***Лекция 29.***

**Безопасность сетевого программного обеспечения и оборудования**

***План:***

***1. Сетевая безопасность***

***2. Программная и аппаратная безопасность***

***3. Методы и средства защиты***

***Ключевые слова:*** *целостность сети, угрозы, несанкционированный доступ, удаленный доступ, аппаратное устройство, программный модуль, токен, несанкционированный доступ, идентификация, аутентификация, авторизация, электронные ключи, уровень защиты, уязвимость, эмулятор, перехват, маскарад, отказ в обслуживании*

**Сетевая безопасность**

Система сетевой безопасности — это комплекс мер, направленных на поддержание удобства использования и защиту целостности сети и данных.

* Она использует аппаратные и программные технологии;
* Она борется с различными угрозами;
* Она блокирует их проникновение и распространение в сети;
* Эффективная система сетевой безопасности управляет доступом к сети.

Сетевая безопасность – это термин достаточно общего плана. Он подразумевает как ограничение нежелательного доступа в сеть и сохранность данных, так и эффективное функционирование компьютерной сети в целом.

Основные принципы сетевой безопасности:

* защита внутренних сетей от несанкционированного доступа;
* обеспечение безопасного подключения к сети Интернет и безопасного удаленного доступа;
* контроль за работой различных онлайн-приложений, через которые также возможен доступ к персональным компьютерам.
* предоставление возможности осуществления коммерческих операций через Интернет.

**Программная и аппаратная безопасность**

Необходимость защиты информации достаточно очевидна. Частые утечки конфиденциальных данных, например, сведений о клиентах банков с номерами их карт или персональных данных, угрожают личной безопасности. Программно-аппаратная защита с использованием современных технических средств призвана снизить риск утечек, ограничив внутренний доступ к информационным системам.

Для чего нужна программно-аппаратная защита информации?

Аппаратные средства защиты в большинстве случаев охраняют информацию, доступ к которой ограничен на основании требований закона, например, государственную или банковскую тайну, персональные данные. Поэтому правила их использования полностью или частично регламентируются на уровне государства. Статус охраняемой информации определяется законами, нормативными актами и различными рекомендациями.

Обеспечение безопасности информации на программно-аппаратном уровне предохраняет сведения от несанкционированного доступа и снижает риски хищения и дальнейшего неправомерного использования полученных сведений.

Комплекс аппаратно-программной защиты состоит из двух частей:

* аппаратное устройство;
* программный модуль.

Принцип работы системы состоит в том, что при попытке получения доступа к данным программа отправляет запрос к устройству, обеспечивающему работу ключа (токену, ридеру, электронному идентификатору, после подключения которого к компьютеру, тот дает разрешение на работу), и функционирует только при его положительной реакции.

Токен - компактное устройство, предназначенное для обеспечения информационной безопасности пользователя, также используется для идентификации его владельца, безопасного удалённого доступа к информационным ресурсам и т. д. С точки зрения надежности эта методика выглядит предпочтительнее, чем просто программная защита, но стоимость аппаратной части делает ее доступной только для крупных и средних компаний или государственных организаций.

Защита от несанкционированного доступа. При выборе методов и средств защиты данных нужно учитывать, что существует несколько принципов защиты от несанкционированного доступа. На них основана работа средств программно-аппаратной защиты:

* доступ к данным предоставляется только тем пользователям, которые уполномочены его получить на уровне внутренних документов компании;
* каждый уполномоченный пользователь имеет доступ только к своему уровню информации, его прав недостаточно для работы с данными, находящимися в сфере ответственности других пользователей;
* перечень операций, которые допустимо выполнять с данными, строго регламентирован, и зависит от изначально заданных прав пользователей.

Для такой защиты в аппаратно-программных средствах должен быть механизм распознавания уполномоченного пользователя и его авторизации (идентификации и аутентификации).

