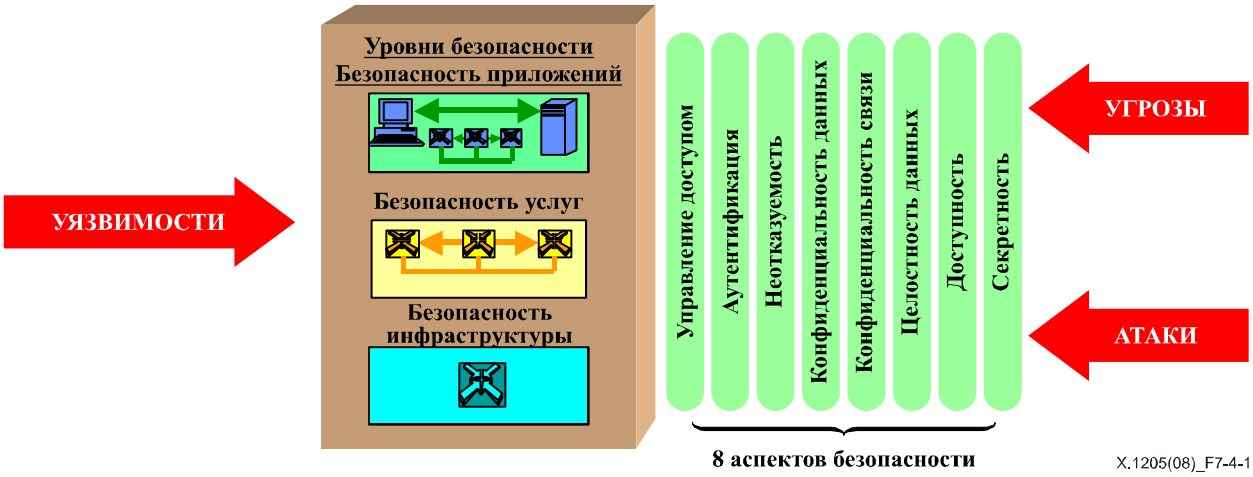

Рисунок 7-4.1 – Применение факторов безопасности к уровням безопасности

В [ITU-T X.805] плоскость безопасности это определенный тип действия сети, защищенный с помощью факторов безопасности. В [ITU-T X.805] определено три плоскости безопасности для представления трех типов защищенных действий, которые происходят в сети. Плоскостями безопасности являются:

1) плоскость управления;

2) плоскость контроля; и

3) плоскость конечного пользователя.

Эти плоскости безопасности предназначены для конкретных нужд безопасности, связанных с деятельностью управления сетью, контроля сети или деятельностью по передаче сигналов и деятельностью конечного пользователя, соответственно. В [ITU-T X.805] предлагается разрабатывать сети таким образом, чтобы события на одной плоскости безопасности хранились изолированно от других плоскостей безопасности. Например, поток поисков DNS на плоскости конечного пользователя, инициированный по запросу конечного пользователя, не должен блокировать интерфейс OAM&P в плоскости управления, что позволит администратору исправить трудную ситуацию.

На рисунке 7.4-2 показана архитектура безопасности с входящими в нее плоскостями безопасности. Концепция плоскостей безопасности позволяет установить различия в конкретных вопросах безопасности, связанных с этими видами деятельности, и дает возможность обращаться к ним независимым образом. Например, в услуге VoIP, к которой обращается уровень безопасности услуг, задача безопасности управления услугой должна быть независима от задачи безопасности контроля этой услуги. Эта задача является независимой от задачи безопасности данных конечного пользователя, которые передаются с помощью этой услуги (например, голос пользователя).

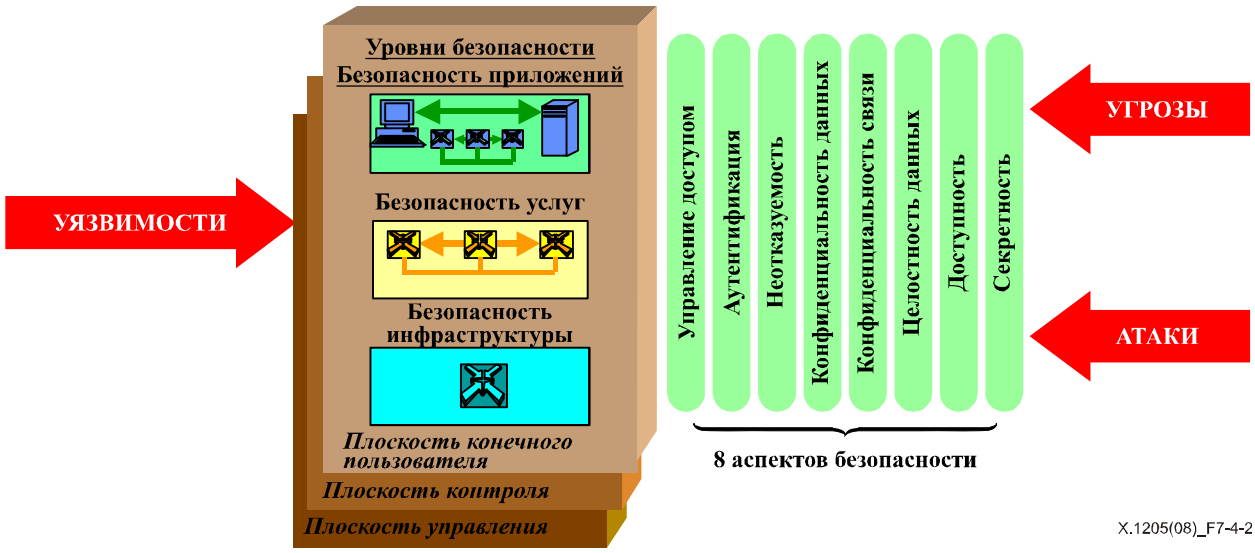

Рисунок 7-4.2 – Плоскости безопасности отражают разные типы деятельности сети

8 Возможные методы защиты сетей

Безопасность охватывает все архитектурные уровни сети. Такой подход предоставляет хорошую отправную точку для разработки безопасных сетей. Это представление позволяет определять требования к безопасности, относящиеся к уровню более высокого порядка, на этом конкретном уровне, а также дает возможность использовать услуги обеспечения безопасности более низких уровней. Уровневый подход к обеспечению безопасности позволяет разработать гибкие, масштабируемые решения в области безопасности по всему сетевому уровню, уровню приложений и уровню управления для всех организаций.

8.1 Управления политикой по принципу замкнутого цикла

Надлежащим образом разработанная и осуществленная политика в области безопасности является безусловным требованием для всех типов предприятий и организаций. Политика в области безопасности – это живой документ и процесс, она проводится, реализуется в целях отражения всех последних изменений в инфраструктуре предприятия или организации и требованиях к обслуживанию.

Политика в области безопасности четко определяет ресурсы организации (также и предприятия), которые подвергаются риску, и методики снижения суммарной угрозы. Политика в области безопасности предусматривает оценку уязвимости и риска, и определяет соответствующие правила управления доступом. Оценка уязвимости и риска выполняется на всех уровнях сети. Эта политика может содействовать определению и обнаружению нарушений безопасности и должна устанавливать конкретные ответы на эти нарушения.

Рекомендуется, чтобы сетевые и IT-администраторы пользовались инструментарием оценки уязвимости в своих сетях. Должен использоваться принцип наименее привилегированного доступа. Задачи сетевых и IT-администраторов включают обеспечение просмотра следов аудитов, замыкая, таким образом, цикл управления политикой. Если проблемы обнаруживаются в аудите, то сетевые и IT-администраторы обеспечивают обновление политики с целью отражения пересмотренных действий.

Политика в области безопасности, которая не проводится, является бесполезной. Проведение политики в области безопасности зависит от людей. Для проведения политики должна иметь место четкая ответственность и подотчетность.

8.2 Унифицированное управление доступом

Термин "управление доступом" используется для определения систем, в которых могут использоваться услуги аутентификации и санкционирования в целях управления использованием ресурса. Аутентификация – это процесс, при котором пользователь или объект требует установления в сети идентификатора. Санкционирование устанавливает уровень привилегий этой идентичности на основе управления доступом. Управление уровнем доступа основано на определении политики управления и ее проведении. На рисунке 8-2 изображена эталонная модель безопасной аутентификации и санкционирования.

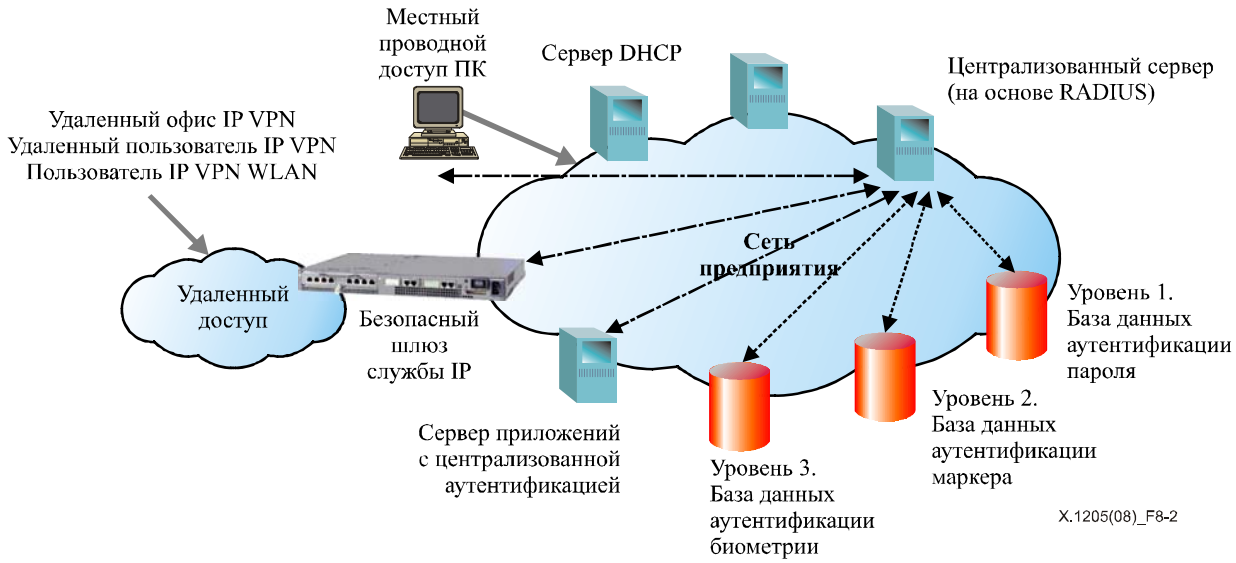

Рисунок 8-2 – Безопасная эталонная модель аутентификации и санкционирования

Исходя из рисунка 8-2 рекомендуется следующее:

1) Использовать механизм централизованной аутентификации в целях упрощения управления и устранения необходимости местного хранения паролей. (Пароли местного хранения проявляют себя как статичные и слабые).

2) Использовать централизованную систему санкционирования с соответствующей степенью структурированности для конкретного предприятия, тесно связанную с системой аутентификации.

3) Обеспечивать выполнения правил сильных (смешанных) паролей для всех паролей.

4) Обеспечивать безопасное хранение всех паролей в формате одностороннего шифрования (хеширования).

5) Использовать принцип простоты, который предусматривает простоту применения и простоту управления. Простая система – это безопасная система, так как весьма вероятно выполнение мер безопасности.

6) Осуществлять безопасную регистрацию всех событий, связанных с безопасностью и относящихся к аутентификации и санкционированию.

Подходы к управлению доступом включают методы фильтрации IP-источников, посредников и методы на основе полномочий. В каждом подходе есть свои преимущества и ограничения. В зависимости от типа предприятия и в рамках заданного типа может использоваться несколько подходов или их сочетание. Например, предприятие может выбрать управление доступом для рабочих станций с использованием метода IP-фильтрации источника, а в отношении всех остальных пользователей применять схему, основанную на полномочиях.

Для аутентификации пользователя могут использоваться несколько методов. К ним относятся пароли, одноразовый пропуск, биометрические методы, смарт-карты и сертификаты. Аутентификация на основе паролей должна использовать сильные пароли, состоящие, например, не менее, чем из восьми символов в длину, и включающие не менее одного буквенного, одного цифрового и одного специального символов. Одной только аутентификации на основе пароля может быть недостаточно. Основываясь на оценке уязвимости, возможно потребуется сочетать

аутентификацию на основе пароля с другими процессами аутентификации и санкционирования, таким как сертификаты, облегченный протокол доступа к сетевому каталогу (LDAP), услуга удаленной аутентификации пользователей по коммутируемым линиям (RADIUS), Kerberos, и инфраструктура открытых ключей (PKI).

У всех механизмов аутентификации есть свои преимущества и недостатки. Сочетания идентификатор/пароль пользователя просты, дешевы, легки в управлении, однако запоминание множества сложных паролей очень трудно для пользователей. Двухфакторная и трехфакторная системы аутентификации придают дополнительную силу аутентификации, однако все они дороги, связаны с дополнительными сложностями и их трудно обслуживать.

Система "единого пароля" с обеспечением применения сильных паролей может быть хорошим решением в отношении аутентификации и санкционирования на предприятии. Такая система гарантирует высокую безопасность аутентификации, структурированное санкционирование, ею проще управлять. С помощью этой системы сильный единый пароль пользователя синхронизируется с большим количеством приложений и систем в рамках предприятия в целях аутентификации и санкционирования. Все системы предприятия и приложения автоматически относят функции аутентификации и санкционирования к системе единого пароля. Так как пользователям нужно помнить только один сильный пароль, то это делает систему простой в использовании, а вероятность того, что эту систему можно обойти, мала. Преимущества системы единого пароля следующие:

- единый последовательный метод для установления паролей;
- единый последовательный метод для аутентификации и санкционирования;
- единый метод для регистрации и закрытия счетов пользователей;
- обеспечение выполнения корпоративных руководящих принципов в отношении силы пароля;
- постоянство – пользователи знают, как поступать;
- стандартизация – легко поддерживать и принимать;
- быстрота – стандартный интерфейс и программные интерфейсы приложений (API);
- чем ниже стоимость, тем меньше звонков с просьбой о помощи.

Открытое и расширенное предприятие сталкивается с самыми большими трудностями, когда разрабатывает свою политику управления доступом. Управление доступом должно быть составным компонентом политики в области безопасности. Такие организации должны разрабатывать унифицированную систему управления доступом с детально разработанными правилами, которые надлежащим образом взаимодействуют с:

- каталогами и базами данных, содержащими атрибуты идентичностей;
- множеством систем аутентификации, таких как система паролей, Kerberos, TACACS и RADIUS;
- главными компьютерами, приложениями и серверами приложений.

Унифицированная система управления доступом осуществляет управление сеансом для каждого пользователя после того, как пользователь аутентифицирован. Рекомендуется использование гибкой конфигурации и проведение политики совместно с детально разработанными правилами, которые могут применяться в отношении конкретных объектов. Надлежащий мониторинг, учет и безопасные следы аудитов. Рекомендуется использование уникальных счетов для каждого администратора с подотчетностью в отношении действий, прослеживаемых до отдельных лиц.

8.3 Безопасная связь

Объединенные сети могут переносить речевые сигналы, данные и видеопакеты. Безопасный сетевой поток должен гарантировать конфиденциальность, целостность и точность передачи по сети. Безопасность должна обеспечиваться в телефонных сетях в отношении трафика вызовов и сигнализации. Должна использоваться технология шифрования для сетей передачи данных, речи и сетей подвижной связи.

Можно выполнить шифрование с помощью:

- методов VPN, используя протокол IPSec с заголовком аутентификации (AH) и безопасное закрытие содержания (ESP) или тунеллирование с помощью протокола тунеллирования уровня 2 (L2TP);
- управления ключом на основе интернет-протокола обмена ключами (IKE);
- управления сертификатом на основе инфраструктуре открытых ключей [b-ITU-T X.509] (PKIX);

- протокола управления сертификатом (CMP) (см. [b-IETF RFC 2510]) и онлайнового протокола состояния сертификата (OCSP) (см. [b-IETF RFC 4557]);
- путем использования на прикладном уровне TLS (безопасность транспортного уровня) (см. [b-IETF RFC 4366]) с сильными ключами.

Важно использовать алгоритмы шифрования и хэши, основанные на таких стандартах, как DES, 3DES, AES, RSA и DSA (см. [b-IETF RFC 2828]). Хэш-функция MD5 (см. [b-IETF RFC 1321]) и алгоритм SHA1 (см. [b-IETF RFC 3174) должны использоваться для обеспечения целостности сообщения, а алгоритмы Диффи-Хеллмана (см. [b-IETF RFC 2631]) и RSA (см. [b-IETF RFC 2828]) – для обмена ключами.

Безопасность, аналогичная защите проводных сетей (WEP), как определено в стандартах [b-IEEE 802.11], определяет метод защиты беспроводной передачи между точками доступа беспроводной LAN (WLAN) и платой сетевого интерфейса (NIC). Было показано, что этот протокол не является безопасным. Должны использоваться дополнительные меры защиты, такие как IPSec для обеспечения безопасности WLAN по WEP. С другой стороны, для дополнительной защиты может использоваться защищенный доступ (WPA) с использованием Wi-Fi.

8.4 Различная степень обеспечения безопасности

Виртуальная сеть VLAN – это группа сетевых устройств, например серверов и других сетевых ресурсов, которые сконфигурированы таким образом, чтобы они работали, как если бы были соединены с одним сетевым сегментом. В сети VLAN ресурсы и серверы других пользователей сети будут невидимы всем другим членам VLAN. Сети VLAN помогают удовлетворить требования к качеству работы путем более эффективной сегментации сети. В сетях VLAN ограничено распространение широковещательного, а также межузлового трафика, таким образом, в сети ограничивается нагрузка со стороны внешнего трафика. В сетях VLAN все пакеты, следующие между сетями VLAN, могут также проходить через маршрутизатор, поскольку данные меры по обеспечению безопасности, основанные на применении маршрутизатора, могут быть предприняты для ограничения доступа к сегменту.

Деление на уровни безопасности приводит к возможности обеспечения различной степени безопасности. Каждый дополнительный уровень безопасности строится на возможностях уровня, лежащего ниже. Каждый дополнительный уровень безопасности обеспечивает все большую степень детализации структуры безопасности.

Например, обособление и сегментация базовой сети предоставляется с помощью виртуальных сетей VLAN. Это дает возможность включать различные бизнес-функции в состав их собственных частных локальных вычислительных сетей и сегментировать их в этих сетях вместе с перекрестным трафиком от других сегментов VLAN, которые строго контролируются или запрещены. Есть несколько преимуществ, которые можно получить при развертывании сетей VLAN по различных местам расположения офисов организации. Так, использование "меток" VLAN дает возможность разделять трафик на конкретные группы, такие как финансы, людские ресурсы и проектирование. Деление потока без "утечек" между сетями VLAN является необходимым элементом для обеспечения безопасности.

Второй уровень безопасности может быть достигнут посредством использования периметра и распределенных возможностей фильтрации с помощью брандмауэра в стратегических точках внутри сети. Уровень брандмауэра позволяет осуществлять дальнейшую сегментацию сети на еще более мелкие области, и обеспечивает возможность выполнения безопасных подключений к сети общего пользования. Брандмауэры ограничивают доступ к входящему и исходящему трафику для тех протоколов, которые конфигурируются непосредственно внутри брандмауэра. Дополнительно может предоставляться возможность аутентификации для входящих и исходящих пользователей. Те брандмауэры, которые поддерживают трансляцию сетевых адресов (NAT), позволяют оптимизировать IP-адресацию в сети, как указано в [IETF RFC 1918] (распределение адресов для частных сетей интернета).

Использование брандмауэров обеспечивает дополнительный уровень защиты, который полезен для целей управления доступом. Применение основанного на политике доступа позволяет индивидуализировать доступ исходя из потребностей деловой деятельности. Использование подхода распределенного брандмауэра приносит дополнительную пользу, состоящую в возможности масштабирования по мере развития потребностей предприятия. В оконечных системах могут быть развернуты персональные брандмауэры для гарантирования целостности приложений.

