ЗАЩИТА ИНФОРМАЦИИ В ИНТЕРНЕТ

Мавлянова Лола Тахировна,
специализированная государственная общеобразовательная школа №19 города Бухары, Бухарской области, учитель информатики

АННОТАЦИЯ

Интернет можно по праву назвать главным символом 21-го века. Глобальная Сеть стала Всемирной, не только охватив своей паутиной все континенты и страны, но и проникнув в каждую сферу жизни. Через Интернет решаются вопросы, начиная от заказа пиццы в ближайшем кафе, заканчивая многомиллионными сделками. Такая территория очень быстро стала привлекать мошенников. Поэтому встаёт вопрос об информационной безопасности.

Ключевые слова: *информационная безопасность, внутренние и внешние угрозы, спуфинг (англ.spoofing - подмена), аутентификация, криптография, симметричное шифрование, брандмауэр, электронно-цифровая подпись.*

PROTECTION OF INFORMATION ON THE INTERNET

Mavlyanova Lola Taxirovna
computer science teacher specialized state secondary school №19 Bukhara cities, Bukhara region

ABSTRACT

The Internet can be rightfully called the main component of the 21st century. The global network has become worldwide, not only covering its web all continents and countries, but also penetrating into every sphere of life. Over the Internet, questions are solved, ranging from the order of pizza in the nearest cafe, ending with multimillion transactions. This territory very quickly began to attract fraudsters. Therefore, there is a question about information security.

Keywords: *Information security, internal and external threats, authentication, spoofing, cryptography, symmetric encryption, firewall, electronic digital signature.*

INTERNETDA AXBOROTNI HIMOYA QILISH

Mavlyanova Lola Taxirovna
Buxoro viloyati, Buxoro shahar,
19-ixtisoslashtirilgan davlat umumta’lim maktabi, informatika fani o’qituvchisi

ANNOTATSIYA

Internetni 21-asrning ramzi deb atash mumkin. Global tarmoq butun dunyoni o'z to'ri bilan qamrabgina qolmasdan, kundalik hayotning barcha sohalariga kirib bordi. Internet orqali oddiy pitsa zakaz qilishdan tortib, qimmatli kelishuvlargacha hal qilsa bo'ladi. Internetning bu globallashuvi firibgarlarni ham o'ziga jalb qildi. Bu firibgarlikka barham berish uchun axborot xavfsizligi nima ekanligi haqida savol tug'iladi.

Kalit so'zlar: *Axborot xavfsizligi, ichki va tashqi tahdidlar, stena (Engl.spoofing - almashtirish), autentifikatsiya, kriptografiya, simmetrik shifrlash, elektron raqamli imzo*

ВВЕДЕНИЕ

Ускорение процесса глобализации по всему миру, широкое распространение информационных технологий во все области жизни общества позволило довести практически до бесконечности уровень доступа информации человечеством. Любой вид деятельности в Интернете: движение финансовых средств, заказы товаров и услуг, оплата пластиковой картой или иным способом, общение в социальных сетях, даже чтение новостей на популярных сайтах связаны с различными рисками и требуют обеспечения информационной безопасности. Информация, передаваемая по Интернету, проходит через сотни устройств, на которых они временно хранятся для обеспечения бесперебойной передачи. И в каждом из них могут возникнуть угрозы её целостности и скрытности. Вместе с этим растет количество раскрытия конфиденциальной информации в Интернете. Основными причинами является человеческий фактор и несанкционированное внешнее вторжение. В результате удачных вторжений из вне уплывает большой объем информации. Но утечка самых ценных данных осуществляется заинтересованными офисными работниками из-за корыстных целей.

Защита информации – это комплекс мер по предотвращению утечки, потери, хищения, подделки, фальсификации информации, а также несанкционированного доступа и размножения.

ОБСУЖДЕНИЕ И РЕЗУЛЬТАТЫ

В компьютерных системах вместе с понятием защиты информации широко распространено понятие информационной безопасности. ***Информационная безопасность*** – обеспечение скрытности, целостности и доступности информации, не ограничивая требований пользования ею. Возможные дыры в

информационной безопасности могут возникнуть с двух направлений: внешняя угроза и внутренняя угроза. Внешние угрозы исходят от людей: доступ к конфиденциальным данным случайно или преднамеренно получают пользователи внешней сети. Это могут быть и сотрудники компании, и злоумышленники, а также и форс-мажорные обстоятельства**,** например, стихийные бедствия. Внутренние угрозы - технические факторы: из-за ошибки программирования может произойти сбой оборудовании или отключение электроснабжения, оставляет возможность проникновения в сеть.

