



СОВРЕМЕННЫЕ ТЕХНОЛОГИИ ЗАЩИТЫ ИНФОРМАЦИИ В ЛОКАЛЬНЫХ СЕТЯХ

¹Дехконов О., ²Киличов Ж.

¹Военный институт информационно-коммуникационных технологий и связи.

²Самаркандский государственный университет имени Шарафа Рашидова.

E-mail: jasurkilichov1987@gmail.com

Аннотация. Современные локальные и корпоративные сети являются важнейшей составляющей информационной инфраструктуры предприятий, государственных учреждений и образовательных организаций. Расширение сетевого взаимодействия одновременно приводит к увеличению числа угроз, связанных с несанкционированным доступом, перехватом и изменением данных, вредоносным программным обеспечением, нарушением доступности ресурсов и другими видами сетевых атак. В статье рассматриваются основные методы и средства обеспечения информационной безопасности локальных сетей. Анализируются технические, программные, организационные и криптографические механизмы защиты. Особое внимание уделяется межсетевым экранам, фильтрации и мониторингу трафика, системам обнаружения вторжений, технологии VPN и протоколу IPsec. Показано, что эффективная защита локальной сети должна строиться на основе комплексного многоуровневого подхода.

Ключевые слова: локальная сеть, информационная безопасность, защита информации, сетевые угрозы, межсетевой экран, мониторинг трафика, IDS, VPN, IPsec, аутентификация, шифрование.

1. Введение. Развитие информационно-коммуникационных технологий сопровождается постоянным увеличением количества вычислительных



устройств, используемых как отдельными пользователями, так и организациями. Для совместного использования информационных и аппаратных ресурсов компьютеры объединяются посредством каналов передачи данных в компьютерные сети.

Одним из наиболее распространённых типов компьютерных сетей является локальная сеть. Она предназначена для объединения устройств, расположенных в пределах определённой территории, например здания, предприятия, организации или структурного подразделения. Локальные сети обеспечивают возможность централизованного хранения и обработки информации, совместного использования оборудования и программных ресурсов, а также оперативного обмена данными между пользователями.

Наряду с очевидными преимуществами объединение вычислительных устройств в сеть приводит к появлению дополнительных угроз информационной безопасности. Чем больше количество устройств и пользователей, тем сложнее обеспечить контролируемый доступ к информационным ресурсам и предотвратить их несанкционированное использование.

Информационная безопасность локальной сети представляет собой совокупность технических, программных, организационных и административных мероприятий. При этом нельзя рассматривать безопасность только как задачу установки антивирусной программы или межсетевого экрана. Существенную роль играет человеческий фактор, поскольку ошибки персонала, нарушение правил эксплуатации и неправильная настройка оборудования могут привести к снижению защищённости всей системы. В исходном материале также подчёркивается необходимость сочетания программных и аппаратных средств защиты.

Таким образом, задача обеспечения информационной безопасности требует комплексного подхода, включающего контроль доступа,



криптографическую защиту, мониторинг сетевой активности, фильтрацию трафика и организацию соответствующей политики безопасности.

2. Основные методы и средства обеспечения информационной безопасности. Одной из основных задач при построении защищённой сети является разработка системы методов и средств, позволяющих снизить вероятность реализации угроз и ограничить возможные последствия нарушений.

К основным методам обеспечения информационной безопасности относятся управление доступом, маскировка, препятствие, регламентация, принуждение и побуждение. Эти методы различаются принципом действия, однако в комплексной системе безопасности они должны применяться совместно.

Управление доступом предназначено для ограничения возможностей пользователей при работе с информационными ресурсами. Оно включает идентификацию субъекта, проверку его подлинности, определение полномочий и регистрацию действий. Такой подход позволяет установить, какой пользователь, в какое время и к каким ресурсам получил доступ.

Регламентация определяет правила обработки, хранения и передачи защищаемых данных. На организационном уровне устанавливаются обязанности пользователей, порядок работы с информацией и ответственность за нарушение требований безопасности.