Уровень 3 сетей VPN может быть добавлен, как третий уровень для обеспечения повышенной безопасности. Сети VPN предоставляют еще большую степень детализации управления доступом пользователя и персонализацию. Сети VPN обладают высоко детализированной структурой

обеспечения безопасности по отношению к уровню индивидуального пользователя и предоставляют возможность для осуществления безопасного удаленного доступа отдаленных отделений и деловых партнеров. В случае VPN использование выделенных линий связи не требуется. Применение динамической маршрутизации по безопасным туннелям в интернете является надежным и масштабируемым решением, обеспечивающим высокую степень безопасности. Использование сетей VPN вместе с сетями VLAN и брандмауэрами позволяет сетевому администратору ограничить доступ одним пользователем или группой пользователей, опираясь на критерии политики и деловые потребности. Сети VPN дают лучшие гарантии целостности данных и конфиденциальности. В целях обеспечения конфиденциальности и целостности данных на этом уровне может быть задействовано криптостойкое шифрование данных.

Решения по обеспечению безопасности, основанные на уровневом подходе, являются гибкими и масштабируемыми. Такое решение можно приспособить к потребностям в обеспечении безопасности предприятия.

8.5 Обеспечение безопасности управления

Независимо от того, считается ли канал или плоскость управления безопасностью "передовым опытом" или составной частью архитектуры безопасности организации или предприятия, он должен быть основой для всех других элементов управления сетью, функционирования и живучести. На рисунке 8-5 изображена предлагаемая эталонная модель обеспечения безопасности управления сети для операционного центра сети (NOC).

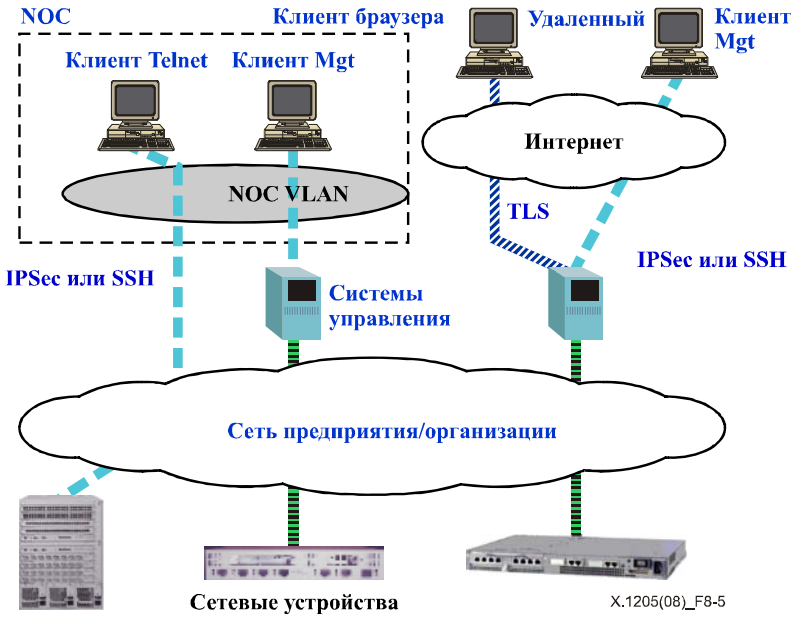

Рисунок 8-5 – Эталонная модель обеспечения безопасности управления

Безопасное управление является целостным подходом, а не набором функциональных возможностей обеспечения безопасности на данном сетевом элементе. По этой причине рекомендуемый в данной Рекомендации подход охватывает важные области сетевой инфраструктуры и предоставляет конкретные действия для снижения потенциальных угроз по отношению к сети. Каждая из предметных областей, указанных ниже, представляет собой важный компонент, который требует внимания с точки зрения безопасности для гарантирования единой структуру защиты вокруг этой сети.

Существует девять ключевых областей управления сетью, на которые нужно обратить внимание в плане безопасности до того, как плоскость управления сетью будет считаться безопасной. Этими областями являются:

- безопасные журналы регистрации деятельности;
- аутентификация оператора сети;
- управление доступом для операторов сети;
- шифрование трафика управления сетью;

- безопасный удаленный доступ для операторов;
- брандмауэры;
- обнаружение вторжения;
- усиление ОС;
- программное обеспечение, не содержащее вирусов.

8.5.1 Управление политикой

Могут использоваться безопасные журналы регистрации для сохранения следа аудита пользователя или действий администратора и событий, созданных самим устройством, что является важным элементом замкнутого цикла управления политикой. Собранные необработанные данные называются "журналом аудита", а проверяемая цепь событий посредством журналов аудита, называется "следом аудита". В целях обеспечения эффективности журналов аудита по безопасности они должны содержать достаточное количество информации для последующего расследования или анализа инцидентов, касающихся безопасности. Эти журналы аудита предоставляют средства для достижения нескольких целей, связанных с безопасностью, включая индивидуальную подотчетность, воссоздание прошлых событий, обнаружение вторжения и анализ проблем. Журналы могут также использоваться для анализа долгосрочных тенденций. Информация из журнала аудита помогает определить основную причину проблемы, связанной с безопасностью, и предотвратить будущие инциденты; эта информация должна быть надежно сохранена. Например, журналы аудита могут использоваться для воссоздания последовательности событий, которые привели к таким проблемам, как получение нарушителем несанкционированного доступа к ресурсам системы или неисправная работа системы, вызванная неверной конфигурацией или ошибочной реализацией.

8.5.2 Безопасное управление доступом

Аутентификация сетевого оператора должна основываться на строгой централизованной аутентификации операторов и администраторов сетей. Централизованное управление паролями дает возможность обеспечения силы паролей и устранения необходимости местного сохранения паролей на сетевых элементах и системах EMS. RADIUS является основным механизмом выбора для автоматической централизованной аутентификации.

Должен применяться передовой опыт в управлении доступом для сетевых операторов. Например, для определения уровня санкционирования можно использовать метод, основанный на серверах RADIUS, чтобы предоставить базовый уровень управления доступом, а если понадобится, то можно добавить сервер LDAP для предоставления более детализированной структуры управления доступом.

8.5.3 Шифрование потока управления сетью

Шифрование рекомендуется для всего трафика данных, используемого в целях обеспечения возможности управления сетью, для гарантии конфиденциальности и целостности данных. Корпорации все больше используют внутреннее управление сетью, и поэтому необходимо обособление трафика управления путем применения шифрования. Шифрование трафика управления предоставляет высокую степень защиты от штатных сотрудников, за исключением немногочисленной группы таких сотрудников, у которых есть законный доступ к ключам шифрования. Должно обеспечиваться шифрование между клиентами центра управления сетью (NOC) и серверами системы управления элементами (EMS) и/или элементами сети, включая трафик SNMP, поскольку существуют известные уязвимости, связанные с SNMP версий 1 и 2; на них обращено внимание в SNMP версии 3. В зависимости от типа трафика для этих линий нужно использовать протоколы безопасности TLS, IPSec и безопасную оболочку (SSH) (см. [b-IETF RFC 4252]). Оболочка SSH является протоколом безопасности уровня приложения, который непосредственно замещает Telnet (см. [b-IETF RFC 854]) и FTP (см. [b-IETF RFC 959]), но не может нормально использоваться для защиты других типов трафика. Протокол IPSec, с другой стороны, работает как раз между сетевым уровнем (уровень 3) и транспортным уровнем (уровни 4) и может использоваться для защиты любого типа трафика данных, независимо от используемых приложений и протоколов. IPSec является предпочтительным методом для использования, однако SSH может использоваться, если трафик состоит только из Telnet и FTP. Если трафик HTTP используется для обеспечения возможности управления сетью между клиентами NOC и EMS и/или сетевыми элементами, то этот трафик может быть защищен с помощью технологии TLS. Внешнее устройство VPN IPSec может использоваться в разных частях сети для защиты потока управления.

8.5.4 Безопасный удаленный доступ для операторов

Должна быть обеспечена безопасность операторам и администраторам, которые управляют сетью из отдаленного местоположения по сети общего пользования. Предпочтительным решением является предоставление безопасной виртуальной частной сети, использующей IPSec, так как она предоставит криптостойкое шифрование и аутентификацию для всех удаленных операторов. Например, возможно размещение продукта VPN в интерфейсе системы управления, и все операторы должны быть оснащены клиентами доступа к экстрасети для своих портативных компьютеров или рабочих станций.

8.5.5 Брандмауэры

Разделение среды управления сетью с помощью использования сетей VLAN и брандмауэров считается целесообразным применительно к приложениям принципов обеспечения безопасности различной степени. Брандмауэр контролирует тип (протокол, номер порта, источник и адрес назначения) трафика, который используется для пересечения границы между доменами безопасности. В зависимости от типа брандмауэра (приложение по отношению к фильтрации пакетов) его действие может быть распространено на фильтрации содержания приложения этого потока данных. Местоположение брандмауэра, его тип и правила фильтрации индивидуальны для каждой конкретной сетевой реализации.

8.5.6 Обнаружение проникновений

Системы обнаружения проникновений на основе главного компьютера можно объединять в серверы управления для предоставления защиты от сетевых проникновений. Системы обнаружения проникновений могут использоваться для предупреждения сетевых администраторов о возможности инцидента, связанного с безопасностью, например взлом сервера или взлома типа "отказ в обслуживании".

8.5.7 Уровень безопасности приложения

Рекомендуется усиление защиты всех операционных систем, используемых для обеспечения возможности управления сетью. С этой целью во всех операционных системах, применяемых для обеспечения возможности управления сетью, должна быть усилена защита, будь то операционные системы общего назначения или встроенные операционные системы с функцией реального времени. Что касается операционных систем, в отношении которых отсутствуют конкретные указания на усиление защиты, то производителю операционной системы следует рекомендовать получать самые последние вставки в программы и процедуры для усиления защиты.

8.5.8 Программное обеспечение, не содержащее вирусов

Все программное обеспечение, как собственной разработки, так и купленное у третьей стороны, следует проверять и в максимально возможной степени гарантировать отсутствие вирусов. Должен быть разработан процесс проверки на вирусы, в который входит сканирование всего программного обеспечения с помощью специального средства обнаружения вирусов до встраивания этого программного обеспечения в продукт.

8.6 Многоуровневая безопасность приложения, сети и управления сетью

В каждой организации и предприятии имеются разный порог безопасности и разная технологическая инфраструктура. Приложения, реализованные на основе интернета, представляют повышенные риски и угрозы для предприятия. Интернет-приложения могут иметь встроенную безопасность на прикладном уровне. Однако, используя функциональные возможности безопасности, которые могут быть предоставлены нижними уровнями сети, можно повысить безопасность приложений.

Предприятия, в которых есть интернет, должны быть особенно осторожными при разработке своих сайтов. [b-IETF RFC 2196] (Справочник по безопасности сайтов) предоставляет хорошую справочную информацию о безопасности сайтов. На прикладном уровне рекомендуется использовать мелкомодульную структуру политики в области безопасности. Должна быть возможность обращения объектов к уровню унифицированных идентификаторов ресурсов (URI). Должны блокироваться те функциональные возможности, в которых нет необходимости. По возможности должен использоваться протокол TLS. Рекомендуется использовать шлюзы прикладного уровня и сосредоточивать внимание на строгих аутентификации и санкционировании. Услуги электронной почты (E-mail) должны быть защищены путем использования S/MIME (см. [b-IETF RFC 2311)] и

таких методов, как программа PGP (см. [b-IETF RFC 1991]), если это возможно в рамках инфраструктуры обеспечения безопасности.

На сетевом уровне должны использоваться те методы, которые описаны в пункте 8.7, для гарантирования предприятию приемлемой безопасности. Безопасность достигается посредством использования уровневой архитектуры, которая может быть приспособлена к требованиям в области безопасности каждого типа предприятия.

Обеспечение безопасности трафика управления сетью является существенным требованием для обеспечения безопасности сети. Этого можно добиться, прежде всего, путем гарантирования того, что усилена защита операционной системы против известных угроз. Производителю операционной системы следует рекомендовать получать самые последние вставки в программы и процедуры для усиления защиты ОС. Должны быть предприняты меры для проверки всего установленного программного обеспечения на отсутствие известных вирусов. Предпочтительно постоянно зашифровывать весь трафик управления, используя IPSec или TLS, для защиты трафика HTTP. Шифрование является целесообразным и рекомендуется, если трафик выходит за пределы местной LAN. SNMPv3 и RADIUS с множеством уровней механизмов контроля, включая использование сильных паролей, рекомендуются операторам сетей в целях управления удаленным доступом, и отдается предпочтение возможности централизованного контроля системы управления доступом. Журналы безопасности важны для сбора данных о трафике управления сетью.

8.7 Живучесть сети даже в момент взлома

В современных условиях сеть предприятия обеспечивает проведение ответственных операций и важна для осуществления деловой деятельности. Сеть должна быть безопасной, надежной и доступной для деловых партнеров.

Существует много методов, которые можно использовать для гарантирования надежности сети. Надежность сети гарантирует надлежащую работу сети, когда программное обеспечение и/или элементы аппаратного обеспечения выходят из строя. Однако при наличии угроз безопасности моделью является концепция живучести сетей. Сеть, обладающая живучестью, это такая сеть, которая продолжает своевременно выполнять минимальный набор важных функций при взломах. Важные выполняемые функции заключаются в своевременном предоставлении важных услуг, даже если какие-то части сети недосягаемы или вышли из строя из-за взлома.

Разработка сетей, обладающих живучестью, должна начинаться с организации сетевых услуг двух категорий – важных услуг и неважных услуг. Живучесть означает, что сеть была способна противостоять попытке нарушения защиты. Должна существовать четкая стратегия того, каким образом действовать и осуществлять восстановление после взлома. В зависимости от типа взлома, возможны разные стратегии противостояния, идентификации и восстановления, которые могут быть продуманы администратором сети. Одной из характеристик сети, обладающей живучестью, является адаптируемость. Например, сеть может изменить маршрут трафика от одного сервера к другому, если на первом сервере обнаружены вторжение или взлом.

На этапе разработки политики в области безопасности необходимо определить важные услуги, которые, как предполагается, сеть будет предоставлять даже в случае взломов. На этом этапе должно быть установлено, как сеть будет противостоять попытке нарушения защиты, каким образом сеть будет бороться с такими попытками и каков наилучший метод восстановление сети после взломов. В анализе должны быть рассмотрены системы управления, главные компьютеры, приложения, маршрутизаторы и устройства коммутации.

Устойчивость сети, обладающей живучестью, к попытками нарушения защиты возрастает при использовании механизмов управления доступом со строгой аутентификацией и шифрованием. Использование фильтрации сообщений и пакетов, а также сегментация сетей и серверов, также повышает устойчивость к попыткам нарушения защиты. Использование соответствующих методов обнаружения вторжения может оказать помощь в выявлении взлома. Для восстановления систем и сетей могут использоваться соответствующие методы резервирования.

Дополнение I

Методы, используемые злоумышленниками

(Настоящее Дополнение не является неотъемлемой частью настоящей Рекомендации)

В данном Дополнении коротко рассмотрены некоторые типы взломов, имеющих конкретное отношение к обработке данных и среде передачи данных.

I.1 Систематика угроз безопасности

Специалистам в области IT рекомендуется рассматривать свою сеть, как ресурс, к которому будут иметь доступ пользователи, которым, в общем случае, нельзя доверять. Существует множество средств, способов и методик, которое имеются у нарушителей для взлома сети. Хакеры могут использовать эти средства для начала многоуровневых попыток нарушения защиты с целью получения доступа к сети. В некоторых случаях злоумышленник будет использовать нарушение безопасности, а затем предпримет вторичные попытки нарушения защиты с тем, чтобы использовать другие части этой сети.

В этом пункте описаны способы, средства и методики, используемые нарушителями, хакерами и злоумышленниками для взлома сети.

I.1.1 Угрозы для санкционирования

Несанкционированный доступ к ресурсам сети является обычно результатом неподходящей конфигурации системы и использования брешей. Нарушители могут получить несанкционированный доступ, используя в своих интересах неудовлетворительную аутентификацию и санкционирование пользователей и задач в корпоративных системах или небрежное отношение служащих к инструкциям (например, сообщение паролей, когда пользователь вынужден запоминать множество паролей).

Практика ненадлежащего распределения скрытой области и совместное использование привилегий приложениями представляют собой серьезные источники уязвимостей. Для получения незаконного доступа могут применяться взломы с использованием обходных путей. Например, нарушители могут получить незаконный доступ, угадывая имена и пароли пользователей, используя словарь общих строк. Нарушители могут получить пароли с помощью алгоритмических средств. Пароли могут быть захвачены при передаче, если они передаются в открытом виде.

После угадывания имени пользователя и связанного с ним пароля злоумышленник получает доступ к ресурсам организации. Уровень доступа зависит от привилегий, который имеется у клиента, в отношении которого произведен взлом. Величина ущерба, который злоумышленник может нанести организации, зависит от его/ее намерений. В большинстве случаев хакеры будут использовать клиента, в отношении которого произведен взлом, для проникновения в это предприятие с "черного" хода.

В протоколах удаленного доступа к электронной почте, например IMAP, POP3 и POP2, используются простые способы аутентификации имен и паролей пользователей. Эти протоколы можно использовать для того, чтобы упростить криптоанализ методом перебора всех возможных вариантов. Существуют публикуемые методы, которые позволяют нарушителям использовать услуги этих протоколов, находясь на отдалении.

Существуют даже еще более сложные способы получения несанкционированного доступа. Для проведения взломов с имитацией соединения системы (спуфинг) могут использоваться черви, в результате чего компонент одной системы маскируется под другой. Например, черви могут использовать бреши в опции отладки sendmail и в .rhosts (например, используемой в UNIX) из-за нестрогой аутентификации. Опция отладки sendmail может быть поставлена в положение OFF (выключено). Оставление опции в положении ON (включено) является примером использования бреши.

I.1.2 IP-спуфинг

IP-спуфинг является сложным типом взлома, при котором используются доверительные взаимосвязи. Злоумышленник присваивает идентификаторы главного компьютера для подрыва безопасности целевого главного компьютера, используя способы маскирования. Поскольку целевой главный компьютер известен, он ведет разговор с пользующимся доверием главным компьютером.

Во время этого нападения нарушитель сначала идентифицирует пользующийся доверием главный компьютер, идентификатор которого будет присвоен. Это осуществляется, прежде всего, путем определения моделей доверия главного компьютера. Сюда обычно входит определение диапазона IP-адресов, которым этот компьютер доверяет. Следующим шагом является выведение главного компьютера из строя, так как злоумышленник присвоит его идентификаторы. Этой цели можно добиться использованием таких методов, как взломы типа лавинной адресации SYN TCP.

Попытки нарушения защиты типа IP-спуфинга могут быть успешными ввиду простоты подделки IP-адресов и ограничений методов аутентификаций сетевых адресов. IP-спуфинг ведется вслепую, так как злоумышленник может и не получить доступ к откликам от целевого главного компьютера. Однако злоумышленник может установить двустороннюю связь, если он будет манипулировать таблицами маршрутизации для использования IP-адреса подложного источника. Попытки нарушения защиты типа IP-спуфинга часто используются, как первая ступень для других нападений, таких как отказ в обслуживании (DoS) и взломы типа лавинной адресации.

Было бы уместно заметить, что у большинства (но, конечно, не у всех) ISP и во многих сетях наиболее ответственных предприятий в настоящее время проводится фильтрация исходящих адресов, что предотвращает прямые попытки нарушения защиты типа IP-спуфинга. В ответ на это нарушители заняты накоплением "ботнетов", для того чтобы сохранить свою анонимность.

I.1.3 Анализаторы сетевых пакетов

Анализаторы сетевых пакетов первоначально появились, как вспомогательный инструмент администраторов сетей, который позволяет им диагностировать проблемы, проводить анализ или улучшать качество функционирования сетей. Анализаторы сетевых пакетов работают на неподключенном сегменте сети, таком как сегменты, подключенные через концентратор. Таким образом, анализатор сетевых пакетов может видеть весь трафик на данном сегменте.