Проблемы, возникающие с безопасностью передачи информации при работе в компьютерных сетях, можно разделить на четыре основных типа:

- перехват информации - целостность информации сохраняется, но ее конфиденциальность нарушена;
- модификация информации - исходное сообщение изменяется либо полностью подменяется другим и отсылается адресату;
- подмена авторства информации;
- перехват сообщения с его изъятием.

Данная проблема может иметь серьезные последствия. Например, кто-то может послать письмо от вашего имени (этот вид обмана принято называть спуфингом) или Web-сервер может притворяться электронным магазином, принимать заказы, номера кредитных карт, но не высылать никаких товаров. В соответствии с перечисленными проблемами при обсуждении вопросов безопасности под самим термином "безопасность" подразумевается совокупность трех различных характеристик обеспечивающей безопасность системы:

1. Аутентификация - это процесс распознавания пользователя системы и предоставления ему определенных прав и полномочий. Каждый раз, когда заходит речь о степени или качестве аутентификации, под этим следует понимать степень защищенности системы от посягательств посторонних лиц на эти полномочия.

2. Целостность - состояние данных, при котором они сохраняют свое информационное содержание и однозначность интерпретации в условиях различных воздействий. В частности, в случае передачи данных под целостностью понимается идентичность отправленного и принятого.

3. Секретность - предотвращение несанкционированного доступа к информации. В случае передачи данных под этим термином обычно понимают предотвращение перехвата информации.

На практике используют несколько групп методов защиты, в том числе:

- **препятствие на пути предполагаемого похитителя**, которое создают физическими и программными средствами;
- **управление**, или оказание воздействия на элементы защищаемой системы;
- **маскировка**, или преобразование данных, обычно – криптографическими способами;
- **регламентация**, или разработка нормативно-правовых актов и набора мер, направленных на то, чтобы побудить пользователей, взаимодействующих с базами данных, к должному поведению;
- **принуждение**, или создание таких условий, при которых пользователь будет вынужден соблюдать правила обращения с данными;
- **побуждение**, или создание условий, которые мотивируют пользователей к должному поведению.

Для обеспечения секретности применяется шифрование, или криптография, позволяющая трансформировать данные в зашифрованную форму, из которой извлечь исходную информацию можно только при наличии ключа. В основе шифрования лежат два основных понятия: алгоритм и ключ. Алгоритм - это способ закодировать исходный текст, в результате чего получается зашифрованное послание. Зашифрованное послание может быть интерпретировано только с помощью ключа. Очевидно, чтобы зашифровать послание, достаточно алгоритма. Однако использование ключа при шифровании предоставляет два существенных преимущества. Во-первых, можно использовать один алгоритм с разными ключами для отправки посланий разным адресатам. Во-вторых, если секретность ключа будет нарушена, его можно легко заменить, не меняя при этом алгоритм шифрования. Таким образом, безопасность систем шифрования зависит от секретности используемого ключа, а не от секретности алгоритма шифрования. Многие алгоритмы шифрования являются общедоступными. Количество возможных ключей для данного алгоритма зависит от числа бит в ключе. Например, 8-битный ключ допускает 256 (28) комбинаций ключей. Чем больше возможных комбинаций ключей, тем труднее подобрать ключ, тем надежнее зашифровано послание. Так, например, если использовать 128-битный ключ, то необходимо будет перебрать $2^{128} \approx 10^{40}$ ключей, что в настоящее время не под силу даже самым мощным компьютерам. Важно отметить, что возрастающая производительность техники приводит к уменьшению времени, требующегося