Принуждение связано с обязательным соблюдением установленных норм, а побуждение ориентировано на формирование у сотрудников ответственного отношения к вопросам защиты информации.

Маскировка предполагает использование криптографических преобразований для предотвращения доступа посторонних лиц к содержанию информации. Особенно важным данный механизм является при передаче конфиденциальной информации по открытым каналам связи.



Препятствие представляет собой физическое ограничение доступа к оборудованию, носителям информации и другим элементам информационной системы.



Рис. 1. Методы и средства обеспечения информационной безопасности.

Средства защиты информации принято подразделять на формальные и неформальные. Формальные средства выполняют свои функции в соответствии с установленными алгоритмами и практически не требуют непосредственного участия человека. К ним относятся технические, программные и специальные средства.

Технические средства могут быть представлены различными электрическими, электронными и электромеханическими устройствами. К данной категории относятся как встроенные элементы компьютерных систем, так и внешнее оборудование, подключаемое через стандартные интерфейсы.

Программные средства предназначены для реализации функций защиты на программном уровне. Они могут обеспечивать контроль доступа, антивирусную защиту, регистрацию событий, мониторинг состояния сети и управление механизмами информационной безопасности.



Специальные средства включают прежде всего криптографические методы. Они используются как для защиты информации внутри информационной системы, так и для обеспечения безопасности данных, передаваемых через каналы связи.

К неформальным средствам относятся организационные, законодательные и морально-этические меры. Организационные средства устанавливают порядок использования оборудования и информационных ресурсов. Законодательные механизмы определяют правовые нормы работы с информацией, а морально-этические средства формируют правила поведения пользователей.

3. Основные угрозы безопасности локальных сетей. Эффективность системы защиты во многом зависит от правильного определения возможных угроз. Локальные сети могут подвергаться как внешнему, так и внутреннему воздействию.

К наиболее распространённым сетевым угрозам относятся перехват трафика, изменение передаваемой информации, анализ сетевой активности, атаки типа «человек посередине», перехват пользовательских сеансов, атаки на пароли, отказ в обслуживании и распространение вредоносного программного обеспечения.

Перехват трафика представляет опасность прежде всего для конфиденциальности данных. Если информация передаётся в незашифрованном виде, злоумышленник может попытаться получить её содержимое путём анализа сетевых пакетов.

Изменение данных направлено на нарушение их целостности. При этом злоумышленник не только перехватывает информацию, но и вносит изменения перед её доставкой получателю.



Атака типа «человек посередине» связана с вмешательством третьей стороны в процесс взаимодействия двух сетевых узлов. В результате нарушитель может попытаться контролировать передаваемую информацию.

Отдельную группу составляют DoS- и DDoS-атаки, направленные на нарушение доступности информационных ресурсов. При их реализации сервер или сетевое устройство получает большое количество запросов, в результате чего законные пользователи могут утратить возможность доступа к сервису.

Кроме того, значительную угрозу представляют вредоносные программы, сетевые черви и другие программные средства, предназначенные для нарушения работы вычислительной системы или получения несанкционированного доступа.



Рис. 2. Классификация основных угроз информационной безопасности локальной сети.

Угрозы могут быть преднамеренными и естественными. К естественным угрозам относятся аварии, пожары, стихийные явления и отказы оборудования, которые также могут стать причиной повреждения или потери информации.



Следовательно, защита локальной сети должна предусматривать противодействие не только действиям злоумышленников, но и непреднамеренным событиям.

4. Обеспечение безопасности сетевого взаимодействия с использованием IPsec. Одним из наиболее важных направлений защиты является обеспечение безопасности информации непосредственно при её передаче между сетевыми устройствами.

В исходном материале безопасность на уровне IP рассматривается с точки зрения трёх основных функций: аутентификации, конфиденциальности и управления ключами. Аутентификация позволяет проверить подлинность источника данных и убедиться, что пакет не был изменён во время передачи. Конфиденциальность достигается посредством шифрования информации, а управление ключами обеспечивает безопасный обмен криптографическими параметрами.