Более старые анализаторы сетевых пакетов считывали заголовки пакетов сетевого трафика и концентрировались на идентификации характеристик пакетов низкого уровня, таких как источник и адрес места назначения. Однако современные анализаторы могут декодировать данные из пакетов на всех уровнях модели OSI (взаимодействие открытых систем).

Злоумышленники могут использовать анализаторы сетевых пакетов для получения информации пользователя и паролей из пакетов, передаваемых по открытым и частным сетям. Путем использования анализаторов злоумышленники могут получать ценную информацию об именах и паролях пользователей, в особенности из таких приложений, как FTP, telnet и других, которые отправляют пароли в открытом виде. В протоколах для удаленного доступа к электронной почте (e-mail), таких как IMAP, POP3 и POP2 используются простые методы аутентификации имен и паролей пользователей. И они чувствительны для попыток нарушения защиты со стороны анализаторов сетевых пакетов.

Так как пользователи склонны многократно использовать пароли во множестве приложений и платформ, то злоумышленники могут использовать захваченную ими информацию для получения доступа к различным источникам в сети, где их конфиденциальность может быть нарушена. Более того, эти ресурсы также могут использоваться как стартовая позиция для других попыток нарушения защиты.

Обычно злоумышленники могут использовать сетевые анализаторы, подрывая физическую безопасность корпорации. Это эквивалентно тому, что кто-то ходит по предприятию и подключает свой портативный компьютер к сети. Эти риски также применимы к беспроводным сетям, в результате чего кто-либо может получить доступ к корпоративной локальной сети, находясь на автостоянке. Получение доступа к базовой сети пакетной передачи позволяет нарушителю определять конфигурации и режимы работы для будущего применения.

I.1.4 Отказ в обслуживании

Взломы типа DoS (отказ в обслуживании) направлены на недопущение законных пользователей к услугам. Взломы типа DoS являются легко реализуемыми, и они могут причинить значительный ущерб. Взломы типа DoS могут нарушить работу предприятия и фактически отключить его от остального мира. Распределенные взломы типа отказа в обслуживании используют ресурсы более чем одного компьютера для запуска синхронизированных взломы типа DoS на ресурс.

Взломы типа DoS могут принимать различные формы и быть нацелены на множество услуг. Взломы типа DoS сосредоточены на истощении ресурсов сети, серверов, главных компьютеров и приложений. Некоторые взломы типа DoS сосредоточены на нарушении возможности установления соединений. Например, в SYN-взломах типа лавинной адресации используются фиктивные полуоткрытые запросы на соединение по протоколу TCP, которые истощают объем памяти целевого ресурса. Эти типы взломов могут препятствовать доступу законных пользователей к главным компьютерам, веб-приложениям и другим ресурсам сети. В результате взломы типа DoS может произойти:

- отказ в возможности установления соединений с интернетом;
- отказ законным пользователям в доступе к сетевым элементам;
- отказ законным пользователям в доступе к приложениям.

Взломы типа DoS используют слабости в архитектуре взламываемой системы. В некоторых случаях используются слабости многих обычных протоколов интернета, таких как протокол управления сообщениями в интернете (ICMP). Например, при некоторых взломах типа DoS большое количество эхо-пакетов (ping) ICMP отправляется по широковещательному IP-адресу. В этих пакетах используется подложный IP-адрес потенциальной цели. Отклики, возвращающиеся назад к цели, могут повредить ее. Эти типы взломов называются "smurf"-взломами. В другой форме взлома используются пакеты UDP, но он действует по тому же принципу.

I.1.5 Взломы типа "пожарная цепочка"

Взломы типа "пожарная цепочка" известны также как "взломы через посредника". В этом виде нападения нарушитель перехватывает сообщения при обмене с открытым ключом между сервером и клиентом. Нарушитель передает эти сообщения повторно, заменяя открытый ключ на тот, который требуется. Первоначальные стороны будут думать, что они общаются друг с другом. Злоумышленник может просто получить доступ к этим сообщениям или может изменять их. Для запуска таких попыток нарушения защиты могут быть использованы анализаторы сетевых пакетов.

I.1.6 Обходные пути

Обходные пути – это методы получения быстрого доступа к сетевым ресурсам, которые могли быть:

- преднамеренно размещены разработчиками системы, чтобы дать возможность быстрого доступа во время разработки, и которые не были удалены после нее;
- размещены служащими в целях содействия выполнению своих обязанностей;
- частью установок стандартной операционной системы, которые не были удалены путем усиления защиты, например комбинации идентификатора пользователя по умолчанию для входа в систему и паролей;
- размещены недовольными служащими, чтобы иметь доступ после завершения;
- созданы при выполнении вредоносных кодов, например вирусов.

I.1.7 Нелегальное проникновение

Нелегальное проникновение связано с необходимостью выдавать себя за обслуживающий либо инженерный персонал для получения доступа к сети, и является лишь верхушкой айсберга, состоящего из целого ряда угроз, которые основаны на брешах в физической безопасности и уязвимости, обусловленной человеческим фактором. Например, нарушитель может изменить данные, связанные с конфигурацией уровней управления и сигнализации, а также данные выставления счетов и данные об использовании.

I.1.8 Взлом защиты путем замещения оригинала

Такой взлом происходит, если сообщение или часть сообщения повторяется для того, чтобы произвести недозволенный эффект. Например, объект повторяет законное сообщение, содержащее информацию об аутентификации, для того, чтобы аутентифицировать себя.

I.1.9 Изменение сообщений

Изменение сообщений происходит, если содержание передачи данных изменяется, оно не обнаруживается и приводит к недозволенному эффекту.

I.1.10 Попытки взлома защиты внутренними нарушителями

Попытки взлома защиты внутренними нарушителями происходят, если законные пользователи или система ведут себя непредусмотренным или неразрешенным образом. Во многих известных компьютерных преступлениях участвовали внутренние злоумышленники, которые нарушали безопасность системы. Тщательный отбор персонала и непрерывное осуществление мер, направленных на защиту аппаратной части, программного обеспечения и осуществление политики в области безопасности, может помочь уменьшить риски, связанные с попытками взлома защиты внутренними нарушителями. Целесообразно также располагать надлежащими следами аудита для увеличения вероятности обнаружения таких попыток.

I.2 Угрозы безопасности

Все типы организаций, например предприятия, сталкиваются с широким кругом угроз. Нужды безопасности и рекомендуемая стратегия безопасности каждой организации уникальны и неодинаковы. Самой требовательной средой с точки зрения обеспечения безопасности является открытое предприятие. В этом случае обеспечение безопасности рассматривается по отношению ко всему предприятию в целях управления доступом служащих, партнеров и даже заказчиков к базам данных и приложениям предприятия.

I.2.1 Попытки нарушения защиты на прикладном уровне

Попытки нарушения защиты на прикладном уровне могут принимать различные формы и использовать различные методы. Так как главные веб-компьютеры доступны большому количеству людей и известны адреса портов, определяемые такими протоколами, как HTTP (порт 80), то хакеры могут использовать эту информацию для осуществления попыток нарушения защиты, которые способны обойти брандмауэры.

Попытки нарушения защиты на прикладном уровне используют уязвимости в операционной системе и приложениях, чтобы получить доступ к ресурсам. Неправильная конфигурация и санкционирование могут привести к образованию брешей в системе безопасности. Например, главный компьютер может быть веб-сервером и должен предоставлять всем запрашиваемые веб-страницами. В соответствии с политикой в области безопасности, главные компьютеры могут ограничивать доступ к командной оболочке санкционированными администраторами.

Сбор данных о счетах нацелен на процесс аутентификации, когда приложение запрашивает идентификатор пользователя для входа в систему и пароль. Приложения, которые создают разные сообщения об ошибках при неверных идентификаторах пользователя для входа в систему и неправильных паролях, уязвимы в отношении попытки взлома этого типа. Основываясь на типе сообщения об ошибках, нарушитель может скорректировать эту попытку, при этом сначала будет определяться действительный идентификатор пользователя для входа в систему, а затем использоваться другая форма методов взлома пароля для его получения.

Попытки нарушения защиты на прикладном уровне могут быть основаны, среди прочего, на вирусах, червях, переполнении буфера и сборе паролей. Появление в технологиях веб-услуг и единой подписи только усугубляет проблему, так как они тяготеют к унаследованным веб-приложениям. Эти приложения разрабатывались без учета возможности осуществления веб-соединений и обеспечения безопасности.

Некоторые попытки нарушения защиты на прикладном уровне просто нацелены на разрушение веб-сайта. Другие попытки портят объекты cookies (маркеры), чтобы получить недозволенную информацию о конкретном сервере. Приложения, как правило, не проверяют действительность объектов cookies и могут стать жертвами выполнения зловредных кодов, которые спрятаны в этих объектах. В современных браузерах существуют известные уязвимости, из-за которых возможны попытки нарушения защиты основе объектов cookies.

Нарушитель также может использовать метод межсайтового создания сценария, чтобы ввести зловредный код в виде сценарной метки, которая добавляется к URL. Этот код начнет выполняться, как только ничего не подозревающий пользователь щелкнет на этот URL. Использование TLS может решить некоторые из этих проблем обеспечения безопасности на уровне приложения. Однако SSL не может полностью защитить веб-приложения. Даже с использованием SSL могут быть предприняты такие попытки нарушения защиты, как сбор счетов и взлом паролей.

Для уменьшения угроз на прикладном уровне рекомендуется усиливать защиту операционных систем, используемых для осуществления возможности управления сетью, будь то операционные системы общего назначения или встроенные операционные системы с функцией реального времени. Необходимо следовать конкретным и самым последним указаниям производителя по усилению защиты. Для некоторых унаследованных систем, в которых применяются более старые операционные системы, у производителя может не оказаться вставок в программу, относящихся к обеспечению

безопасности. Также рекомендуется использовать безопасную электронную почту, брандмауэры прикладного уровня, системы обнаружения и предотвращения вторжений в главный компьютер, методики сильной аутентификации, сильные пароли, и надлежащий выходной контроль на веб-сайтах, который предотвратит отображение несанкционированных изменений веб-содержания.

I.2.2 Угрозы на сетевом уровне

Злоумышленник может использовать профессиональные средства для осуществления попыток нарушения защиты на сетевом уровне, имеющих различную степень серьезности. Расширенные и открытые предприятия особенно уязвимы к взломам защиты на сетевом уровне. Ряд серьезных угроз безопасности обычно связывается с сетевой инфраструктурой. К этим угрозам относятся вредительство, вандализм, плохая конфигурация системы, отказ в обслуживании, перехват, промышленный шпионаж и кража услуг. Попытки нарушения защиты могут предприниматься внутренними злоумышленниками, а также внешними источниками, например хакерами.

Новые достижения хакерских технологий, такие как сканеры портов на основе подвижных терминалов, показывают, что попытки нарушения защиты сетевой инфраструктуры могут также осуществляться с подвижных терминалов. Рекомендуется создать надлежащую политику в области безопасности и разработать четкий процесс ее обеспечения для защиты сетевой инфраструктуры. Коммутаторы, маршрутизаторы, точки доступа, серверы удаленного доступа, точки беспроводного доступа, главные компьютеры и другие ресурсы являются типичными объектами, которые следует защищать.

Следующие угрозы сетевой инфраструктуре и ее уязвимости, являются типичными для пакетных IP-сетей:

1) Распространение небезопасных протоколов: В некоторых сетях все еще используют протоколы, у которых, как известно, есть уязвимости для безопасности. К таким протоколам относятся ICMP, TELNET, SNMP версий 1 и 2, DHCP, TFTP, RIP версии 1, NTP, DNS и HTTP.
2) Использование слабых, локально управляемых статичных паролей: в некоторых сетях все еще разрешается использовать слабые пароли, основанные на коротких словах обычного словаря, которые легко разгадать. Некоторые администраторы могут использовать один пароль к сетевым элементам; который может использоваться совместно и может быть известен всем администраторам.
3) Незащищенная информация, относящаяся к безопасности: в некоторых сетях такая важная информация, как файлы паролей, не зашифровывается. Другая информация, например пароли, передается по сети в открытом виде. Наборы правил для брандмауэров установлены ненадлежащим образом, и применяются слабые шифроключи.
4) Загрузки неаутентифицированного программного обеспечения и файлы конфигурации: угрозы для сети может представлять загрузка неверного или зловредного программного обеспечения или файлов конфигурации, это может вызвать потери в обслуживании и повлечь за собой неудовлетворительное качество функционирования. Такая практика открывает такие бреши в безопасности, как установка троянских коней или другого зловредного кода внутренними нарушителями или посторонними субъектами. Эта практика также ведет к неверной конфигурации устройств.
5) Сетевые элементы и операционные системы, не имеющие усиленной защиты: угрозы для сетей могут представлять загрузки заводских операционных систем, не имеющих усиленной защиты от распространенных попыток взлома. К этому же относится функционирование ненужных услуг, в отношении которых продолжают действовать счета и пароли по умолчанию.
6) Порты и интерфейсы управления, без необходимости открытые для сети общего пользования: угрозы для сети могут исходить от внутриполосных интерфейсов управления, которые остаются доступными для интернета общего пользования. Дополнительные угрозы могут возникать из-за злоупотреблений со стороны вспомогательного механизма, например доступа к базовой сети во вспомогательном режиме по коммутируемой телефонной линии, ЦСИС или путем другого соединения.

I.2.3 Несанкционированный доступ

Несанкционированный доступ – этот термин, который может относиться к ряду различных видов попыток нарушения защиты. Максимальный результат для нарушителя заключается в получении доступа к некоторому ресурсу незаконным образом. Эта проблема безопасности имеет место для всех типов предприятий. Любое предприятие, обеспечивающее возможности доступа в интернет или к удаленным LAN, подвержено попыткам взлома защиты для получения несанкционированного доступа.

Услуги удаленного доступа, которые позволяют находящимся в поездке служащим подключаться к сети для доступа к электронной почте, удаленным офисам, соединенным по телефонным линиям, внутренним сетям и экстрасетям, соединяющим внешние стороны с сетью предприятия, могут сделать сеть уязвимой для хакеров, вирусов и других нарушителей. Хакеры могут использовать профессиональные средства для получения доступа к сети предприятия, при этом информация, содержащая особо важные сведения, может подвергаться риску, или сеть может использоваться для осуществления попыток взлома других сетей.

Защита сетей на различных уровнях может помочь предотвратить несанкционированный доступ. На сетевом уровне использование брандмауэров, серверов-посредников и фильтрации при подключении пользователя к сеансу может дать дополнительную защиту, но похоже, что хакеры все время оказываются сообразительнее. Использование управления доступом пользователя на уровне сети и прикладном уровне с соблюдением надлежащей аутентификации и санкционирования может также минимизировать риски несанкционированного доступа.

I.2.4 Перехват

Перехват является трудной для обнаружения угрозой. Целью злоумышленника в этом случае является прослушивание и наиболее точная запись исходных данных о LAN предприятия. В этой попытке нарушения защиты используется "случайный режим" серийных Ethernet-адаптеров, которые продаются на рынке. Этот режим позволяет злоумышленнику захватывать каждый пакет в сети. В настоящее время в интернете имеется большое количество бесплатных анализаторов сетевых пакетов, которые злоумышленник может использовать для перехвата.

Предприятие любого типа, позволяющее осуществлять удаленный доступ, уязвим для такого рода атак. Наибольшему риску подвергаются открытые и расширенные предприятия. Коммутация по сети Ethernet является совершенно неэффективной для противодействия угрозам перехвата, так как ARP-спуфинг может полностью разрушить механизм коммутации. Коммутация Ethernet может помешать только "ленивому перехватчику". Использование строгих методов управления и шифрования может минимизировать угрозу таких попыток нарушения защиты.

Дополнение II

Области технологий кибербезопасности

(Настоящее Дополнение не является неотъемлемой частью настоящей Рекомендации)

Сложность и эффективность технологии нападения все время совершенствуется. В наше время злоумышленники могут быстро разрабатывать атаки, чтобы использовать уязвимые места, обнаруженные в продукции. Нападающие могут автоматизировать эти атаки и сделать их доступными для широкой публики. Примеры доступных технологий представлены в таблице II.1.

Таблица II.1 – Технологии кибербезопасности

Методы	Категория	Технология	Цель
Криптография	Сертификат и архитектура открытого ключа	Цифровые подписи	Используется для того, чтобы разблокировать выпуск и сохранение сертификатов, которые будут использоваться в цифровом виде
		Шифрование	Используется для шифрования данных во время передачи и хранения данных
		Обмен ключами	Устанавливает или сеансовый ключ, или ключ управления информационным обменом, чтобы им пользоваться для безопасной связи
	Гарантия	Шифрование	Страхует аутентичность данных
Контроль доступа	Защита периметра	Брандмауэр	Контроль доступа в сеть и из сети
		Управление содержанием	Ведет текущее наблюдение за потоком несовместимой информации
	Аутентификация	Однофакторная	Система, использующая комбинации идентификатора/пароля пользователя для проверки идентификатора
		Двухфакторная	Система, которой требуется два компонента для того, чтобы предоставить доступ пользователя к системе, такие как владение физическим маркером плюс знание секрета
		Трехфакторная	Добавляет еще один фактор идентификации, такой как биометрический или измеренную характеристику человеческого тела
		Смарт-маркеры	Устанавливает заслуживающие доверия идентификаторы с помощью особой схемы в устройстве, например смарт-карте
	Санкциониро-вание	На ролевой основе	Механизмы санкционирования, которые управляют доступом пользователя к соответствующим ресурсам системы, основанные на присвоенной роли
		На основе правил	Механизмы санкционирования, которые управляют доступом пользователя к соответствующим ресурсам системы, основанные на особых правилах, связанных с каждым пользователем, независимо от его роли внутри организации

Таблица II.1 – Технологии кибербезопасности

Методы	Категория	Технология	Цель
Целостность системы	Антивирус	Методы подписи	Защищает от злонамеренного компьютерного кода, такого как вирусы, черви и Троянские кони, используя их кодовые подписи
		Методы поведения	Проверяет текущие программы на несанкционированное поведение
	Целостность	Обнаружение вторжения	Может использоваться для предостережения системных администраторов о возможности происшествий, связанных с безопасностью, таких как дискредитация файлов на сервере
Аудит и мониторинг	Обнаружение	Обнаружение вторжения	Сравнивает поток сети и элементы регистрации в узле для подбора данных о подписях, которые являются указаниями на хакеров
	Предотвращение	Предотвращение вторжения	Обнаружение атак на сеть и проведение мероприятий, как определено организацией, для смягчения этих атак. Подозрительные действия запускают сигналы тревоги администратора и другие реконфигурируемые отклики
	Регистрация	Инструменты регистрации	Ведет текущее наблюдение и сравнивает поток в сети и элементы регистрации в узле для подбора данных о подписях и профилях адресов в узле, которые являются указаниями на хакеров
Управление	Управление сетью	Управление конфигурацией	Учитывает контроль и конфигурацию сетей и аварийный функциональный набор
		Управление внесением исправлений	Устанавливает самые последние обновления, подстраивает к устройствам сети
	Политика	Принуждение	Дает возможность администраторам вести мониторинг и принудительно проводить политики безопасности

II.1 Криптография

Криптография это применение операции преобразований к данным в простом виде для того, чтобы зашифровать их секретным кодом. Дешифрование секретных данных может восстановить первоначальный простой текст. Современные имеющиеся в наличии методы криптографии могут использоваться для шифрования/дешифрования данных. Она также может использоваться для аутентификации отправителя сообщения и неотказуемости.

Криптография играет важную роль в защите информации во время хранения ее в устройстве или на носителе данных и во время ее передачи по линиям связи.

В криптографии задача зашифровывания данных в секретный код посредством использования математических алгоритмов известна, как шифрование данных. Дешифрование данных, с другой стороны, выполняет противоположную функцию для того, чтобы ее применение к зашифрованным данным восстанавливало первоначальные данные. Криптография пользуется секретными ключами для выполнения процесса шифрования и дешифрования.