для вскрытия ключей, и системам обеспечения безопасности приходится использовать все более длинные ключи, что, в свою очередь, ведет к увеличению затрат на шифрование. Поскольку столь важное место в системах шифрования уделяется секретности ключа, то основной проблемой подобных систем является генерация и передача ключа. Существуют две основные схемы шифрования: симметричное шифрование (его также иногда называют традиционным или шифрованием с секретным ключом) и шифрование с открытым ключом (иногда этот тип шифрования называют асимметричным). При симметричном шифровании отправитель и получатель владеют одним и тем же ключом (секретным), с помощью которого они могут зашифровывать и расшифровывать данные. При симметричном шифровании используются ключи небольшой длины, поэтому можно быстро шифровать большие объемы данных. Симметричное шифрование используется, например, некоторыми банками в сетях банкоматов. Однако симметричное шифрование обладает несколькими недостатками. Во-первых, очень сложно найти безопасный механизм, при помощи которого отправитель и получатель смогут тайно от других выбрать ключ. Возникает проблема безопасного распространения секретных ключей. Во-вторых, для каждого адресата необходимо хранить отдельный секретный ключ. В-третьих, в схеме симметричного шифрования невозможно гарантировать личность отправителя, поскольку два пользователя владеют одним ключом. В схеме шифрования с открытым ключом для шифрования послания используются два различных ключа. При помощи одного из них послание зашифровывается, а при помощи второго - расшифровывается. Таким образом, требуемой безопасности можно добиться, сделав первый ключ общедоступным (открытым), а второй ключ хранить только у получателя (закрытый, личный ключ). В таком случае любой пользователь может зашифровать послание при помощи открытого ключа, но расшифровать послание способен только обладатель личного ключа. При этом нет необходимости заботиться о безопасности передачи открытого ключа, а для того чтобы пользователи могли обмениваться секретными сообщениями, достаточно наличия у них открытых ключей друг друга. Недостатком асимметричного шифрования является необходимость использования более длинных, чем при симметричном шифровании, ключей для обеспечения эквивалентного уровня безопасности, что сказывается на вычислительных ресурсах, требуемых для организации процесса шифрования.

Даже если послание, безопасность которого мы хотим обеспечить, должным образом зашифровано, все равно остается возможность модификации исходного сообщения или подмены этого сообщения другим. Одним из путей решения этой проблемы является передача пользователем получателю краткого представления передаваемого сообщения. Подобное краткое представление называют ***контрольной суммой*** или ***дайджестом*** сообщения. Контрольные суммы используются при создании резюме фиксированной длины для представления длинных сообщений. Алгоритмы расчета контрольных сумм разработаны так, чтобы они были по возможности уникальны для каждого сообщения. Таким образом, устраняется возможность подмены одного сообщения другим с сохранением того же самого значения контрольной суммы. Однако при использовании контрольных сумм возникает проблема передачи их получателю. Одним из возможных путей ее решения является включение контрольной суммы в так называемую электронную подпись. При помощи электронной подписи получатель может убедиться в том, что полученное им сообщение послано не сторонним лицом, а имеющим определенные права отправителем. Электронные цифровые подписи создаются шифрованием контрольной суммы и дополнительной информации при помощи личного ключа отправителя. Таким образом, кто угодно может расшифровать подпись, используя открытый ключ, но корректно создать подпись может только владелец личного ключа. Для защиты от перехвата и повторного использования подпись включает в себя уникальное число - порядковый номер.

Аутентификация является одним из самых важных компонентов организации защиты информации в сети. Прежде чем пользователю будет предоставлено право получить тот или иной ресурс, необходимо убедиться, что он действительно тот, за кого себя выдает. При получении запроса на использование ресурса от имени какого-либо пользователя сервер, предоставляющий данный ресурс, передает управление серверу аутентификации. После получения положительного ответа сервера аутентификации пользователю предоставляется запрашиваемый ресурс. При аутентификации используется, как правило, принцип, получивший название "что он знает", - пользователь знает некоторое секретное слово, которое он посылает серверу аутентификации в ответ на его запрос. Одной из схем аутентификации является использование стандартных паролей. Эта схема является наиболее уязвимой с точки зрения безопасности - пароль может быть перехвачен и использован другим лицом. Чаще всего используются схемы с

применением одноразовых паролей. Даже будучи перехваченным, этот пароль будет бесполезен при следующей регистрации, а получить следующий пароль из предыдущего является крайне трудной задачей. Для генерации одноразовых паролей используются как программные, так и аппаратные генераторы, представляющие собой устройства, вставляемые в слот компьютера. Знание секретного слова необходимо пользователю для приведения этого устройства в действие.