Для реализации этих задач применяется комплекс протоколов IPsec. Его использование позволяет обеспечить защищённую передачу информации в локальных, корпоративных и глобальных сетях.

IPsec может применяться для организации:

- защищённого взаимодействия между филиалами;
- удалённого доступа пользователей;
- безопасного соединения между организациями;
- защищённого обмена данными через Интернет.

Особенностью IPsec является возможность защиты сетевого трафика непосредственно на IP-уровне. В результате механизм безопасности становится применимым к различным типам программных приложений и сервисов.

5. Межсетевые экраны и фильтрация трафика. Одним из основных механизмов обеспечения безопасности локальной сети является фильтрация



трафика. Под фильтрацией понимается анализ сетевых пакетов маршрутизаторами или межсетевыми экранами с последующим разрешением, блокировкой либо изменением маршрута их передачи.

Правила фильтрации могут устанавливаться сетевым администратором на основании принятой в организации политики информационной безопасности.

Центральным компонентом системы сетевой защиты является межсетевой экран, или фаервол. Он представляет собой программный, аппаратный либо программно-аппаратный комплекс, предназначенный для разграничения сетей и контроля проходящего между ними информационного обмена.

Основными функциями межсетевого экрана являются фильтрация трафика и аудит событий. В современных системах он может также выполнять дополнительные задачи: антивирусную проверку, шифрование, трансляцию сетевых адресов, фильтрацию содержимого, обнаружение сетевых атак и организацию VPN.



Рис. 3. Основные функции межсетевого экрана.



Межсетевой экран является важным рубежом защиты, однако его применение не гарантирует полного исключения возможных атак. Новые или неизвестные методы воздействия могут пройти через установленные фильтры. Поэтому межсетевое экранирование должно дополняться мониторингом сетевого трафика.

6. Мониторинг трафика и системы обнаружения вторжений.

Мониторинг сетевого трафика представляет собой непрерывное автоматизированное наблюдение за параметрами информационного обмена. Его применение позволяет контролировать состояние сети, обнаруживать аномалии, выявлять потенциальные атаки и анализировать причины возникающих проблем.

В исходном материале в качестве основных средств мониторинга рассматриваются анализаторы протоколов, маршрутизаторы с поддержкой NetFlow и системы обнаружения вторжений IDS.

Анализаторы протоколов позволяют захватывать сетевой трафик и представлять полученные данные в удобной для изучения форме. При этом итоговый анализ полученной информации может осуществляться администратором.

Технология NetFlow обеспечивает получение обобщённых сведений о потоках сетевого трафика и передачу результатов специализированным программным системам.

Системы обнаружения вторжений IDS используются для автоматического выявления потенциальных атак и нарушений безопасности.



Рис. 4. Средства мониторинга сетевого трафика.

IDS могут классифицироваться по источнику анализируемых данных и используемому методу обнаружения. В исходной статье выделяются сетевые, хостовые и прикладные IDS, а также системы на основе сигнатур, аномалий и спецификаций.

Таким образом, совместное применение межсетевого экрана и IDS позволяет реализовать более эффективную многоуровневую защиту. Межсетевой экран ограничивает нежелательные соединения, а система обнаружения вторжений выявляет подозрительную активность в разрешённом сетевом трафике.

7. Использование VPN для защиты передаваемых данных. При организации взаимодействия между территориально удалёнными сегментами корпоративной сети или подключении удалённых пользователей требуется обеспечить конфиденциальность передаваемой информации.

Для этого может использоваться технология виртуальной частной сети VPN. Она позволяет организовать логически защищённое соединение через общедоступную сеть.

Для построения VPN применяются аппаратные, программные и комбинированные средства. Исходная статья рассматривает несколько протоколов VPN и сравнивает их по таким параметрам, как поддерживаемые



операционные системы, сложность настройки, безопасность, скорость и особенности соединения.

Таблица 1.

Сравнительная характеристика основных VPN-протоколов.