Методы криптографии могут быть поделены на два основных типа: симметричного ключа и асимметричного ключа.

1) Криптография симметричного ключа использует алгоритмы, в которых ключ шифрования и ключ дешифрования один и тот же. Безопасность такой модели зависит от трудности разгадки этого ключа. Стороны, обменивающиеся информацией, должны договориться по поводу ключа и держать этот ключ в тайне от остальных. В примеры алгоритмов симметричного ключа можно включить стандарт тройного шифрования данных (3DES) и улучшенный стандарт шифрования (AES).

2) Криптография асимметричного ключа использует один ключ для шифрования данных и другой ключ для дешифрования закодированного текста. В этом виде криптографии у пользователя будет свой частный ключ, известный только ему, и открытый ключ, известный другим. Открытым ключом пользуются все остальные для шифрования открытого текста. Но только держатель соответствующего частного ключа сможет расшифровать зашифрованный текст.

Методы криптографии симметричного ключа в общем случае более быстродействующие, чем методы асимметричного ключа. Однако главное осложнение для криптографии симметричного ключа заключается в проблеме рассылки ключа. Как таковые, они обычно не рассматриваются для обширных развертываний. С другой стороны, криптография асимметричного ключа (также известная, как криптография открытого ключа) снимает некоторые ограничения управления ключом криптографии симметричного ключа. Криптография открытого ключа полагается на использование цифровых сертификатов для решения вопроса управления открытым ключом и отмены. Для повышения быстродействия методы криптографии открытого ключа могут использоваться как средство обмена безопасным образом симметричным ключом, для использования в сеансе или в операции связи.

Цифровые подписи являются примером практической реализации технологии криптографии открытого ключа. Цифровой сертификат обеспечивает гарантию связи между открытым ключом и владельцем сертификата. Цифровые подписи могут обеспечить аутентификацию, целостность данных и неотказуемость для операций связи. Цифровые подписи могут использоваться для подтверждения доказательства заявленного идентификатора отправителя сообщения. Цифровые подписи часто используются в связке с цифровыми сертификатами. Цифровые сертификаты используются, как транспортные средства, переносящие информацию, которая требуется в криптографии открытого ключа, и цифровые подписи. Цифровые сертификаты могут быть выпущены для пользователей посредством утвержденных или доверенных органов.

Код аутентификации сообщений (MAC) является контрольной суммой аутентификации, полученной с помощью применения схемы аутентификации вместе с секретным ключом к сообщению. В противоположность методам цифровых подписей, MAC вычисляется и проверятся с помощью использования одного и того же ключа. Таким образом коды MAC могут быть проверены только предназначенным адресатом. В хэш-функции, на основе кодов MAC (HMAC) (см. [b-IETF RFC 2104]) ключ (или ключи) используется в связке с хэш-функцией для получения контрольной суммы, которая прикрепляется к сообщению.

II.2 Технологии контроля доступа

Контроль доступа нацелен на гарантирование того факта, что только санкционированный пользователь может получить доступ к устройству сети или к подключенной системе. Фактически, контроль доступа дает возможность специалисту IT лучше проанализировать и понять тип и природу атак, которые происходят в его сети. Существует много методов, которые могут быть использованы для реализации контроля доступа. Эти методы обсуждаются в следующих пунктах.

II.2.1 Защита периметра

Технология защиты периметра предотвращает доступ к сети или компьютеру со стороны непроверенных или несанкционированных внешних пользователей. Технологии защиты периметра устанавливают логические или физические границы между защищаемыми областями и областями, открытыми для общего пользования и для непроверенных внешних пользователей (это не относится к непроверенным внутренним пользователям). Технология защиты периметра может применяться для защиты сети или отдельного устройства. В примеры технологий защиты периметра входят:

1) Фильтрация содержания или программное обеспечение управления содержанием ограничивает тип данных, которые могут быть доступны или распространены в сети (см. [b-ISO/IEC 10828-3]). Она ограничивает возможность пользователей получать доступ к содержанию за пределами их границ. Это минимизирует возможности скачать вирусы и другие злонамеренные коды из непроверенных мест. Фильтрация содержания может принимать форму фильтров URI (см. [IETF RFC 2396]), с ее помощью может быть отказано в доступе пользователям веб-страниц с сомнительным содержанием. Фильтрация содержания может использоваться для сканирования сообщений приложений, таких как электронная почта на предмет вирусов спама или неутвержденного содержания.

2) Брандмауэр: Эту технологию (см. [b-ISO/IEC 10828-3]) можно разделить на четыре обширные категории: фильтры пакетов, шлюзы уровней цепи, шлюзы уровней приложений и брандмауэры многоуровневой проверки с изменяемым состоянием

- Брандмауэр фильтрации пакетов работает на уровне IP. Они обычно являются частью брандмауэра маршрутизатора. Они сравнивают каждый пакет IP с определенным набором правил до того, как переадресовать его по следующему маршруту или в его конечный пункт назначения. В зависимости от результатов проверки, брандмауэр может удалить этот пакет, переадресовать его или отправить сообщение автору. В правила может входить адрес IP источника или пункта назначения, номер порта источника или места назначения и используемый протокол. Маршрутизаторы протокола трансляции сетевых адресов (NAT) предлагают преимущества брандмауэров фильтрации пакетов и дополнительно могут также скрыть адреса IP устройств за этим брандмауэром. Брандмауэры фильтрации пакетов оказывают незначительное влияние на работу сети и предоставляют некоторую степень защиты на этом сетевом уровне.
- Шлюзы уровней цепи работают на уровне протокола управления передачей (TCP) протоколов TCP/IP для того, чтобы осуществлять мониторинг квитирования TCP между пакетами для выяснения того факта, является ли запрашиваемый сеанс законным или нет. Более того, запросы, исходящие для удаленного компьютера через шлюз уровней цепи, предстанет перед получателем, как если бы он был создан в этом шлюзе. Этот метод помогает скрыть информацию о защищаемой сети. Шлюзы уровней цепи не фильтруют индивидуальные пакеты.
- Прокси-серверы или шлюзы уровней приложений могут фильтровать пакеты на уровне приложений модели OSI. Входящие или исходящие запросы не могут получить доступ к услугам, в которых нет прокси-серверов. Прокси-серверы проверяют пакеты на уровне приложений, чтобы отфильтровать конкретные команды приложений, такие как HTTP POST (см. [b-IETF RFC 2616]). Прокси-сервер не допустит, чтобы не конфигурированный поток добрался до приложения. Прокси-серверы могут также использоваться для регистрации деятельности пользователя и регистрационных имен. Прокси-серверы могут предоставить высокий уровень безопасности при значительном влиянии на работу сети.
- Брандмауэры многоуровневой проверки с изменяемым состоянием объединяют аспекты, описанных выше типов брандмауэров. Многоуровневые брандмауэры фильтруют пакеты на сетевом уровне, устанавливают, являются ли пакеты сеанса действительными и фильтруют содержание пакетов на уровне приложения. Многоуровневые брандмауэры являются прозрачными для соединений между отправителем и получателем.

3) Протокол трансляции сетевых адресов (NAT): Эта технология предоставляет возможность скрыть схему адресации сети за средой брандмауэра. В NAT адрес IP системы во внутренней сети отображается на другой, соответствующий ему, внешний маршрутизируемый адрес IP. В NAT многие системы за брандмауэром имеют возможность совместно использовать один и тот же внешний адрес IP. Ресурсы за брандмауэром остаются доступными для внешних пользователей с помощью переадресации входящих подключений на определенные номера портов. NAT может быть реализован на большинстве сетевых устройств, таких как коммутаторы, маршрутизаторы и брандмауэры.

4) Шлюзы уровней приложений: Эти системы (см. [b-ISO/IEC 10828-3]) состоят из аппаратной и программной частей базового устройства или набора устройств. Они разрабатываются для того, чтобы ограничить доступ между двумя отдельными сетями. В этих системах используются методы проверки пакетов с изменяемым состоянием и прокси-сервером приложений для того, чтобы ограничить доступ между сетями. Можно также использовать сочетания и вариации (например, брандмауэры уровня цепи) этих методов. Более того, NAT может выполняться с помощью шлюзов уровней приложений.

5) Прокси-приложение: Эти системы (см. [b-ISO/IEC 10828-3]) обеспечивают понимание прикладного уровня предпринятых подключений, проверяя пакеты на высшем уровне стека протокола. У прокси-приложений имеется полный обзор обмена данными на уровне приложений. Эта возможность позволяет им без труда разглядеть мельчайшие подробности каждой попытки подключения и реализовать, в результате, политики безопасности. У прокси-приложений может иметься возможность прекращения подключений клиента и инициации нового подключения к внутренней защищенной сети. Эта возможность предоставляет дополнительную безопасность, так как она разделяет внешние и внутренние системы.

II.2.2 Виртуальная частная сеть (VPN)

В [b-ISO/IEC 18028-5] предоставлен всесторонний обзор использования VPN для организации защиты подключений в сетях.

Сети VPN в настоящее время используются для выполнения задач сетей взаимного подключения и как способ подключения удаленных пользователей к сетям. Сети VPN в их самой простой форме предоставляют механизм для создания безопасного канала или каналов данных по всей существующей сети или сквозной связи. Сети VPN могут создаваться и удаляться динамическим образом. Главная сеть может быть частной или общего пользования.

Удаленный доступ, использующий VPN реализуется на вершине обычной сквозной связи, которая уже установлена между местным пользователем и удаленным местоположением (см. [b-ISO/IEC 18028-5]). Сети VPN могут быть предоставлены, как управляемая услуга, в которой, на совместно используемой инфраструктуре, предоставляется безопасное, надежное подключение, управление и адресация, эквивалентные тем, которые есть в частной сети.

Существует множество способов представления типов сетей VPN (см. [b-ISO/IEC 18028-5]). В принципе, сеть VPN может быть:

– единичной сквозной связью (например, устройство клиента, имеющее удаленный доступ к сети предприятия через шлюз сайта); или

– связь пункт-эфир (используя методы MPLS (многопротокольная коммутация на основе признаков)).

Существует три основных типа VPN (см. [b-ISO/IEC 18028-5]):

– Сети VPN уровня 2 эмулируют средство LAN, используя подключения VPN, идущие по главной сети для связывания сайтов предприятия вместе, или для предоставления удаленного подключения к какой-либо организации. Типичными предложениями поставщиков услуг являются: виртуальное частное телеграфное агентство (VPWS), которое предоставляет только моделированное проводное соединение, или услуга виртуальной частной LAN (VPLS), которая предоставляет более полную эмулированную услугу LAN.

– Сети VPN уровня 3 эмулируют средство глобальной сети (WAN), используя сети VPN, проходящие по инфраструктуре сети. Предлагается возможность использования частных схем адресации IP по всей инфраструктуре общего пользования; практика, которая не разрешена в соединениях IP общего пользования. Однако использование частных адресов в сетях общего пользования посредством NAT может затруднить создание и использование безопасности Интернет протокола (IPSec) (см. [b-IETF RFC 2411]) VPN.

– Сети VPN уровня 4 используются для безопасных операций связи в сетях общего пользования. В этом типе VPN соединения обычно устанавливаются в TCP, который является протоколом уровня 4. Этот тип сетей VPN предоставляет безопасный канал между соединенными приложениями для гарантирования конфиденциальности и целостности данных на период операции связи.

Сети VPN могут быть реализованы внутри частной сети под управлением частного бизнеса или они могут быть реализованы в сетях в доменах общего пользования. Также возможны реализации, использующие сочетания этих двух схем. С одной стороны, каналы могут создаваться применением безопасных каналов, посредством использования туннелей, идущих через сети поставщиков интернет услуг. В этом отношении интернет общественного пользования является, фактически, базовой транспортной системой. По существу, конфиденциальность данных, которые переносятся сетью VPN, подвергается рискам в большей степени.

Туннель это тракт данных между устройствами, объединенными в сеть, который создается через существующую сетевую инфраструктуру. Этот туннель прозрачен для действий сети. Сеть VPN, созданная с помощью туннелей, в общем случае является более гибкой, чем сеть, на основе физических связей. Туннели могут создаваться посредством использования виртуальных сетей, коммутации с помощью меток-признаков или инкапсуляции протоколов.

Аспекты безопасности различных типов сетей VPN предоставлены в таблице II.2.2 (см. [b-ISO/IEC 18028-5]).

Таблица II.2.2 – Аспекты безопасности VPN

VPN	Технология	Аутентификация пользователя	Шифрование данных	Управление ключом	Проверка целостности
VPN уровня 2	Ретрансляция кадров, ATM, MPLS, PPP, L2F	N/A	N/A	N/A	N/A
	L2TP (см. [b-IETF RFC 2661])	Как в протоколе CHAP	N/A	N/A	N/A
VPN уровня 3	IPSec	Ключи предварительного общего секрета, на основе сертификата (пакета)	Несколько алгоритмов (пакетов), подлежащих согласованию	IKE	Подлежит согласованию
	IPSec с L2TP	Ключи предварительного общего секрета, на основе сертификата (пакета)	Несколько алгоритмов (пакетов), подлежащих согласованию	IKE	Подлежит согласованию
	MPLS	N/A	N/A	N/A	N/A
VPN уровня 4	TLS	На основе сертификата	Подлежит согласованию	Подлежит согласованию	Подлежит согласованию
	Безопасная оболочка	Созданная системой пара ключей (не сертифицированная)	Подлежит согласованию	Обмен открытыми ключами с отправителем данных	Подлежит согласованию
ПРИМЕЧАНИЕ 1. – Протокол защищенных секретов (SSL) может использоваться вместо протокола защиты транспортного уровня (TLS). ПРИМЕЧАНИЕ 2. – В [b-IETF RFC 3031] предоставлен обзор архитектуры многопротокольной коммутации на основе признаков (MPLS). В [b-IETF RFC 1661] описан протокол сквозного соединения (PPP). В [b-IETF RFC 2427] обсуждается многопротокольное соединение посредством ретрансляции кадров.					

II.2.3 Аутентификация

Для аутентификации пользователя могут применяться несколько методов. В эти методы входят: пароли, одноразовый пропуск, биометрические методы, смарт-карты [b-ISO/IEC-7816-x] и сертификаты. Аутентификация на основе паролей должна использовать сильные пароли (например, состоящие, по крайней мере, из восьми символов в длину и содержащие, как минимум, один буквенный, один численный и один специальный символ). Аутентификация только на основе пароля может оказаться недостаточной. Опираясь на оценку уязвимости, возможно понадобится сочетание аутентификации на основе пароля с другим процессом аутентификации и санкционирования, таким как сертификаты, облегченный протокол доступа к сетевым каталогам (LDAP), (см. [b-IETF RFC 3377]), служба удаленной аутентификации пользователей по коммутируемым линиям (RADIUS) (см. [b-IETF RFC 2869], [b-IETF RFC 3579] и [b-IETF RFC 3580]), Kerberos (см. [b-IETF RFC 1510]) и инфраструктура открытого ключа (PKI) (см. [b-IETF RFC 2459]).

Системы аутентификации могут быть поделены на категории в зависимости от количества требуемых факторов идентификации. Однофакторная аутентификация относится к системе, которая использует один фактор (например, сочетание идентификатора пользователя/пароля). Двухфакторная идентификация описывает процесс, в котором требуется два компонента для того, чтобы получить доступ в систему, такие как владение физическим маркером плюс знание секрета (например, пароля). В трехфакторной системе добавляется еще один фактор идентификации, такой как биометрический параметр или измерение характеристики человеческого тела. Использование большего количества факторов аутентификации приводит к более гарантированной аутентификации; однако включение большего количества факторов добавляет сложность, стоимость и расходы на управление. Отыскание оптимального соотношения выгод и потерь между простотой и безопасностью является основной задачей в любой системе аутентификации.

Однофакторная аутентификация на основе идентификатора пользователя/пароля в настоящее время является самой распространенной применяемой системой аутентификации. Системы аутентификации на основе пароля просты, легки в управлении и очень хорошо знакомы пользователям. При использовании сильных паролей однофакторные системы аутентификации могут обеспечить высокий уровень безопасности. Однако у действующих систем паролей есть некоторые проблемы, так как сильные пароли со сложной структурой трудны для запоминания пользователями. Как будет обсуждаться в этих рекомендациях ниже, эти недостатки можно свести к минимуму предоставлением оптимального решения с помощью системы "единого сильного пароля".

Во многих системах аутентификации в качестве второго фактора добавляются маркеры, такие как смарт-карты. Маркеры предоставляют дополнительную гарантию аутентификации, так как пользователь должен подтвердить физическое владение таким маркером для того, чтобы подтвердить свою подлинность. Атакующему также понадобится владение маркером пользователя для того, чтобы получить доступ в систему. Однако более высокий уровень аутентификации сопровождается дополнительным удорожанием системы из-за необходимости маркеров и устройств, считывающих маркеры. Вдобавок, маркеры легко теряются, а это означает высокие административно-хозяйственные расходы на повторный выпуск маркеров.

Сильная аутентификация, основанная на шифровании, может быть предоставлена при использовании цифровых сертификатов, которые выпускаются для пользователей и хранятся на маркерах или внутри памяти компьютера пользователя. Для гарантии того, что конкретный сертификат выпущен для пользователя законным образом, используются криптографические алгоритмы. Для гарантий выпуска и сопровождения цифровых сертификатов используется инфраструктура открытого ключа. Системы на основе сильного шифрования предоставляют очень сильную аутентификацию, однако такие системы дороги и, следовательно, требуются дополнительные расходы на управление; фактически, такие системы находят место в настоящее время только внутри сред с очень сильной охраной.

II.2.4 Санкционирование

После однократной аутентификации, механизмы санкционирования контролируют доступ пользователя к соответствующим ресурсам системы. Санкционирование может быть поделена на категории в зависимости от глубины детализации контроля, то есть, в зависимости от того, насколько подробно произведено разделение между ресурсами системы. Мелкомодульное санкционирование относится, в общем, к системам, в которых доступ контролируется с очень мелким шагом, таким например, как доступ к индивидуальным приложениям или услугам.

Санкционирование часто проводится "на ролевой основе", в соответствии с чем доступ к ресурсам системы основан на роли, назначенной для личности человека в организации. Для роли системного администратора может предоставляться доступ высокого уровня ко всем ресурсам системы, в то время как для роли обычного пользователя будет позволен доступ только к подмножеству этих ресурсов. Если применяется более мелкомодульное санкционирование, то для роли администратора трудовых ресурсов может предоставляться неограниченный доступ к очень секретным базам данных трудовых ресурсов (HR), а для роли учетной деятельности может предоставляться неограниченный доступ к базам данных систем бухгалтерского учета.

Санкционирование также возможно "на основе правил", в соответствии с которыми доступ к ресурсам системы основан на конкретных правилах, связанных с каждым пользователем, независимо от ее или его роли в организации. Например, правила могут устанавливаться только для доступа к считыванию или доступа к считыванию/записи всех или некоторых файлов внутри системы.

II.2.5 Протоколы аутентификации и санкционирования

Несколько протоколов обычно адаптировались для служб аутентификации. Протокол RADIUS (служба удаленной аутентификации пользователей по коммутируемым линиям) (см. [b-IETF RFC 2865]) широко используется для централизации служб аутентификации паролей. Первоначально задуманный для аутентификации удаленных пользователей, применяющих наборные устройства, протокол RADIUS был адаптирован для служб аутентификации обычных пользователей. LDAP (облегченный протокол доступа к сетевым каталогам) находит широкое применение в системах аутентификации и санкционирования. LDAP предоставляет подходящий метод для сохранения аутентификации пользователя и мандатов санкционирования.

Часто серверы аутентификации RADIUS применяются в паре с хранением мандатов в каталогах LDAP, для предоставления централизованной системы аутентификации и санкционирования. Когда пользователь делает попытку получить доступ к какому-то конкретному приложению в такой системе, приложение делает запрос о мандатах аутентификации у этого пользователя и они

отправляются в централизованную систему. В сервере RADIUS будет проведена проверка представленных мандатов на предмет совпадения с мандатами, хранящимися в базе данных LDAP, а также будет сделан запрос в базу данных LDAP об информации о правилах санкционирования. Результаты аутентификации (успешно пройдена или не пройдена) возвращаются в приложение с информацией о правиле санкционирования для конкретного пользователя. Правила санкционирования будут затем выполнены в приложении для того, чтобы дать пользователю доступ к конкретным данным или услугам. С точки зрения конечного пользователя, эти системы аутентификации и санкционирования являются автоматическими и простыми в использовании.