В последнее время корпоративные сети все чаще включаются в Интернет или даже используют его в качестве своей основы. Учитывая то, какой урон может принести незаконное вторжение в корпоративную сеть, необходимо выработать методы защиты. Для защиты корпоративных информационных сетей используются брандмауэры. ***Брандмауэр*** - это система или комбинация систем, позволяющие разделить сеть на две или более частей и реализовать набор правил, определяющих условия прохождения пакетов из одной части в другую. Как правило, эта граница проводится между локальной сетью предприятия и Интернетом, хотя ее можно провести и внутри. Однако защищать отдельные компьютеры невыгодно, поэтому обычно защищают всю сеть. Брандмауэр пропускает через себя весь трафик и для каждого проходящего пакета принимает решение - пропускать его или отбросить. Для того чтобы брандмауэр мог принимать эти решения, для него определяется набор правил. Брандмауэр может быть реализован как аппаратными средствами (то есть как отдельное физическое устройство), так и в виде специальной программы, запущенной на компьютере. Как правило, в операционную систему, под управлением которой работает брандмауэр, вносятся изменения, цель которых - повышение защиты самого брандмауэра. Эти изменения затрагивают как ядро ОС, так и соответствующие файлы конфигурации. На самом брандмауэре не разрешается иметь разделов пользователей, а следовательно, и потенциальных дыр - только раздел администратора. Некоторые брандмауэры работают только в однопользовательском режиме, а многие имеют систему проверки целостности программных кодов. Брандмауэр обычно состоит из нескольких различных компонентов, включая фильтры или экраны, которые блокируют передачу части трафика. Все брандмауэры можно разделить на два типа: пакетные фильтры, которые осуществляют фильтрацию IP-пакетов средствами фильтрующих маршрутизаторов; серверы прикладного уровня, которые блокируют доступ к определенным сервисам в сети. Таким образом, брандмауэр можно определить как набор компонентов или систему, которая

располагается между двумя сетями и обладает следующими свойствами: - весь трафик из внутренней сети во внешнюю и из внешней сети во внутреннюю должен пройти через эту систему;- только трафик, определенный локальной стратегией защиты, может пройти через эту систему. В таком случае система надежно защищена от проникновения.

ЗАКЛЮЧЕНИЕ

Несмотря на существенные угрозы, исходящие из интернета, реально создать эффективно работающую систему безопасности. Первое что нужно сделать провести IT-аудит безопасности данных, подключить программы на ПК, позволяющие сохранить конфиденциальную и любую другую важную для бизнеса или частной жизни информацию. Технических средств и методик более чем достаточно, также можно обеспечить своей компании мониторинг IT-инфраструктуры. Весь вопрос – в желании и возможности их применять.

REFERENCES

1. Баранова Е.К. Информационная безопасность и защита информации: Учебное пособие/ Е.К.Баранова, А.В.Бабаш. –М.:Риор, 2018. – 400с.
2. Мельников В.П., Защита информации: Учебник/ В.П.Мельников. – М.: Академия. 2019. – 320 с.
3. Шаньгин В.Ф., Информационная безопасность и защита информации/ В.Ф.Шаньгин. – М.: ДМК, 2014. – 702 с.
4. Семенко В.А. Информационная безопасность: Учебное пособие/ В.А.Семенко. – М.: МГИУ, 20147. – 277 с.
5. Тайлаков Н.И. Информатика и информационные технологии: Учебник для учащихся 11 классов/ Н.И.Тайлаков, А.Б.Ахмедов, М.Д.Пардаева, А.А.Абдуганиев, У.М.Мирсанов. – Ташкент. 2018. -90 с., 107 с.

Интернет ресурсы:

1. http://bourabai.kz/einf/chapter117.htm
2. https://sky-dynamics.ru/stati/metody-i-sredstva-zashhity-informacii-v-internete/
3. https://integrus.ru/blog/it-decisions/metody-sredstva-tehnologii-zashhity-informatsii-v-seti-internet.html