Параметры	PPTP	SSTP	L2TP	L2TP/IPsec	IPsec IKE2	OpenVPN
Поддерживаемые ОС	Windows, MacOS X, Linux, iOS, Android, Windows Phone	Windows	Windows, MacOS X, Linux, iOS, Android, Windows Phone	Windows, MacOS X, Linux, iOS, Android, Windows Phone	Windows, MacOS X, Linux, iOS, Android, Windows Phone	Windows, MacOS X, Linux, iOS, Android
Популярность ОС	Очень высокий	Низкий	Высокий	Очень высокий	Высокий	Высокий
Настройка	Очень простая. Не требует дополнительного ПО.	Необходимо установка сертификатов.	Простая. Не требует дополнительного ПО.	Простая. Не требует дополнительного ПО.	Простая. Не требует дополнительного ПО.	Необходимо установка сертификатов.
Баланс нагрузки на МП	Да	Да	Да	Да	Да	Нет



Безопасность	Низкий	Высокий	Низкий	Высокий	Очень высокий	Высокий
Уровень шифрования	Текст ячейки	Текст ячейки	Текст ячейки	Текст ячейки	Текст ячейки	Текст ячейки
Надёжность	Да	Да	Да	Да	Да	Да
Протокол	GRE	TCP	UDP	UDP/ESP	UDP, ESP	TCP
Установка соединения	Средний	Средний	Средний	Медленный	Очень быстрой	Медленный
Скорость	Высокая	Отличная производительность	Требовательная к ресурсам ЦП.	Требовательная к ресурсам ЦП.	Требовательная к ресурсам ЦП.	Отличная производительность
Маршруты толчка	Нет	Нет	Нет	Нет	Да	Да
Обход NAT	Да	Да	Да	Да	Да	Да
Имеет интерфейс	Да	Да	Да	Да	Нет	Да



Используй- мые порты	TCP 1723, GRE.	TCP 443.	UDP 1701. UDP 500. UDP 4500. ESP.	UDP 1701. UDP 500. UDP 4500. ESP.	UDP 1701. UDP 500. UDP 4500. ESP.	TCP 993. TCP 443.
Итого	Быстры й и очен легкий в настрой ке.	Высокая произво дительно сть, безопас ность и стабиль ность.	Хороший выбор, если устройств а не поддержи вают	Хороший выбор, если устройств а не поддержи вают	Хороший выбор, если устройств а не поддержи вают	Высокая произво дительно сть, безопас ность и стабиль ность.

Защита VPN основывается на нескольких механизмах: шифровании, аутентификации, авторизации и туннелирования.

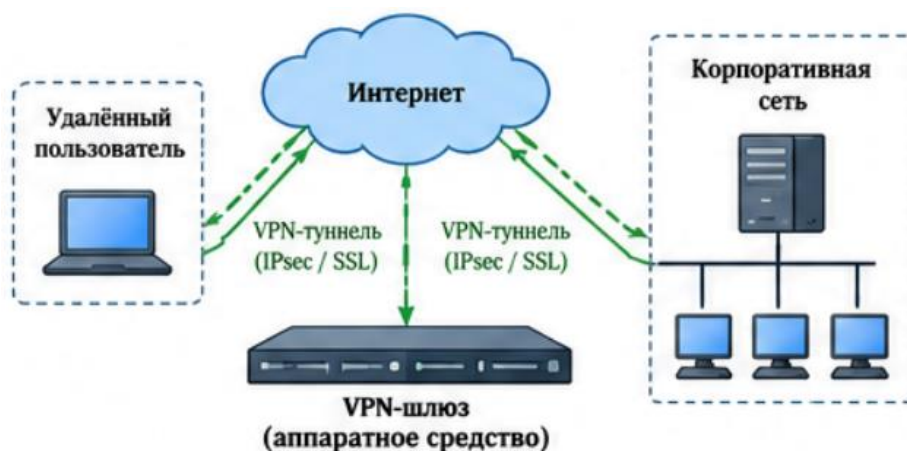


Рис. 5. VPN на базе специализированных аппаратных средств.

Таблица 2.