II.3 Антивирус и целостность системы

Черви, злонамеренные коды, вирусы и Троянские кони могут изменить систему и ее данные. Таким образом, важное значение приобретает использование технологий, которые проводят сканирование на наличие вирусов и гарантируют сохранность целостности системы.

Червь это программа, которая воспроизводится при помощи тиражирования самой себя из одной системы в другую, не требуя вмешательства человека. Вирусы могут прикрепляться к файлам пользователя и возрождаться к жизни тиражируя себя в другие файлы, если ничего не подозревающий пользователь предпримет какие-то действия, такие как открытие инфицированного файла. Троянский конь ведет себя иначе, представляя себя обычно ничего не подозревающему пользователю, как полезная программа, в которой заключен вредный код.

Антивирусные технологии помогают защитить системы от атак червей, злонамеренных кодов и Троянских коней. Это программное обеспечение может быть установлено в устройства пользователя или предоставлено, в качестве услуги, сетью или поставщиком интернет услуг. Технологии целостности систем используют программное обеспечение, которое проверяет тот факт, что только санкционированные обновления применяются к важным файлам системы.

В антивирусном программном продукте могут использоваться методы сигнатур строк для идентификации вирусов и злонамеренных кодов. Для этой технологии требуется предварительное знание злонамеренного кода, до того, как антивирусная программа сможет его распознать. По существу, для эффективной защиты требуются текущие значения их сигнатур в базе данных.

Проверка действий с помощью сканеров на наличие разрешенных действий осуществляется с помощью бегущего кода. Программное обеспечение уведомляет пользователя о подозрительных действиях. Активные сканнеры не всегда успешно действуют против вирусов, но могут быть более эффективными против червей и Троянских коней. Статические эвристические сканеры сканируют код для того, чтобы попытаться идентифицировать действия которые могут быть связаны с поведением, напоминающим поведение вирусов.

Методы целостности системы используют программное обеспечение, которое ведет текущее наблюдение за изменениями, которые проводятся в отношении важных файлов системы. Эти методы могут использоваться администраторами IT для выполнения проверок системы и определения того факта, удалось ли хакерам проникнуть в систему (у хакеров есть склонность оставлять тайные ловушки).

II.4 Аудит и мониторинг

Методы аудита и мониторинга дают возможность администраторам IT оценить безопасность системы в целом, включая инструкции по обнаружению и программное обеспечение для предотвращения вторжений. Администраторы IT могут использовать этот метод для выполнения анализа системы с целью обнаружения ее слабых мест после атаки. В некоторых случаях анализ системы может быть выполнен во время активной атаки на систему.

Система обнаружения вторжений (IDS) (см. [b-ISO/IEC 18043]) может использоваться для текущего наблюдения за сетью для гарантий того, что ни один несанкционированный пользователь не имеет доступа к сети. В большинстве приложений IDS сравнивается сетевой поток с регистрационными записями хоста для того, чтобы сравнить подписи данных и профили адресов хоста, указывающие на хакеров. Система обнаружения вторжений идентифицирует модели потока, которые указывают на присутствие несанкционированных пользователей. Подозрительные действия запускают сигналы тревоги администратора и другие конфигурируемые отклики. Система обнаружения вторжений (IDS) может быть в общих чертах поделена на категории, в соответствии со следующими критериями:

- Временные рамки обнаружения инцидента: в реальном времени или в режиме отключенной линии, в зависимости от того, производится ли анализ учетных записей системы и сетевого потока в момент времени, когда это событие происходит, или в пакетном режиме в течение нерабочих часов;

- Тип установки: в сети или в хосте. В IDS, установленное в сеть, как правило, включено множество устройств текущего контроля (часто предварительно-сконфигурированных приложений), которые устанавливаются в пунктах фильтрации в сети (где можно наблюдать весь поток между двумя пунктами). Для IDS, установленном в хосте, необходимо, чтобы программное обеспечение устанавливалось непосредственно на защищаемые серверы; с его помощью ведется текущее наблюдение за сетевыми связями и за деятельностью пользователя на этих серверах; и
- Тип реакции на инцидент: вмешивается ли IDS активным образом для предотвращения атак (например, с помощью изменения правил для брандмауэра или для фильтров маршрутизатора) или просто уведомляет персонал или другие сетевые системы о возникшей проблеме.

Большинство коммерческих продуктов IDS предоставляют сочетание возможностей мониторинга: сетевых и на основе хоста, в которых хост центрального управления получает сообщения от разных устройств наблюдения и подает сигнал тревоги для персонала поддержки сети. Использование программ IDS с сетевыми связями рекомендуется для большинства сетевых установок, в зависимости от конкретных нужд потребителей.

II.5 Управление

Методы управления конфигурацией дают возможность администраторам IT устанавливать и проверять установочные параметры безопасности на устройства в своих сетях. Управление политикой позволяет администраторам IT определять безопасность управления бизнесом и политики качества обслуживания QoS, осуществлять их в организации без необходимости понимания всех правил, относящихся к конкретным устройствам, и установочных параметров, которые необходимы для осуществления этих политик. Технически, политики являются набором правил для руководства, управления и контроля доступом к ресурсам IT; они должны быть выведены из деловых политик, определенных организацией. В пространстве безопасности управление политикой предназначено для запутанных проблем и трудных кривых обучения, связанных с этими методами (например, брандмауэрами, IDS, перечнями и фильтрами доступа, методами аутентификации), и недостатком системного обзора на разные части сети (центр обработки данных, удаленный офис, комплекс зданий).

В то время, как существуют многочисленные решения, предназначенные для частей проблемы, окончательная система управления политикой предоставляет централизованную сетевую конфигурацию, гарантирующую согласованную установку параметров безопасности в многочисленных узлах, что снижает риск уязвимости сети. Это не означает, что существует только одна система политики; в сети большего размера с многочисленными административными доменами, может возникнуть необходимость во множестве систем политики, каждая из которых отвечает за управление подмножеством устройств и согласованность между доменами.

Основным преимуществом полностью реализованной системы управления политикой является легкость в использовании и более защищенная среда. В идеальном случае сетевые администраторы хотели бы иметь возможность определять стратегии сетевых операций, используя не технический словарь, а кроме того, у них должна быть система политики, которая автоматически переводит эти термины в надлежащие механизмы безопасности, для их реализации в сети.

II.5.1 Эталонная модель управления политикой

На рисунке II.5.1 изображена архитектурная структура IETF для управления политикой ([b-IETF RFC 2753]). Эта эталонная модель используется в качестве образца для управления политикой, как безопасностью, так и управлением QoS. Таким образом, если управление политикой основано на этой модели, будет реализовано в сети и на всех уровнях данной архитектуры и будет доступно для всех типов пользователей и приложений, включая служащих, технических специалистов службы сети, партнеров и даже потребителей.

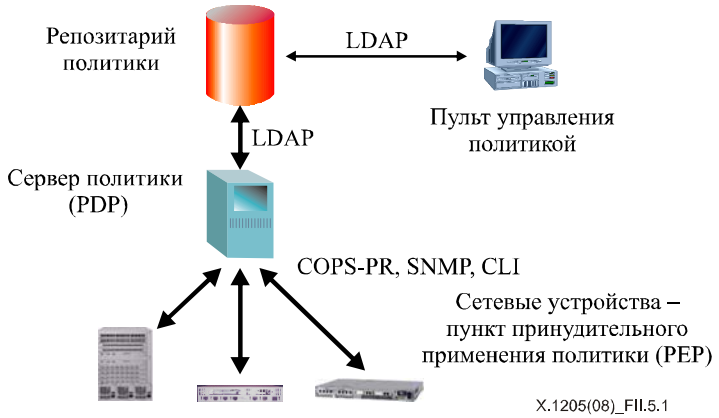

Рисунок II.5.1 – Эталонная модель управления политикой

В компоненты данной модели входят:

- *Пункт принудительного применения политики (PEP)*: Устройство сети или системы безопасности, которое принимает политику (правила конфигурации) из пункта выбора политики и принудительно применяет ее в отношении сетевого потока, проходящего через это устройство. Это принуждение выгодно использует сетевые и вспомогательные для сети механизмы безопасности должным образом.
- *Пункт выбора политики (PDP)*: Пункты PDP или абстрактные сетевые стратегии сервера политики в сообщениях управления конкретными устройствами, которые затем следуют к пунктам проведения политики. Эти серверы политики часто являются автономными системами, которые управляют всеми коммутаторами и маршрутизаторами внутри конкретного административного домена; они сообщаются с этими устройствами, используя протокол управления (например, COPS, набор команд SNMP, протокол Telnet или, относящийся к конкретному устройству, интерфейс командной строки CLI).
- *Общая открытая служба политики (COPS)*: Служба COPS это простой протокол запроса и отклика, на основе TCP с изменяемым состоянием, который может использоваться для изменения информации политики, между пунктом выбора политики (PDP) и пунктами проведения политики своих клиентов (PEPs). Она обусловлена в [b-IETF RFC 2748]. Служба COPS всегда опирается на PEP для установления связей с первичным (и вторичным PDP, если первичный недосягаем). С другой стороны, может использоваться прокси-устройство COPS, которое переводит сообщения COPS, первоначально созданные в сервере политики, в команды протокола SNMP или интерфейса CLI, понятные для сетевых устройств и устройств безопасности.

  Протокол COPS поддерживает две разные модели расширения для управления политикой: динамичную с привлечением внешних исполнителей (аутсорсинг) модель COPS-RSVP, обусловленную в [b-IETF RFC 2749], и модель конфигурации или инициализации COPS-PR, обусловленную в [b-IETF RFC 3084]. Расширения инициализации к протоколу COPS позволяют установку политик в PEP "впереди" с помощью PDP, позволяя, таким образом, PEP принимать решения о политике для пакетов данных, основанных на этой информации, относящейся к периоду до инициализации. Дальнейшая связь между PDP и PEP необходима для поддержания инициализированных политик в репозитарии данных (т. е. каталоге) синхронных с теми, которые были отправлены в PEP.
- *Репозитарий политики*: Сетевой каталог является репозитарием для всей информации о политике; в нем описаны пользователи сети, приложения, компьютеры и услуги (т. е. объекты и атрибуты), и взаимосвязи между этими объектами. Существует тесная интеграция между адресом IP и конечным пользователем (через протокол динамического конфигурирования хоста DHCP и доменную систему имен DNS). Каталог обычно реализуется в специализированной машине баз данных. Облегченный протокол доступа к сетевым каталогом является тем механизмом, который серверы политик используют для доступа к каталогу.

Репозитарий политик используется для хранения довольно статичной информации о сетях (например, конфигурации устройств), в то время как серверы политик хранят более динамичную информацию о состоянии сетей (например, распределение ширины полосы или информацию об установленных соединениях). Сервер политики извлекает информацию о политике из каталога и развертывает ее к соответствующим сетевым элементам.

Не существует установленных стандартов для описания структуры базы данных такого каталога, т. е. каким образом объекты и их атрибуты определены и представлены. Нужна обычная схема каталога, если множество приложений поставщиков оборудования должны совместно использовать одну и ту же информацию каталогов; например, всем поставщикам оборудования нужен обычный способ для интерпретации и хранения информации о конфигурации о маршрутизаторах. Появление в ближайшем будущем стандарта сети, поддерживающего службу каталога (DEN), который в настоящее время находится в стадии разработки в DMTF (Рабочая группа по управлению настольными системами), отвечает этим требованиям. DEN включает в себя информационную модель, которая предоставляет обобщение профилей и политик, устройств, протоколов и услуг. Он предоставляет единообразную модель для объединения пользователей, приложений, сетевых услуг и расширяемую структуру, ориентированную на обслуживание.

- *Облегченный протокол доступа к сетевым каталогам* (LDAP версия 3) обусловлен в [b-RFC 3377]: LDAP является протоколом клиент-сервер для организации доступа к услуге каталога. Информационная модель LDAP основана на элементе, в котором заключается информация о каком-то объекте (например, о субъекте), и он состоит из атрибутов, у которых есть тип и одно или более значений. У каждого атрибута есть синтаксис, который определяет, какие виды значений разрешены в данном атрибуте и как эти значения себя ведут во время работы каталога.
- *Пульт управления политикой*: Люди взаимодействуют с системой управления политикой посредством пульта управления, обычно посредством набора на персональном компьютере или на рабочей станции. С другой стороны, может использоваться веб-браузер для предоставления доступа для руководителя фактически с любого места, с соблюдением политики безопасности объект-уровень, для ограничения, политики которых могут быть изменены конкретной личностью. Именно посредством пульта управления в каталоге создаются экземпляры политики. Пульт предоставляет интерфейс для графического пользователя и инструменты, необходимые для руководителей, чтобы определить сетевые политики в качестве бизнес-правил. Он также может дать доступ оператору к конфигурациям безопасности нижнего уровня в индивидуальных коммутаторах и маршрутизаторах.

Элементы эталонной модели управления политикой взаимодействуют для доставки управления политикой замкнутого шлейфа. В нее входит конфигурация оконечных устройств, принудительное проведение политик в сетях и проверка функционирования сетей с точки зрения приложения конечного пользователя. Принудительное проведение политик в сети включает в себя элементы управления входом приложений или пользователей, конкурирующих за доступ к ресурсам сети. Управление политикой может идти по пути некоторого упрощения среды управления конфигурацией внутри предприятий, сводя к минимуму возможности ошибок со стороны человеческого фактора.

II.5.2 Усиление защиты сервера ОС

Усиление защиты операционных систем (ОС) является ключевым элементом в организации безопасности информационных систем внутри уровня защиты приложения. В типовом предприятии может быть множество разных операционных систем для различных приложений в области данных (включая управление сетью), а также для серверов приложений, поддерживающих IP-телефонию и интенсивные приложения связи. Довольно часто можно найти многочисленные версии одной и той же разновидности ОС, развернутой в инфраструктуре IT, что делает задачу безопасности даже более сложной.

Самая распространенная операционная система в области данных также используется в значительной степени для серверов приложений, поддерживающих IP-телефонию и интенсивные приложения связи. Поставщики оборудования предлагают усиленные версии таких систем с готовым к использованию программным обеспечением безопасности для таких функций, как антивирусная защита, обнаружение вторжения и аудиты регистрационных записей. Усиление ОС начинается с требований избегать клонирования (изготовления точных копий) сервера и требований к надежности среды, откуда происходит скачивание операционной системы, и исходит из этого. Для операционных систем, в которых отсутствуют конкретные указания для усиления, поставщику ОС надо посоветовать приобретать самые последние модели и процедуры усиления ОС.

Дополнение III

Пример обеспечения безопасности сети

(Настоящее Дополнение не является неотъемлемой частью настоящей Рекомендации)

В настоящем Дополнении предоставлены примеры различных аспектов организации защиты для организации или большого предприятия, с использованием тех методов, которые обсуждались в данной Рекомендации.

Конкретно, принципы построения решений многоуровневой безопасности для организации безопасности на территории предприятия, включая шлюзы к интернет, информационный центр, удаленный офис, удаленный доступ и IP-телефония. Методы, которые обсуждаются в данной Рекомендации, используются для иллюстрации того, что безопасность для предприятия не умещается в одну модель, подходящую на все случаи. В таблице III.1 предоставлен пример соответствующих необходимых аспектов безопасности. В первом примере представлено небольшое предприятие, на котором используется ограниченное число физических частных линий между офисами, обеспечивается ограниченный удаленный доступ для служащих, а соединение с веб-сетью осуществляется через информационный интернет-центр поставщика услуг (который отвечает за создание безопасной среды). Во втором примере представлено открытое предприятие, деловая модель которого позволяет партнеру, поставщику и клиенту использовать интернет в целях ограниченного доступа к приложениям, управляемым предприятием. В примере второго предприятия внутренние и внешние пользователи осуществляют доступ к сети предприятия из дома, удаленных офисов или других сетей с использованием проводных или мобильных устройств.

Таблица III.1 – Руководство в отношении подходящих аспектов безопасности предприятия

Область сети	Пример предприятия 1	Пример предприятия 2
Организация безопасности на территории предприятия	Да	Да, представляя самые строгие требования к безопасности
Организация безопасности удаленного офиса	Опция шифрования по виртуальным или физическим частным линиям	Да, включая доступ к интернет удаленного офиса
Организация безопасности удаленного доступа	Да, но только для частного коммутируемого доступа	Да, включая партнеров и потребителей
Организация безопасности информационного центра	Да, для внутренних информационных центров	Да, включая информационные центры интернет
Организация безопасности IP-телефонии	Да	Да, выгодно используя VPN

III.1 Организация защиты удаленного доступа

Методы удаленного доступа позволяют предприятию или организации эффективно использовать людей и ресурсы, которые расположены почти повсеместно. Однако у этих методов также имеется потенциал представления проблем безопасности для этого предприятия. Отдельные служащие предприятия, которые находятся в поездке или работают из дома представляют большинство пользователей с удаленным доступом, но в эту категорию также входят маленькие офисы, которые по требованию подключаются к сети предприятия. Основные трудности возникают из-за безопасности сети и безопасного управления доступом. Безопасность сетевого управления реализуется в центральном узле. Безопасность приложения существенна, поскольку удаленное устройство нужно защитить посредством программного обеспечения антивирусного сканирования и личными брандмауэрами.

Одной из значительных угроз для удаленных пользователей является кража оборудования пользователя (UE). Кражу оборудования удаленного пользователя нельзя допустить, так как это приведет к вторжению в другие области сети предприятия или к доступу к информации, которая может храниться в этой системе. С другой стороны, подвижные пользователи хотят носить с собой свои устройства или терминалы для осуществления доступа к сети из любого места. Это обусловливает необходимость шифрования важной информации, хранимой в системах и

использующейся для удаленного доступа, предпочтительно с использованием системы, которая эффективно интегрируется в обычное использование приложений. Системы шифрования, доступные в настоящее время, дают возможность пользователю работать в штатном режиме, не требуя ручного или индивидуального шифрования/дешифрования файлов. Например, вся система файлов или "папки" могут храниться в зашифрованном виде с дешифрованием, объединенным со штатным доступом к системе файлов. Другая форма угрозы может возникнуть, если пользователь удаленного доступа работает на беспроводных LAN, возможно дома или в гостинице. В этом случае важно наличие современного личного брандмауэра и антивирусной программы.

Самой распространенной формой удаленного доступа для передачи данных является коммутируемый доступ или напрямую к предприятию, или к поставщику услуг интернета (ISP), и прямой доступ, основанный на интернет-технологиях, использующий цифровую абонентскую линию (DSL), кабельные модемы, местный Ethernet (например, в гостинице), и беспроводные сети LAN (например, в аэропортах). Беспроводные службы общего пользования для передачи данных, поддерживающие доступ к интернет, также являются быстрорастущей областью, которая предоставляет все более возрастающую подвижность для портативных компьютеров и карманных компьютеров. Растущая готовность и выгоды от интернет требуют его быстрого роста для сетей VPN удаленного доступа, используя как коммутируемый, так и прямой доступ. На рисунке III.1 дан пример организации безопасности удаленного доступа.

Рисунок III.1 – Организация защиты удаленного доступа

Используя методы, представленные в данной Рекомендации, нужно предпринять следующие шаги, для того чтобы сделать удаленный доступ безопасным:

1) *Коммутируемый доступ к централизованному узлу предприятия*

Пользователь, имеющий коммутируемый удаленный доступ, устанавливает телефонный вызов от модема, прикрепленного к его компьютерной системе, к модемному пулу (также называемому коммутатором удаленного доступа), расположенному в центральном или региональном узле предприятия. Системы коммутируемого доступа должны быть конфигурированы для использования безопасной системы управления доступом, которая предоставляет аутентификацию и санкционирование доступа, как описано ранее. Прямой коммутируемый доступ, который широко использовался в 1980-е годы и начале 1990-х годов, быстро заменяется сетями VPN удаленного доступа на основе интернет-технологий.