Процесс авторизации состоит из трех этапов:

*1. Идентификация.* Пользователь должен передать системе свой идентифицирующий признак, например, логин и пароль. При использовании аппаратных средств становится возможной и более глубокая степень идентификации по отпечатку пальца, сетчатке глаза, иным биометрическим признакам или на основании владения определенным устройством (магнитная карточка, электронный ключ);

*2. Аутентификация.* Этот процесс в работе программно-аппаратных средств нацелен на сравнение заявленного пользователем идентифицирующего признака с теми, которые хранятся в памяти устройства. В ходе аутентификации устанавливается подлинность пользователя. Она может реализовываться на основе простой или усложненной PIN-идентификации. В обоих случаях персональный идентификационный номер пользователя сравнивается с эталоном. При простом механизме идентификации система проводит обычное сравнение и в случае совпадения выдает разрешение на дальнейшую работу. При сложном, защищенном, система посылает запрос ключу, тот «отвечает» отправкой 64-разрядного ключа.

Система складывает число с введенным пользователем PIN-кодом, направляя полученный результат ключу, тот проводит итоговую идентификацию, при положительном результате которой выдает разрешение на работу;

*3. Авторизация.* После того как подлинность пользователя установлена, аппаратно-программным средством определяется объем предоставленных ему прав.

*Электронные ключи*

Работа программно-аппаратных средств защиты информации становится невозможной, если их архитектурой не предусмотрено наличие электронных ключей. Они представляют собой явление предметного мира, физическое устройство, снабженное электронной начинкой и содержащее уникальную информацию, позволяющую идентифицировать пользователя.

Ключи бывают трех видов:

1. Специализированный электронный чип.
2. Микросхема перепрограммируемой памяти, имеющая собственные источники электропитания.
3. Ключ на базе микропроцессора.

Выбор технологии, на которой основан ключ, связан с типом аппаратного средства. Ранее ключи совмещались с рабочей станцией посредством обычных портов, через которые подключаются принтер, что создавало неудобство для пользователей. Развитие USB-технологий упростило использование электронных ключей при работе с аппаратно-программными средствами защиты информации.

Как работает электронный ключ? Устройство, содержащее код пользователя, опознается программной частью системы, в результате осуществляется допуск к работе. Помимо данных, идентифицирующих пользователя, в ключе могут содержаться сведения о программе, используемой аппаратной частью: номер, данные о выпуске, дата оформления лицензии.

Данные, содержащиеся в памяти ключа, могут перепрограммироваться в дистанционном режиме, что усиливает безопасность.

Электронные ключи применяются и для защиты авторских прав разработчика программы: считают число лицензий и не допускают их использование в большем количестве, чем оговорено в соглашении.

Принимая решение о выборе аппаратно-программного средства, необходимо понимать, что современные технологии позволяют взламывать системы с недостаточным уровнем защиты. При этом стоимость аппаратной части высока. Современные версии ключей, токены, основаны на новейших технологиях, которые позволяют избежать ряда рисков, но не в полном объеме.

Для несанкционированного проникновения (взлома) в систему обычно используется один из двух методов:

* поиск и использование уязвимостей в программной части;
* эмулирование (подмена) данных, содержащихся в электронном ключе.

В первом случае из программы (приложения) удаляются части, в которых содержится код, обеспечивающий работу механизмов защиты. Это могут быть команды опроса электронного ключа (направление запроса в отдельном токе данных) или команды сравнения введенных данных с эталоном.

Второй путь взлома, эмулирование электронного ключа, связан с использованием специальных программных средств – эмуляторов. Программа отправляет приложению обращения, содержащие, правильные ответы.

Если в первом случае методом защиты будет стандартное ограничение прав пользователей, исключающее вмешательство в программный код, во втором рекомендуется вкладывать в конструкцию устройства алгоритм хаотического обмена данными.

Следует учитывать, что реализация схемы эмуляции ключа крайне сложна и доступна немногим специалистам. Взаимодействие эмулятора ключа с программой осуществляется одним из двух способов:

* путем подмены драйвера;
* через точку входа API вызова ключа.

В первом случае решением станет регулярный аудит системных файлов, проверяющих их изменения.