Основные механизмы обеспечения безопасности VPN.



Механизм	Основное назначение
Шифрование	Обеспечение конфиденциальности информации
Аутентификация	Проверка подлинности пользователя или устройства
Авторизация	Определение разрешённых пользователю ресурсов
Туннелирование	Создание логически защищённого канала передачи данных

VPN особенно важно использовать при удалённой работе сотрудников, когда подключение к корпоративной инфраструктуре осуществляется через внешние сети.

8. Комплексная защита локальной сети. Защита локальной сети должна осуществляться одновременно на нескольких уровнях.

Первым уровнем является физическая безопасность. Доступ к серверным помещениям, сетевым шкафам и носителям информации должен предоставляться только уполномоченным сотрудникам. В исходном материале физическая защита рассматривается как одно из первоочередных мероприятий по предотвращению несанкционированного доступа.

Второй уровень включает межсетевое экранирование. Межсетевой экран должен фильтровать входящий и исходящий трафик, блокируя потенциально опасные соединения.

Следующим компонентом является антивирусная защита рабочих станций, серверов, шлюзов и других информационных ресурсов. В исходной статье отдельно отмечается необходимость защиты серверов, рабочих станций, интернет-шлюзов и других элементов корпоративной инфраструктуры.

Отдельное внимание необходимо уделять удалённым подключениям. Для этого целесообразно применять защищённые VPN-соединения.



Важным элементом является также безопасность корпоративной электронной почты. Для противодействия спаму и фишинговым сообщениям могут применяться специализированные программные средства, списки подозрительных адресов и анализ вложений.



Рис. 6. Многоуровневая структура защиты корпоративной локальной сети.

Комплексная система защиты локальной сети должна включать физическую безопасность оборудования, идентификацию и аутентификацию пользователей, разграничение доступа, межсетевое экранирование, антивирусную защиту, шифрование, VPN, мониторинг трафика, IDS и регистрацию событий безопасности.

Заключение. Обеспечение информационной безопасности локальных и корпоративных сетей представляет собой комплексную задачу, требующую применения различных взаимодополняющих методов защиты.

Ни один отдельно взятый механизм не способен полностью обеспечить безопасность информационной инфраструктуры. Межсетевой экран выполняет функцию фильтрации трафика, однако для обнаружения прошедших через него угроз требуется применение систем мониторинга и



IDS. Антивирусная защита позволяет противодействовать вредоносному программному обеспечению, однако не заменяет механизмов разграничения прав пользователей и криптографической защиты данных.

При передаче информации через общедоступные сети целесообразно применять VPN и IPsec, позволяющие обеспечить шифрование и аутентификацию сетевого взаимодействия.

Наиболее эффективным является многоуровневый подход, предусматривающий совместное применение технических, программных, криптографических и организационных средств защиты. При этом значительную роль играет правильно разработанная политика безопасности, регламентирующая порядок доступа пользователей к информационным ресурсам. Аналогичный вывод сформулирован в исходной статье: объединение различных методов и средств позволяет существенно повысить уровень защищённости сети.

Список литературы.

1. Орловская Л.А., Поначугин А.В. Локальные вычислительные сети // Научное сообщество студентов XXI столетия. Тех. науки. - 2016. - № 5(41).
2. Кучина А., Рафикова В. Безопасность локальных сетей // Вестник науки. - 2018. - № 2(2).
3. Абраров Р.Д., Курязов Д.А. Информационная безопасность в компьютерных сетях // Молодой ученый. - 2016. - № 9.5. - С. 10-12.
4. Ковалев М.С. Оптимизация размещения средств защиты информации в узлах коммутации VPN-сети: диссертация кандидата технических наук. - Серпухов, 2017.
5. Буренин А.Н., Легков К.Е. Современные инфокоммуникационные системы и сети специального назначения. Основы пос. и упр. - М., 2015.
6. Tsai P.-W. et al. Network Monitoring in Software-Defined Networking: A Review // IEEE Systems Journal. - 2018. - Vol. 12, № 4. - P. 3958-3969.