2) *Сети VPN удаленного доступа*

Удаленный доступ на основе интернет-технологий предоставляет чрезвычайную гибкость и широкую полосу пропускания. Существует два подхода: сети VPN на основе IPSec, использующие клиентов удаленного доступа VPN или сети VPN на основе возможностей SSL (Протокола защищенных гнезд) браузера пользователей.

3) *Сети VPN на основе IPSec*

IPSec является подходом сетевого уровня, который может использоваться по всем приложениям (например, если установлено соединение VPN на основе IPSec, то

пользователь может добираться к электронной почте, обслуживающим себя самостоятельно приложениям и бродить по внутренней сети, и приложениям с авторизованным доступом. Клиенту IPSec необходимо осуществить загрузку в UE, для того чтобы его можно было использовать для удаленного доступа. Клиенты также будут доступны для карманных компьютеров. В это UE должно быть также загружено антивирусное программное обеспечение.

Неважно, основан ли на коммутируемом доступе к ISP POP или на проводном или беспроводном прямом доступе, клиент VPN аутентифицирует пользователя, проверяет целостность собственной компьютерной системы пользователя и устанавливает безопасную линию связи (или туннель) к предприятию. Клиент VPN предоставляет возможности (например, брандмауэры) для того, чтобы гарантировать тот факт, что сама удаленная систем безопасна, особенно во время установления соединения с предприятием. В фазе установления сеанса используется зашифрованный и аутентифицированный поток к предприятию.

Предполагается, что сети VPN удаленного доступа должны быть в состоянии обнаружить и, если возможно, обойти обычные препятствия в интернет, такие как NAT и исходящие брандмауэры (например, для установления связи с сетью предприятия из другой, защищенной брандмауэрами, сети), или, по крайней мере, снабдить удаленного пользователя информацией о природе возникших препятствий.

На границах предприятия, соединения удаленного доступа от интернет обрабатываются с помощью системы шлюзов IPSec. На границе предприятия должна быть предоставлена защита от единичного сбоя с помощью применения множества шлюзов с множеством трактов, ведущих к интернет. В зависимости от области применения предприятия, также рекомендуется географическое разделение шлюзов. Шлюз должен предоставить множество функций для поддержания эффективного удаленного доступа в масштабах предприятия. В рекомендуемые функции входит: простая конфигурация клиента, возможность прокладывания соединений через внутреннюю сеть предприятия в противоположность завершению сеанса, и возможность предоставления функциональных возможностей брандмауэров с изменяемым состоянием для того, чтобы избежать потребности в отдельном брандмауэре. Более того, рекомендуется, чтобы в шлюзе применялись разнообразные механизмы аутентификации, такие как RADIUS, PKI и LDAP для дополнительной гибкости в выборе уровня аутентификации пользователя. Шлюз должен давать возможность предприятию проявлять гибкость, для объединения других схем, таких как RADIUS, ID/пароли пользователей на основе каталогов, или даже аутентификацию с использованием смарт или маркер-карт на портативных компьютерах пользователей, что возможно уже используется. Полезной является поддержка для L2TP и PPTP.

III.2 Организация защиты IP-телефонии

Организации и предприятия начинают развертывать решения по IP-телефонии, ставя цель получения выгоды от конвергенции в LAN и WAN, и от конвергированных приложений. Каждая система VoIP является программно/аппаратным решением, составленным из набора четырех логических функций:

- IP-телефоны и клиенты программного обеспечения ПК.
- Серверы соединений (также называемые серверами управления или привратниками).
- Шлюзы среды, предоставляющие гибкий доступ к сети (например, через традиционные PBX (телефонные системы для частного пользования) и коммутируемую телефонную сеть общего пользования (КТСОП), и беспроводную сеть общего пользования и далее).
- Серверы приложений (например, комплексная работа с сообщениями, конференц-связью и объединенными приложениями с задействованным протоколом SIP).

Эти функции, так же как связанные коммуникационные серверы приложений, такие как те, которые поддерживают Центр телефонного обслуживания и комплексную работу с сообщениями, распределены по телефонной сети или сети IP бизнес-класса, которая предоставляет необходимый уровень надежности, качества речи и управления перегрузкой. Предоставляется увеличенная досягаемость и подвижность по беспроводным сетям LAN и по интернет посредством сетей IP VPN.

На рисунке III.2 изображен типичный подход организации к организации защиты IP-телефонии.

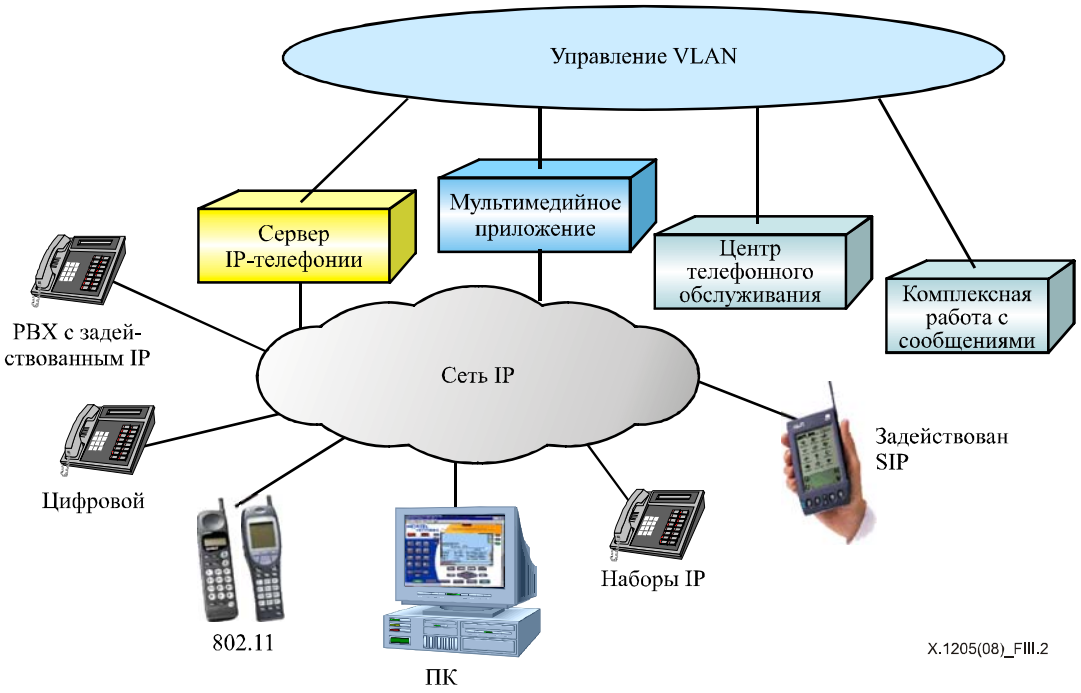

Рисунок III.2 – Организация защиты IP-телефонии

IP-телефония является приложением, которое работает в сетях IP и использует с выгодой для себя функциональные возможности безопасности, предоставляемые сетью. В отличие от большинства информационных приложений, IP-телефония чувствительна к фактору времени и это качество является важным для ведения дел. Точно так же, как и другие информационные приложения, системы IP-телефонии могут подвергаться ряду атак. Например:

- Атаки на маршрутизатор могут привести к отрицательному влиянию, как на речевое, так и на информационное обслуживание в организации.
- Отказ в обслуживании может создать перегрузку коммуникационного сервера IP-телефонии или клиента.
- Атака "Ping of death" может нарушать операции VoIP, отправляя многочисленные пакеты информации устройствам VoIP.
- Сканирование порта может найти уязвимости в клиентах и серверах VoIP.
- В процессе анализа пакетов может происходить запись и/или перехват разговоров.
- IP подмена может исказить источник или место назначения среды или поток сигнализации.
- Вирусы, черви. Троянские кони и бомбы, синхронизируемые по времени, могут атаковать серверы и клиентов.

IP-телефония может быть рассекречена. Например, были случаи, когда хакеры захватывали клиентов IP, из-за слабости в администрировании паролей в одном случае и из-за уязвимостей, связанных с управлением XML (Расширяемый язык разметки) (см. [b-W3C XML 1.0]) в другом случае. Такие атаки могут быть основной угрозой, если управление VoIP осуществляется с самого начала через интернет, и меньшей угрозой, если IP-телефония используется строго в рамках предприятия и по туннельным связям через интернет.

Как и с любым другим приложением, нужно выполнить оценку рисков IP-телефонии для вычисления его действительной стоимости, должны быть поняты последствия потерь внутри организации и должна быть сформулирована политика безопасности. Телефония является важной бизнес-функцией и поэтому, как и сама сеть, систему телефонии в целом необходимо будет защищать от угроз безопасности и от атак.

В общем случае, от пользователи телефонии аутентифицируют себя для исходящего доступа, используя набор признаков, называемый доступ к добавочной линии путем прямого установления входящего соединения (DISA). С другой стороны, нет ничего необычного в требовании к информационным пользователям применять пользовательские идентификаторы и пароли, имеющие сложную структуру, для доступа к сетям и приложениям. Такая сложность противоречит организации защиты среды предприятия. Простота будет даже более важной с VoIP, так как ожидается прямой тональный вызов. Излишне говорить, что любые механизмы безопасности VoIP не могут затруднять необходимую возможность осуществления соединений и качество речи.

В основные руководящие указания в организации защиты IP-телефонии входят:

1) Решения IP-телефонии предприятия работают внутри границ этого предприятия, взаимодействуя с сетью общего пользования через подключения с коммутацией каналов.

2) Системы IP-телефонии предприятия рассчитывают на то, что инфраструктура налаживания IP связей обеспечена из перспективы данных, и должна быть сконструирована и разработана таким образом, чтобы отвечать требованиям запаздывания и надежности телефонии.

3) Коммуникационные серверы IP-телефонии предприятия являются важными для бизнеса и физически безопасными и защищенными от внутренних и внешних атак.

4) Обеспечивается безопасная аутентификация клиентов VoIP.

5) Шифрование речи требуется только тогда, когда есть пересечение с совместно используемой средой LAN или через интернет.

6) Принимается целостный подход к вопросу безопасности по всей телефонной среде, включая клиентов VoIP и серверы, серверы приложений (например, для комплексной работы с сообщениями и центрами телефонного обслуживания) и традиционные системы PBX.

Для решений об организации защиты IP-телефонии требуется скоординированный подход во всех уровнях сетей. Управление политикой и безопасное управление доступом гарантирует аутентификацию пользователя и контролирует свойство IP-телефонии и возможности вызова. Должны использоваться методы безопасного управления для защиты устройств VoIP, таких как коммуникационные серверы и шлюзы среды. Механизмы безопасности, которые были введены туда, где размещаются данные, могут использоваться с выгодой для VoIP, например, используя IPSec для безопасного удаленного доступа, подключаемость ветвей и для доступа к беспроводной LAN. Дополнительной безопасности посредством управления политикой можно добиться, если добавить проверку VoIP с изменяемым состоянием для брандмауэров и сетевой функциональной возможности перевода адресов. Безопасности приложений можно добиться разными способами, включая усиление защиты ОС и установленную на UE защиту от вирусов.

III.2.1 Организация защиты приложений и коммуникационных серверов IP-телефонии

Центральным узлом системы IP-телефонии является коммуникационный сервер, который может быть автономным сервером или объединенным с администратором, передающим бизнес данные, PBX с задействованным IP. Равноценную значимость имеют серверы приложений, обслуживающие центр телефонного обслуживания, мультимедийные приложения, комплексную работу с сообщениями и самообслуживающуюся интерактивную систему речевых откликов. Организация защиты этих серверов начинается с усиления операционных систем, как было описано.

III.2.2 Организация защиты клиентов VoIP

Решения VoIP поддерживают широкий диапазон клиентов и конфигураций доступа, включая проводные и беспроводные телефоны IP и программных клиентов на основе ПК. Когда они подключены к сети IP, то они уязвимы для атак.

Существует ряд различных протоколов телефонной сигнализации, таких как SIP. Поток сигнальных сообщений обычно использует TCP на транспортном уровне. В будущем способность обезопасить поток сигнальных сообщений в клиенте VoIP станет общедоступной. В системах IP-телефонии речевой сигнал пакетируется с использованием стандарта, такого как [b-ITU-T G.729] (при 8 кбит/с) и алгоритма обнаружения речевой активности, и использует протокол реального времени (RTP), протокол с UDP (Протокол пользовательских данных) на транспортном уровне.

Есть существенные различия в способах минимизации рисков для IP-телефонов и для программных клиентов телефонии на основе ПК. IP-телефоны это сделанные на заказ приборы, предназначенные исключительно для телефонии. В самом телефоне нет памяти или каких-либо активов, которые нужно защищать (кроме того, что он присутствует в сети, как надежное устройство). Идентификация вызывающего лица и сам вызов являются единственными активами, которые нужно защищать. Эти телефонные устройства чаще всего используют протокол пользователя клиент-терминал, который рассчитывает на коммуникационный сервер для обеспечения функций/возможностей и безопасности. Такой подход отличается от реализаций, в которых рассчитывают на XML в наборе VoIP для функциональной работы, которая может быть уязвимым местом.

Программные клиенты VoIP находятся в оборудовании пользователей вместе с другими приложениями и активами, и работающими операционными системами, к которым открыт широкий доступ. Успешная атака может дорого обойтись, так как в ПК существует много ценных активов, включая приложения и бизнес, финансовые и личные данные. Общей практикой является использование одного или нескольких приложений безопасности, написанных для платформ ПК, предоставляющих личные брандмауэры, программы обнаружения вирусов и клиентов IP VPN. Для программных клиентов VoIP можно использовать те же механизмы, которые применимы к данным.

III.2.3 Организация защиты VoIP в коммутационных шкафах и по территории предприятия

Существует два способа коммутации IP устройств в сеть на территории предприятия: совместно используемая среда и выделенный коммутируемый Ethernet. Общее промышленное направление это выделенный коммутируемый Ethernet, такой выбор диктуется возрастающим потоком данных и требованиями к легкости в управлении. К тому же, безопасность и легкость в управлении также ведут к развертыванию сетей VLAN (см. [b-ISO/IEC 18028-5]) в сетях предприятий. Беспроводные сети LAN предлагают третью альтернативу, которая бурно развивается в таких средах, как образование и здравоохранение.

С введением IP-телефонии настоятельно рекомендуется, чтобы программные клиенты VoIP и приложения VoIP подключались к коммутируемым средам Ethernet прямо на рабочем столе. Это условие отвечает следующим требованиям:

– Изменение запаздывания VoIP сводится к минимуму с помощью исключения операции CDMA (многостанционный доступ с кодовым разделением каналов) операции Ethernet с совместно используемой средой;

– Безопасность VoIP возрастает из-за недопущения потенциально возможного перехвата другими рабочими столами вызовов VoIP.

Вдобавок, предприятие может сделать выбор в пользу логической группы VoIP телефонов в своих собственных сетях VLAN, для того чтобы упростить управление.

IP-телефония может существенно поднять производительность пользователей, если использовать беспроводные сети LAN внутри предприятия, расширяя телефонные функций/возможности от рабочего стола до, например, конференц-зала или до классной комнаты. Из-за неблагоприятной природы этих сетей WLAN, рекомендуется архитектура с защитой, как сигнальных, так и речевых плоскостей по всему беспроводному сегменту. Эту задачу можно выполнить с помощью конфигурирования программных клиентов, находящихся вместе с клиентом IP VPN в портативном компьютере. С другой стороны, шифрование и аутентификация встроена в некоторые WLAN IP-телефоны. Оба подхода предоставляют сильную аутентификацию пользователя и шифрование, необходимые для сред WLAN.

III.2.4 Организация защиты ветвей для IP

Существует несколько подходов к поддержке решений удаленного офиса и VoIP ветвей. Сюда входят телефоны VoIP и программные клиенты, поддерживаемые коробочными решениями для офиса. Другие подходы используют распределенную природу VoIP с полной выгодой, развертывая клиентов от централизованного сервера. Во всех этих случаях рекомендуется, чтобы поток VoIP в этой ветви безопасно проходил по IP VPN, установленной для данных.

III.2.5 Организация защиты удаленного доступа для IP-телефонии

IP-телефония может значительно повысить производительность удаленных пользователей независимо от того, работают ли они дома, в гостинице или в дороге; во всех случаях телефонные функции/возможности простираются от рабочего стола в сторону удаленного места. Для часто передвигающихся служащих программные клиенты VoIP находились бы вместе с клиентом IP VPN в портативном компьютере. Такая же конфигурация могла бы применяться для использования преимущества точек доступа WLAN в гостиницах, аэропортах и комплексах для конференций. VoIP телефоны могли бы предоставить богатый выбор функций связи для "надомных работников" и агентов в комплексах для конференций с безопасностью, предоставляемой с помощью домашнего офиса IP VPN.

III.2.6 Безопасность управления сетями для IP-телефонии

С точки зрения перспектив управления, физически выделенный порт Ethernet должен быть конфигурирован. Это должно быть частью управления VLAN со всем потоком данных, не относящихся к управлению, заблокированном на уровне маршрутизатора посредством перечней доступа и безопасности периметра. Доступ, не входящий в состав сети, для поставщиков, системные интеграторы и/или реселлеры VAR (реселлер, добавляющий ресурсы) могут предоставляться посредством сетей IP VPN. Неиспользуемые порты (например, для доступа пультов или удаленных модемов) должны быть отключены. Только программное обеспечение разрешенных приложений должно работать на этих серверах. Должна использоваться многоуровневая безопасность с различными уровнями привилегий (вести текущее наблюдение, конфигурировать, контролировать) для освидетельствованного рабочего персонала. Пароли пользователей надежно хранятся, а форматирование паролей и управление изменениями строго контролируется. Поток управления (такой, как информация о рассылке счетов) может дополнительно шифроваться даже для внутренней передачи с помощью технологии IP VPN.

III.3 Организация защиты удаленного офиса

Удаленный офис может быть любого размера, от домашнего рабочего места до крупной корпоративной территории. Хотя существует много общих элементов между "удаленным офисом" и "удаленным доступом", могут быть различия, основанные на постоянстве возможностей для двунаправленной связи между удаленным местом и остальным предприятием. Другими словами, удаленный офис это рабочее место, которое постоянно подключено к остальному предприятию и способно обмениваться сообщениями с остальным предприятием в течение рабочих часов. С другой стороны, удаленный доступ это временное подключение к предприятию, устанавливаемое по требованию пользователя(ей) с удаленным доступом.

Сеть, организованная разветвлением, является самым важным дорогостоящим транспортом оказания услуг во многих промышленных сферах, таких как банковская сфера, имеющая дело с обслуживанием мелкой клиентуры, здравоохранение и правительство. Традиционно среды разветвления сетей основаны на различных технологиях LAN и на многопротокольных маршрутизаторах, работающих в сетях с ретрансляцией кадров с резервированием с коммутацией цепей ЦСИС. Четыре основные разработки создали основные возможности для преобразования разветвления сетей: 1) конвергенция на Ethernet, как на стандарте LAN; 2) универсальное принятие IP, как протокола выбора; 3) интернет; 4) растущий перечень услуг VPN уровня 2 и 3. Однако эти разработки ввели также и ряд проблем, связанных с безопасностью, особенно для более крупных организаций и предприятий. Это изображено на рисунке III.3.