Во втором – шифрование той части программы, которая отвечает за взаимодействие с ключом, или реализация опции постоянного контроля его целостности.

Программно-аппаратные механизмы защиты информации находят все большее применение. Они используются не только для защиты локальных сетей, но и для работы с облачными хранилищами. Цена устройств по мере развития технологий снижается. Поэтому при разработке архитектуры собственной информационной системы, в целях обеспечения максимально достижимого уровня безопасности, следует рассмотреть возможность их применения.

**Методы и средства защиты информации в сети Интернет**

К типовым угрозам безопасности информации при использовании глобальных компьютерных сетей относятся:

* анализ сетевого трафика («перехват»);
* подмена субъекта или объекта сети («маскарад»);
* внедрение ложного объекта сети («человек посередине», «Мап-in-Middle» — MiM);
* отказ в обслуживании (Deny of Service — DoS) или «распределенный» отказ в обслуживании (Distributed Deny of Service — DDoS).

Другими угрозами безопасности информации при работе в сети Интернет, вытекающими из перечисленных выше типовых угроз, являются:

• выполнение на компьютере пользователя небезопасного (потенциально вредоносного) программного кода;

• утечка конфиденциальной информации пользователя (персональных данных, коммерческой тайны);

• блокирование работы сетевой службы (Web-сервера, почтового сервера, сервера доступа Интернет-провайдера и т. п.).

Основные причины, облегчающие нарушителю реализацию угроз безопасности информации в распределенных компьютерных системах:

• отсутствие выделенного канала связи между объектами распределенной КС (наличие широковещательной среды передачи данных);

• использование недостаточно надежных протоколов аутентификации объектов распределенной компьютерной сети перед установлением виртуального канала между ними, что позволяет нарушителю при перехвате передаваемых сообщений выдать себя за одну из сторон соединения;

• отсутствие возможности контроля маршрута получаемых сообщений, что не позволяет подтвердить адрес отправителя данных и определить инициатора удаленной атаки на компьютерную сеть;

• отсутствие полной информации об объектах компьютерной сети, с которыми требуется создать соединение;

• отсутствие шифрования передаваемых сообщений, что позволяет нарушителю получить несанкционированный доступ к информации в распределенной компьютерной сети.

К основным методам создания безопасных распределенных компьютерных сетей относятся:

* использование выделенных каналов связи путем физического соединения каждой пары объектов распределенной компьютерной сети или применения топологии «звезда» и сетевого коммутатора, через который осуществляется связь между объектами;

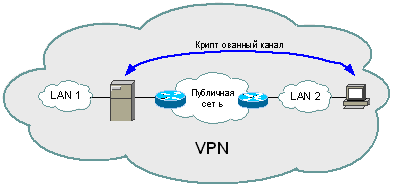
• контроль маршрута поступающих сообщений;

• разработка распределенной компьютерной сети с полной информацией об ее объектах.

Одним из методов защиты от перечисленных выше угроз является технология виртуальных частных сетей (Virtual Private Network — VPN). Подобно созданию выделенного канала связи VPN позволяют установить защищенное цифровое соединение между двумя участниками (или сетями) и создать глобальную сеть из существующих локальных сетей.

Трафик VPN передается поверх IP-трафика и использует в качестве протокола транспортного уровня датаграммы, что позволяет ему спокойно проходить через Интернет. Для скрытия передаваемых данных в VPN осуществляется их шифрование. Существуют аппаратные решения VPN, обеспечивающие максимальную защиту, а также программные или основанные на протоколах реализации.





**Контрольные вопросы:**

1. Что такое сетевая безопасность?
2. Основные принципы сетевой безопасности.
3. Части аппаратно-программной защиты.
4. Что такое токен?
5. Опишите процесс авторизации.
6. Виды электронных ключей.
7. Как происходит несанкционированное проникновение в систему?
8. Типовые угрозы безопасности в глобальных компьютерных сетях.
9. Причины, облегчающие реализацию угроз.
10. Что такое VPN?