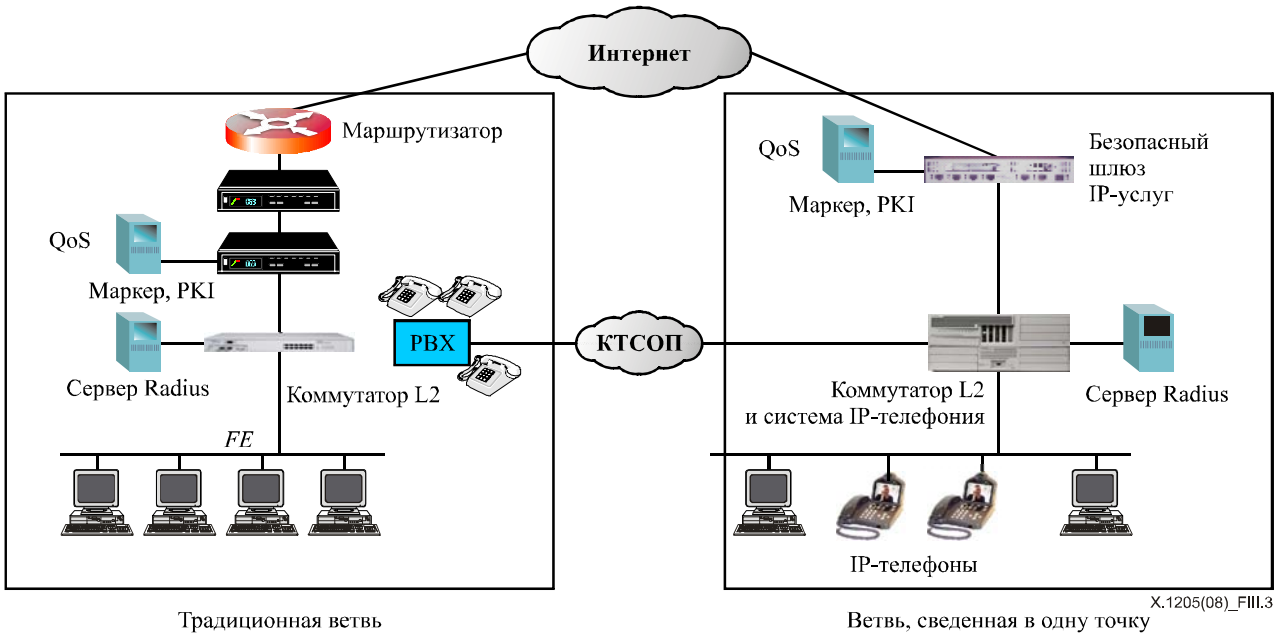

Рисунок III.3 – Организация защиты удаленного офиса

Граничные требования сети WAN на уровне ветви включают в себя маршрутизацию между сетями VLAN в определенном месте и внутри сети, управление QoS и шириной полосы, а также масштабируемая установка связи в сети WAN. Сюда входит поддержка схемы инкапсуляции в сети WAN и на любом подходящем уровне надежности. Основным требованием является эффективная в отношении затрат безопасность по интернет (и даже по ретрансляции кадров). Еще одной проблемой является управление переходом от сравнительно традиционных технологий безопасных сетей WAN к IP VPN. Некоторые предприятия хотят иметь прямой доступ к интернет из каждого удаленного офиса, активизируя требования для удаленных брандмауэров. Другие хотят высокую надежность подключаемости с динамической маршрутизацией между ветвями и магистралью предприятия, с централизованными брандмауэрами в интернет, в некоторых случаях с использованием ретрансляции кадров в качестве первичного тракта, а интернет как магистраль, или они склоняются к IP VPN в качестве первичной конфигурации. Динамическая маршрутизация используется для увеличения масштабируемости и надежности с помощью:

- автоматического изучения топологии сети;
- автоматического изучения адресов конечных пользователей на предприятии;
- автоматическое приспособление к изменениям в топологии сети.

Однако безопасность в маршрутизируемых сетях была на втором месте, а не требованием дня номер один. Например, не было эффективных способов осуществления динамической маршрутизации по VPN-зашифрованным туннелям, и управление ими было очень затруднительным.

Как правило, все вышеуказанное приводило предприятия к покупке, установке, обслуживанию и управлению многочисленными устройствами безопасности и организации сетей, что было сложным и дорогостоящим в управлении.

С продвижением в сторону использования IP VPN по всему интернет, полный набор требований к безопасности должен отвечать требованиям эффективности затрат насколько это возможно. Сюда входят функции защиты сети, такие как IP маршрутизация по безопасным туннелям, организация виртуальной частной сети (VPN) и шифрование, проверка брандмауэров с изменяемым состояние на уровне поддерживаемой сети и аутентификация удаленного офиса и служба каталогов на безопасном уровне управления доступом, все должно предоставляться в комплексе. Принуждение в управлении политикой безопасности должно входить в это решение, давая возможность предоставления каждому пользователю уникального профиля безопасности, который сохраняется за этим индивидуумом безотносительно к тому, регистрируется ли он/она со своего домашнего ПК через общедоступный интернет, или подключается по месту внутри офисной ветви. Безопасность управления сетью также

нужно расширить до удаленного офиса, без путей обхода системы защиты, которые могут рассекретить сетевую безопасность. Наконец, требуется предоставить безопасность приложений, если информационные серверы и/или IP-телефония разворачиваются в удаленном офисе.

III.4 Организация защиты WLAN

Происходит развитие возможностей для связи между штаб-квартирами, объединенными в корпорацию, филиалами компаний, удаленными служащими, консультантами и бизнес партнерами. Компании в настоящее время могут выгодно использовать новые беспроводные технологии IEEE 802.11 (см. [b-IEEE 802.11]) для ведения дел в любое время и в любом месте. Вместе с этими решениями, однако возникает необходимость централизованного и эффективного управления доступом пользователей, во время организации защиты ресурсов организации.

Сети WLAN особенно уязвимы для нарушений безопасности. Перехват в системах связи на основе стандартной LAN требует физического доступа к кабельной инфраструктуре. Беспроводная передача данных, с другой стороны, является предметом для перехвата по воздуху и оставляет сеть без защиты для вторжений со стороны любого человека, имеющего стандартную плату беспроводной LAN.

Сети WLAN расширяют корпоративную сеть с помощью использования беспроводных устройств и протокола IEEE 802.11. В число оборудования для сетей WLAN входят беспроводные сетевые интерфейсные платы (NIC) для подвижного оборудования, такого как портативные компьютеры и настольные системы; все они воспринимаются, как подвижные узлы (MU) или станции (STA). Платы NIC дают возможность переносить сетевые сигналы от соединительного устройства через промежуточное устройство, шлюз беспроводной LAN, или концентратор, известный как беспроводная точка доступа (AP), которая преобразует беспроводные сигналы в сигналы проводной линии связи в проводной сети.

Используя концентратор Ethernet или коммутатор, компании могут подключать беспроводные точки доступа LAN к проводным LAN так же просто, как если бы они подключали проводного пользователя. С помощью подключения точек доступа к коммутатору, для них гарантируется выделенная линия со скоростью 10/100 Мбит/с, таким образом предоставляется возможность всем доступным точкам доступа работать как коммутатор и нет необходимости соперничать за часть ширины полосы проводного концентратора.

Исходный стандарт [b-IEEE 802.11] является семейством технических условий, из которых IEEE 802.11a, IEEE 802.11b, IEEE 802.11g и IEEE 802.11i доступны сегодня и которые используются, основываясь на среде сетевых сигналов, при этом делается попытка найти компромисс между расстоянием и шириной полосы.

III.4.1 Вопросы безопасности WLAN

Независимо от механизмов безопасности WLAN, сигналы WLAN передаются и принимаются по воздуху посредством радиоволн, и потому у них нет физических барьеров против несанкционированного пользователя. Эти сигналы, к сожалению, являются предметом подслушивания и возможных вторжений в корпоративную сеть. Таким образом, добавление беспроводного узла к корпоративной сети влечет за собой принятие надлежащих мер предосторожности, связанных с безопасностью, и применение надлежащей практики в области безопасности для защиты всех ресурсов сети WLAN.

Уровень инфраструктуры сетей WLAN состоит из всех компонентов сети, кабелей, среды подсоединений и передачи (пространство оболочки), например точек доступа, мобильных станций, шлюзов и серверов, выполняющих роль ведущих узлов в отношении соответствующих услуг, как например RADIUS, DNS и др.

Служебный уровень включает услуги беспроводного доступа LAN и другие услуги, обеспечивающие возможность осуществления беспроводного доступа, например аутентификацию, санкционирование, учет (AAA), ключевые услуги управления и др.

Угрозы для безопасности, вводимые сетями WLAN включают в себя:

- Нарушения конфиденциальности и целостности беспроводного потока. Нападающий имеет возможность подслушивать информацию, передаваемую между подвижным компьютером и беспроводной точкой AP, и, таким образом, захватить секретную или не подлежащую разглашению информацию, не предназначенную для третьих лиц. И наоборот, у нападающего есть возможность ввести информацию в подлинное входное сообщение без ведома законных пользователей.

- Незащищенность корпоративной сети LAN. Если подвижные платформы не аутентифицированы надежным образом, то атакующий может просто подключить WLAN, используя соответствующее устройство IEEE 802.11 и став "аутентифицированной" станцией в сети WLAN, добиваясь, таким образом, доступа к корпоративной LAN.

Используя модель угроз X.800, попытки нарушения защиты можно кратко представить следующим образом:

Модель угроз X.800	Методы осуществления попыток нарушения защиты
Разрушение информации и/или других ресурсов	Проникновение через точку доступа
Искажение или изменение информации	Взлом WEP-ключей, попытка взлома типа "злоумышленник в середине"
Кража, изъятие, или потеря информации и/или других ресурсов	Проникновение через точку доступа, взлом WEP-ключей, попытка взлома через посредника, спуфинг адреса MAC, вредоносные устройства, ведение войны, захват уровня 3, специальные сети
Раскрытие информации	Проникновение через точку доступа, взлом WEP-ключей, попытка взлома через посредника, спуфинг адреса MAC, вредоносные устройства, ведение войны, захват уровня 3, специальные сети
Прерывание обслуживания	РЧ глушение, лавинная адресация данных, захват уровня 2, фиктивная точка доступа, подложный деаутенцифицированный кадр, отказ в обслуживании с помощью программы FATA-Jack

Подобно проводным сетям, сети WLAN требуют конфиденциальности, целостности и контроля доступа. Основная проблема для беспроводных сетей состоит в том, что те, кто находится снаружи, могут легко подключаться к сети WLAN, передавая и принимая информацию, независимо от того, считаются ли он вне пределов досягаемости.

Это позволяет атакующим перехватывать и вводить несанкционированные точки AP (называемые как мошеннические AP), чтобы начать атаки, такие как атака через посредника и захват сеанса, и с легкостью атаковать пользователей WLAN изнутри этой WLAN. Таким образом, нападающий может обманным способом заставить пользователя подключиться к AP атакующего, позиционируя ее, как легальный узел в сети и, вследствие этого, свободно и автоматически совместно пользоваться идентификаторами ID, паролями и другой персональной информацией пользователя.

Следующими методами можно выгодно воспользоваться для организации защиты беспроводной среды:

- сетевыми именами: идентификаторы служебного набора (SSID);
- регистрацией карты: списки контроля доступа MAC (ACL);
- шифрованием общего ключа: через использование протоколов безопасности (такие, как WPA/WPA2).

Дополнительно можно использовать следующие типы аутентификации:

- Аутентификация открытой системы: дает возможность любому, имеющему SSID точки AP, получить доступ.
- Аутентификация общего ключа: для того, чтобы получить аутентификацию пользователь имеет общий секрет.

В исходных технических условиях [b-IEEE 802.11] безопасный роуминг происходит посредством предварительной аутентификации подвижного блока (MU) к окружающим точкам AP. Между точками AP нет переадресации сообщений, так как все точки AP и блоки MU используют один и тот же общий ключ, позволяющий новой AP предполагать законность аутентификации MU. Таким образом, переадресация вызова является быстрой, но аутентификация менее надежна, потому, что кадры управления не аутентифицированы.

III.4.2 Механизмы и требования к безопасности внутри и перед беспроводной точкой доступа

Единственный способ действительно защитить открытую природу беспроводной среды это использовать шифровальные решения и подходящие меры аутентификации, которые утверждают конечного пользователя. Поток шифруется до шлюза, идентификатор которого может быть подтвержден криптографически.

Два основных требования для безопасной WLAN это безопасный поток и безопасный роуминг. Для безопасных подключений самым основным требованием является использование шифрования для потока от подвижного устройства к AP, к шлюзу за AP (например, используя IPSec шлюз), или к серверу приложений (безопасный веб-сайт). Для безопасного роуминга подвижные пользователи могут перемещаться от одной AP к другой без потери их активных сеансов и без повторной аутентификации для новой AP. Роуминг жестко ограничен по времени, так чтобы это оказало минимальное влияние на приложение пользователя. Пользователи рассчитывают и предполагают, что их полномочия соответствующим образом защищены при переходах между доменами. То это должно быть выполнено безопасным образом.

III.4.3 Улучшения безопасности для технических условий IEEE 802.11

Вышеуказанные риски для безопасности приводят к улучшениям в исходном стандарте [b-IEEE 802.11] для предоставления более эффективных средств безопасности для беспроводных сетей LAN. IEEE 802.11i вводит IEEE 802.1X (см. [b-IEEE 802.1X]) контроль доступа, динамическую смену одного или более шифровальных ключей, механизмы распределения посеансового ключа и сильные шифровальные алгоритмы. [b-IEEE 802.1X] вводит больший контроль аутентификации/доступа для точек AP посредством использования расширяемого протокола аутентификации (EAP), который является набором сообщений для обсуждения условий аутентификации и методом транспортировки аутентификации между клиентом и сервером (см. [b-IETF RFC 2716], [b-IETF RFC 3748] и [b-IETF RFC 4017]). Протокол EAP поддерживает несколько методов аутентификации, включая MD5, Протокол защиты транспортного уровня (TLS) с MD5, который является наиболее широко поддерживаемым и доступным. Независимо от выбора протокола EAP, все три IEEE 802.1X (см. [b-IEEE 802.1X]) компонента должны поддерживать один и тот же метод (см. рисунок III.4.3).

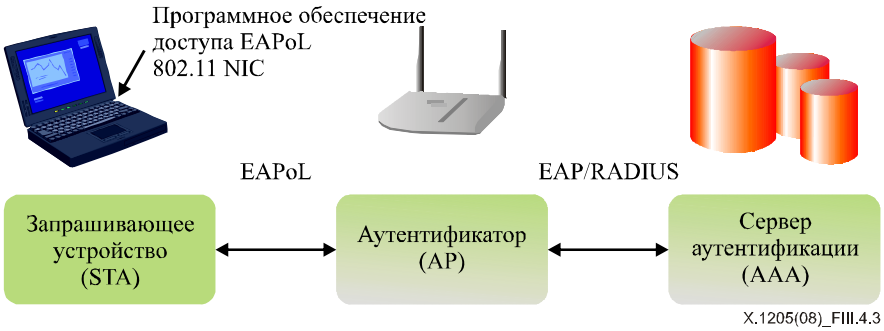

Рисунок III.4.3 – Компоненты IEEE 802.1X

Задача организации защиты роуминга IEEE 802.1X требует, чтобы пользователь все время повторно аутентифицировался в каждой новой AP, к которой он подключается в режиме роуминга. Посеансовые ключи и работа инфраструктуры открытых ключей затрудняет быструю аутентификацию. Таким образом, будут созданы некоторые трудности с этими опциями аутентификации для переадресаций вызова между точками AP во время роуминга.

Для [b-IEEE 802.1X], EAP-TTLS и PEAP предоставляют быструю повторную аутентификацию для роуминга. Это может быть достигнуто путем использования в своих интересах механизма восстановления связи, предоставляемого в протоколе квитирования TLS. Полная аутентификация не требуется, если допустить, что знание главного секрета, как явствует из способности возобновлять сеанс TLS, достаточно для аутентификации.

III.4.4 Многоуровневый подход к организации защиты беспроводных сетей LAN

Для хороших архитектур безопасности WLAN требуется многоуровневый подход, в котором применяется множество технологий, совсем как в обычных средах LAN. Окончательным решением должна быть объединенная архитектура безопасности WLAN/LAN. Везде, где это возможно, существующие механизмы безопасности LAN должны быть расширены для обслуживания WLAN.

III.4.4.1 Точка доступа

Могут использоваться ID ESS и MAC ACL, даже если они предоставляют очень слабую безопасность. Все подвижные блоки (MU) и AP, конфигурированные с одними и теми же ID ESS могут легко соединяться. Стандарт [b-IEEE 802.11] поддерживает "ретрансляцию ID ESS," что позволяет соединять MU с AP, не зная ID ESS. Безопасность может быть повышена, если эта функция отключена. В MAC ACL содержится перечень разрешенных адресов MAC и может содержаться перечень запрещенных адресов, но надо помнить о том, что это становится трудновыполнимым, если в работе участвует много компьютеров.

В настоящее время продукты AP характеризуются как предварительный стандарт и частные механизмы безопасности, в которые входят: WPA, WPA2, динамичный WEP улучшенный стандарт шифрования (AES), временный протокол целостности ключа (TKIP), и 128-битное шифрование могут легко применяться. Динамичный WEP является средством более частого изменения WEP, в предопределенном интервале. AES является новым, одобренным FIPS стандартом для замены алгоритма шифрования DES. TKIP усиливает алгоритм диспетчеризации ключа для защиты от атак возврата ключа для классических WEP. Из-за этой слабости в [b-IEEE 802.11] рекомендуется не использовать TKIP, за исключением использования в качестве вставки в программу к старому оборудованию.

ПРИМЕЧАНИЕ. – Wi-Fi защищенный доступ (WPA) возник, как промышленная инициатива, которая обуславливает усовершенствования для беспроводной локальной безопасности сети (LAN). WPA-PSK является особым режимом WPA для домашних пользователей без сервера аутентификации предприятия и предоставляет сильную защиту шифрованию. В WPA-PSK шифровальные ключи меняются автоматически (смена ключа) и проводится аутентификация между устройствами спустя указанный период времени или после передачи указанного количества пакетов. WPA-PSK использует общий ключ, который вносится как в беспроводную точку доступа внешних, так и WPA клиентов. Общий секрет может иметь длину между 8 и 63 символами. Временный протокол целостности ключа (TKIP) используется после того, как исходный общий секрет внесен в беспроводные устройства и занимается обработкой шифрования и автоматической сменой ключа. WPA разрабатывается для модернизации программного обеспечения. Поставщики беспроводного оборудования и профессионалы по вопросам безопасности ожидают, что сегодняшние WPA и WPA-PSK будут полезны еще очень долгое время. WPA определяет использование улучшенного стандарта шифрования (AES), как дополнительную необязательную замену для WEP шифрования.

III.4.4.2 Воздушное пространство

С помощью направленной антенны с большим коэффициентом усиления постороннее лицо, желающее получить несанкционированный доступ к WLAN, может добраться до WLAN с удаления в несколько миль. Было бы предпочтительно блокировать это постороннее лицо, чтобы воспрепятствовать ему в этом. Таким методом блокирования несанкционированных посторонних лиц от использования в своих интересах доступности сигнала, передающегося по открытой воздушной среде, с помощью использования направленной антенны с большим коэффициентом усиления, может быть окружение периметра корпоративных земель или сети WLAN точками AP, которые не соединены с внутренней сетью (см. рисунок III.4.4.2). Постороннее лицо блокировано от просмотра внутренней WLAN потому, что внешние точки AP работают на тех же несущих частотах, что и внутренние и, на самом деле, предлагают более высокий уровень сигнала для постороннего лица, "заглушая" внутренний сигнал для постороннего лица. Эта схема может быть улучшена с помощью подключения этих внешних точек AP к изолированной сети и добавления системы обнаружения вторжений (IDS) и программы "honeypot" для обнаружения вторжений и сбора доказательств.

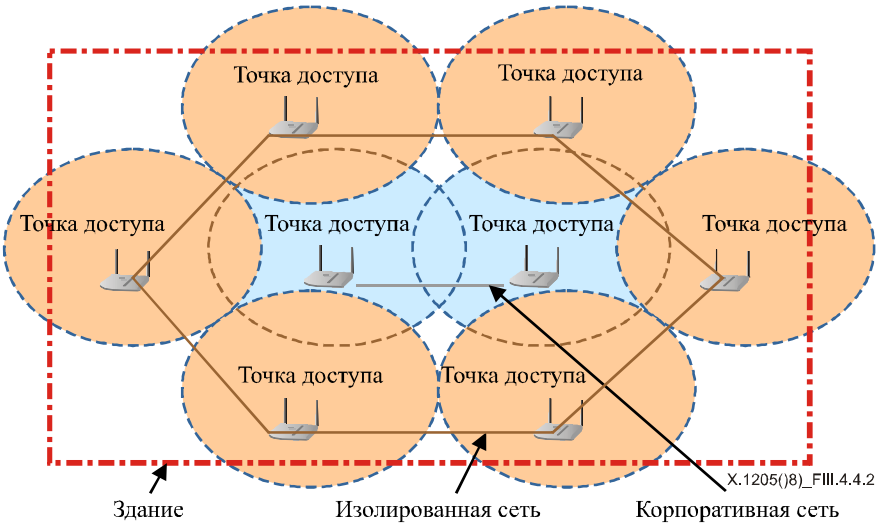

Рисунок III.4.4.2 – Защита точками AP для защиты периметра

III.4.4.3 Сегментация

Везде, где это возможно, существующие механизмы защиты LAN должны быть расширены для обслуживания WLAN. Дополнительные механизмы, такие как шифрование по сетям VPN и TLS, сегментация беспроводных сегментов по виртуальным сетям LAN (VLAN) и защита периметра через брандмауэр, являются эффективными, безотносительно к дополнительным улучшениям к [b-IEEE 802.1X]. На рисунке III.4.4.3 показаны обобщенные точки AP WLAN IEEE 802.11 с обыкновенной SSID или подсетью, подключенной к коммутатору уровня 2. Коммутатор уровня 2 может разумным образом ограничить трафик, идущий к другим точкам AP, а некоторые имеют способность VLAN. Для тех точек AP, которые находятся в другой подсети или SSID, подключение может быть выполнено через коммутатор, прокладывающий маршруты, уровня 2/3. Для этой архитектуры безопасная связь, безопасный роуминг, переадресации вызова и защита периметра воспринимаются как часть защищенной и объединенной сетевой среды WLAN/LAN.

IPSec являются испытанными и доверенными протоколами для организации защиты связи. Для сред, которые могут выгодно использовать клиентов IPSec на подвижных устройствах или у которых есть приложения с программами пользовательского интерфейса не только на основе Web, IPSec является самым подходящим средством для организации защиты связи. Основное преимущество VPN IPSec состоит в том, корпорация полностью контролирует сильную политику безопасности, так что у того, кто подключается к LAN есть все привилегии пользователя локальной LAN.

Такие же методы работают для "горячей точки", WLAN. Например, для удаленного служащего, получающего доступ гостиничного ISP (поставщика услуг интернета), этот служащий может подключится через DSL, используя клиента PPPoE и идентификатор ID/пароль пользователя, предоставляемый гостиницей для доступа ISP. Этот служащий может затем подключиться к своей корпоративной сети, используя клиента IPSec.

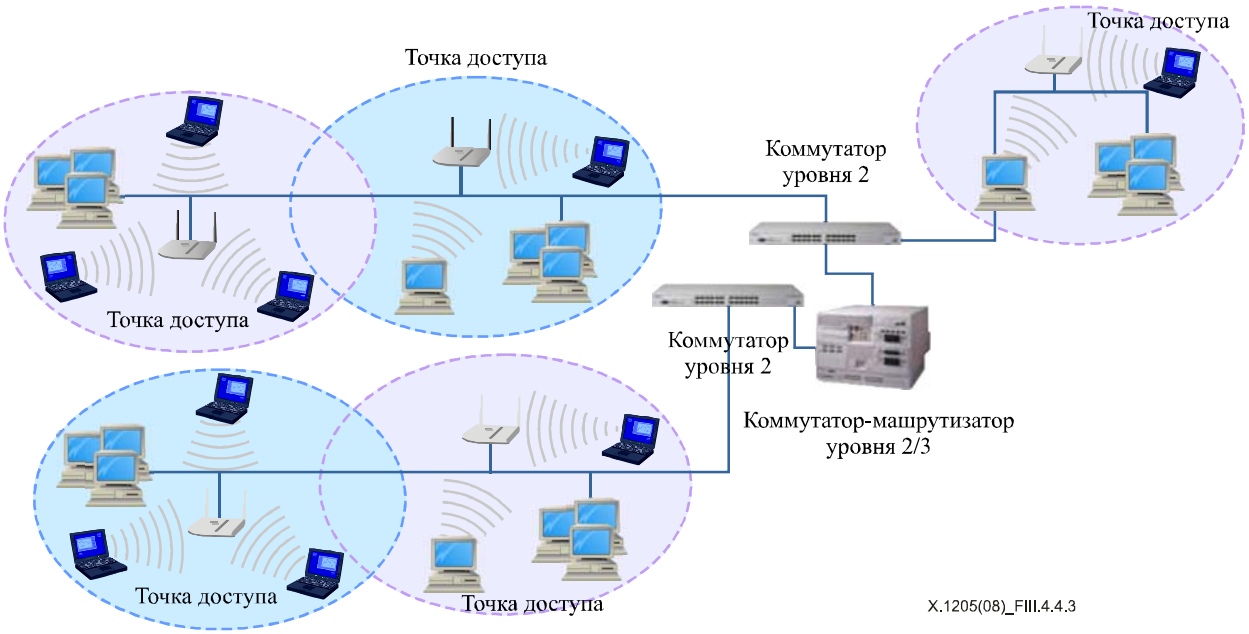

Рисунок III.4.4.3 – Обобщенные точки AP WLAN IEEE 802.11 с обыкновенным SSID

III.4.4.4 Уровень управления

Управленческие и оперативные меры противодействия тоже должны использоваться для защиты сетей WLAN, например, путем распространения политики безопасности организации на WLAN. Везде, где это возможно, существующие механизмы безопасности LAN должны быть расширены для обслуживания WLAN; иначе, новые механизмы нужно объединять с существующими механизмами. Например, выгодное использование решений IPSec дает предприятию централизованное управление пользователями WLAN, удаленными пользователями, и правилами брандмауэров, и не требует дополнительного приложения управления, если оно уже используется для доступа к сети экстранет. Поставщики оборудования добавляют осознание WLAN к механизмам, таким как обнаружение сети, сканнеры уязвимости и IDS.

III.4.4.5 Анализ протоколов доступа WLAN

Относительные сильные и слабые стороны различных протоколов Wi-Fi, рассмотренные в пунктах выше, а именно IEEE 802.11i, WPA2[2], WPA и WEP, могут быть проанализированы с использованием измерений, приведенных в Рекомендации МСЭ-Т X.805. Анализ проиллюстрирован парой измерений и может быть расширен до всех восьми измерений.

Качественные результаты по каждому измерению сведены в таблицы с использованием следующих условных обозначений:

√	удовлетворительный
P	частичный
X	Не рассматривается стандартом

Управление доступом

Исходные спецификации [b-IEEE 802.11], в том числе WEP, не включают встроенного механизма управления доступом, поэтому шлюз WLAN больше используется при развертывании WLAN в целях

[2] WPA2 и IEEE 802.11i имеют схожие функции обеспечения безопасности, однако из-за того, что WPA2 может взаимодействовать с менее защищенным WPA, слабые стороны WPA отражаются на безопасности WPA2.

управления доступом. На основании этого предположения управление доступом для предоставления услуги WLAN конечным пользователям было оценено как частично достаточное.

[b-IEEE 802.1X] – это механизм управления доступом конечного пользователя при использовании услуги Wi-Fi для IEEE 802.11i, WPA и WPA2.

Таблица III.2 – Охват в отношении измерения управления доступом

Измерение безопасности управления доступом								
Плоскости безопасности	**Уровни обеспечения безопасности**							
	Инфраструктура				**Услуги**			
	IEEE 802.11i	**WPA2**	**WPA**	**WEP**	**IEEE 802.11i**	**WPA2**	**WPA**	**WEP**
Конечный пользователь	√	√	√	X	√	√	√	P
Контроль	√	X	X	X	√	√	√	X
Управление	X	X	X	X	X	X	X	X

Аутентификация

В IEEE 802.11i, WPA2 и WPA для аутентификации используется IEEE 802.1X/EAP. В отличие от этого, в WEP применяется "открытая" аутентификация или аутентификация с "общим секретом", в которой для шифрования используется один и тот же статический ключ. Таким образом, аутентификация WEP оценивается как "частичная". Аутентификация в других стандартах может иметь ту же оценку, если для [b-IEEE 802.1X] выбран слабый протокол EAP, например MD5.

Аутентификация информации управления по точкам доступа и другим сетевым элементам (для обеспечения роуминга) рассматривается только в IEEE 802.11i. В точках доступа, работающих в других стандартах, обычно используются фирменные механизмы обмена информацией, а вопросы роуминга и проверки безопасности таких реализаций выходят за рамки сферы применения данной рекомендации.

Таблица III.3 – Охват в отношении измерения аутентификации

Измерение безопасности аутентификации								
Плоскости безопасности	**Уровни безопасности**							
	Инфраструктура				**Услуги**			
	IEEE 802.11i	**WPA2**	**WPA**	**WEP**	**IEEE 802.11i**	**WPA2**	**WPA**	**WEP**
Конечный пользователь	√	√	√	P	√	√	√	P
Контроль	√	X	X	X	√	√	√	X
Управление	X	X	X	X	X	X	X	X

Готовность

Попытки нарушения безопасности типа отказа в обслуживании, например РЧ глушение, лавинная адресация данных и захват сеанса уровня 2, являются попытками нарушения готовности. Ни один из стандартов обеспечения безопасности WLAN не может предотвратить попытки нарушения защиты на физическом уровне, просто потому что они действуют на уровне 2 и выше. Аналогичным образом, ни в одном из этих стандартов не может рассматриваться отказ AP.

Таблица III.4 – Охват в отношении измерения готовности

Измерение безопасности в отношении готовности								
Плоскости безопасности	**Уровни безопасности**							
	Инфраструктура				**Услуги**			
	IEEE 802.11i	**WPA2**	**WPA**	**WEP**	**IEEE 802.11i**	**WPA2**	**WPA**	**WEP**
Конечный пользователь	P	P	P	X	P	P	P	X
Контроль	P	P	P	X	P	P	P	X
Управление	X	X	X	X	X	X	X	X

Очевидно, что на основе IEEE 802.11i или WPA2 можно создавать, внедрить и обслуживать относительно безопасные сети WLAN. Однако просто внедрение этих стандартов не обеспечит сквозной безопасности сетей WLAN. Как показано в этом тематическом исследовании, измерение готовности не рассматривается.

Библиография

[b-ITU-T G.729] Recommendation ITU-T G.729 (2007), *Coding of speech at 8 kbit/s using conjugate-structure algebraic-code-excited linear prediction (CS-ACELP)*.

[b-ITU-T X.509] Рекомендация МСЭ-Т X.509 (2005 г.), *Информационные технологии – Взаимосвязь открытых систем – Справочник: Структуры сертификатов открытых ключей и атрибутов*.

[b-ITU-T Y.2201] Рекомендация МСЭ-Т Y.2201 (2007 г.), *Требования к сетям последующих поколений версии 1*.

[b-IETF RFC 854] IETF RFC 854 (1983), *TELNET Protocol Specification* <http://www.ietf.org/rfc/rfc0854.txt?number=854>.

[b-IETF RFC 959] IETF RFC 959 (1985), *File Transfer Protocol (FTP)* <http://www.ietf.org/rfc/rfc0959.txt?number=959>.

[b-IETF RFC 1321] IETF RFC 1321 (1992), *The MD5 Message-Digest Algorithm* <http://www.ietf.org/rfc/rfc1321.txt?number=1321>.

[b-IETF RFC 1510] IETF RFC 1510 (1993), *The Kerberos Network Authentication Service (V5)* <http://www.ietf.org/rfc/rfc1510.txt?number=1510>.

[b-IETF RFC 1661] IETF RFC 1661 (1994), *The Point-to-Point Protocol (PPP)* <http://www.ietf.org/rfc/rfc1661.txt?number=1661>.

[b-IETF RFC 1991] IETF RFC 1991 (1996), *PGP Message Exchange Formats* <http://www.ietf.org/rfc/rfc1991.txt?number=1991>.

[b-IETF RFC 2104] IETF RFC 2104 (1997), *HMAC: Keyed-Hashing for Message Authentication* <http://www.ietf.org/rfc/rfc2104.txt?number=2104>.

[b-IETF RFC 2196] IETF RFC 2196 (1997), *Site Security Handbook* <http://www.ietf.org/rfc/rfc2196.txt?number=2196>.

[b-IETF RFC 2311] IETF RFC 2311 (1998), *S/MIME Version 2 Message Specification* <http://www.ietf.org/rfc/rfc2311.txt?number=2311>.

[b-IETF RFC 2411] IETF RFC 2411 (1998), *IP Security Document Roadmap* <http://www.ietf.org/rfc/rfc2411.txt?number=2411>.

[b-IETF RFC 2427] IETF RFC 2427 (1998), *Multiprotocol Interconnect over Frame Relay* <http://www.ietf.org/rfc/rfc2427.txt?number=2427>.

[b-IETF RFC 2459] IETF RFC 2459 (1999), *Internet X.509 Public Key Infrastructure Certificate and CRL Profile* <http://www.ietf.org/rfc/rfc2459.txt?number=2459>.

[b-IETF RFC 2510] IETF RFC 2510 (1999), *Internet X.509 Public Key Infrastructure Certificate Management Protocols* <http://www.ietf.org/rfc/rfc2510.txt?number=2510>.

[b-IETF RFC 2616] IETF RFC 2616 (1999), *Hypertext Transfer Protocol – HTTP/1.1* <http://www.ietf.org/rfc/rfc2616.txt?number=2616>.

[b-IETF RFC 2631] IETF RFC 2631 (1999), *Diffie-Hellman Key Agreement Method* <http://www.ietf.org/rfc/rfc2631.txt?number=2631>.

[b-IETF RFC 2661] IETF RFC 2661 (1999), *Layer Two Tunnelling Protocol "L2TP"* <http://www.ietf.org/rfc/rfc2661.txt?number=2661>.

[b-IETF RFC 2716] IETF RFC 2716 (1999), *PPP EAP TLS Authentication Protocol* <http://www.ietf.org/rfc/rfc2716.txt?number=2716>.

[b-IETF RFC 2748] IETF RFC 2748 (2000), *The COPS (Common Open Policy Service) Protocol* <http://www.ietf.org/rfc/rfc2748.txt?number=2748>.

[b-IETF RFC 2749] IETF RFC 2749 (2000), *COPS usage for RSVP* <http://www.ietf.org/rfc/rfc2749.txt?number=2749>.

[b-IETF RFC 2753] IETF RFC 2753 (2000), *A Framework for Policy-based Admission Control* <http://www.ietf.org/rfc/rfc2753.txt?number=2753>.

[b-IETF RFC 2828] IETF RFC 2828 (2000), *Internet Security Glossary* <http://www.ietf.org/rfc/rfc2828.txt?number=2828>.

[b-IETF RFC 2865] IETF RFC 2865 (2000), *Remote Authentication Dial In User Service (RADIUS)* <http://www.ietf.org/rfc/rfc2865.txt?number=2865>.

[b-IETF RFC 2869] IETF RFC 2869 (2000), *RADIUS Extensions* <http://www.ietf.org/rfc/rfc2869.txt?number=2869>.

[b-IETF RFC 3031] IETF RFC 3031 (2001), *Multiprotocol Label Switching Architecture* <http://www.ietf.org/rfc/rfc3031.txt?number=3031>.

[b-IETF RFC 3084] IETF RFC 3084 (2001), *COPS Usage for Policy Provisioning (COPS-PR)* <http://www.ietf.org/rfc/rfc3084.txt?number=3084>.

[b-IETF RFC 3174] IETF RFC 3174 (2001), *US Secure Hash Algorithm 1 (SHA1)* <http://www.ietf.org/rfc/rfc3174.txt?number=3174>.

[b-IETF RFC 3377] IETF RFC 3377 (2002), *Lightweight Directory Access Protocol (v3): Technical Specification* <http://www.ietf.org/rfc/rfc3377.txt?number=3377>.

[b-IETF RFC 3579] IETF RFC 3579 (2003), *RADIUS (Remote Authentication Dial In User Service) Support For Extensible Authentication Protocol (EAP)* <http://www.ietf.org/rfc/rfc3579.txt?number=3579>.

[b-IETF RFC 3580] IETF RFC 3580 (2003), *IEEE 802.1X Remote Authentication Dial In User Service (RADIUS) Usage Guidelines* <http://www.ietf.org/rfc/rfc3580.txt?number=3580>.

[b-IETF RFC 3748] IETF RFC 3748 (2004), *Extensible Authentication Protocol (EAP)* <http://www.ietf.org/rfc/rfc3748.txt?number=3748>.

[b-IETF RFC 4017] IETF RFC 4017 (2005), *Extensible Authentication Protocol (EAP) Method Requirements for Wireless LANs* <http://www.ietf.org/rfc/rfc4017.txt?number=4017>.

[b-IETF RFC 4252] IETF RFC 4252 (2006), *The Secure Shell (SSH) Authentication Protocol* <http://www.ietf.org/rfc/rfc4252.txt?number=4252>.

[b-IETF RFC 4366] IETF RFC 4366 (2006), *Transport Layer Security (TLS) Extensions* <http://www.ietf.org/rfc/rfc4366.txt?number=4366>.

[b-IETF RFC 4557] IETF RFC 4557 (2006), *Online Certificate Status Protocol (OCSP) Support for Public Key Cryptography for Initial Authentication in Kerberos (PKINIT)* <http://www.ietf.org/rfc/rfc4557.txt?number=4557>.

[b-ISO/IEC 7816-x] ISO/IEC 7816-x, *Identification cards – Integrated circuit(s) cards with contacts* <http://www.iso.org/iso/search.htm?qt=7816&searchSubmit=Search&sort=rel&type=simple&published=on>.

[b-ISO/IEC 18028-2] ISO/IEC 18028-2:2006, *Information technology – Security techniques – IT network security – Part 2: Network security architecture* <http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=40009>.

[b-ISO/IEC 18028-3] ISO/IEC 18028-3:2005, *Information technology – Security techniques – IT network security – Part 3: Securing communications between networks using security gateways* <http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=40010>.

[b-ISO/IEC 18028-5] ISO/IEC 18028-5:2006, *Information technology – Security techniques – IT network security – Part 5: Securing communications across networks using virtual private networks* <http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=40012>.

[b-ISO/IEC 18043] ISO/IEC 18043:2006, *Information technology – Security techniques – Selection, deployment and operations of intrusion detection systems* <http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=35394>.

[b-IEEE 802.11] IEEE 802.11-2007, *IEEE Standard for Information technology – Telecommunications and information exchange between systems – Local and metropolitan area networks – Specific requirements – Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications* <http://standards.ieee.org/getieee802/download/802.11-2007.pdf>.

[b-IEEE 802.1X] IEEE 802.1X-2004, *IEEE Standard for Local and metropolitan area networks: Port-Based Network Access Control* <http://www.ieee802.org/1/pages/802.1x.html>.

[b-W3C XML 1.0] W3C XML 1.0 (2004), *Extensible Markup Language (XML) 1.0 (Third Edition),* W3C Recommendation, Copyright © [4 February 2004] World Wide Web Consortium, (Massachusetts Institute of Technology, Institut National de Recherche en Informatique et en Automatique, Keio University), <http://www.w3.org/TR/REC-xml/>.

[b-SSL3] The SSL Protocol Version 3.0, <http://wp.netscape.com/eng/ssl3/draft302.txt>.

[b-WPA] Wi-Fi Alliance, *Wi-Fi Protected Access*, <http://www.wi-fi.org/white_papers/whitepaper-022705-deployingwpawpa2enterprise/>.

СЕРИИ РЕКОМЕНДАЦИЙ МСЭ-Т

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

Отпечатано в Швейцарии
Женева, 2009 г.