РАЗДЕЛ IV. ИНФОРМАТИКА И ВЫЧИСЛИТЕЛЬНАЯ ТЕХНИКА

Батчаева З.Б., Хачирова Ф.М., Урtenова К.К., Кундохова К.Р.

Обеспечение информационной безопасности и защита персональных данных

ФГБОУ ВО «Северо-Кавказская Государственная академия»

(Россия, Черкесск)

doi: 10.18411/trnio-11-2021-36

Аннотация

В статье рассматриваются определение информационной безопасности, виды и угрозы информационной безопасности, способы применяемых мер для обеспечения защиты информации.

Ключевые слова: информационная безопасность, информация, угроза, компьютер, защита данных.

Abstract

The article discusses the definition of information security, types and threats to information security, methods of applied measures to ensure the protection of information.

Keywords: information security, information, threat, computer, data protection.

Виртуальная жизнь зачастую вытесняет настоящее существование. Почти у каждого человека есть смартфон, который хранит персональные данные..

Но также, как и в реальной жизни, в интернете существуют грабители, жулики, мошенники. К сожалению, не все задумываются о безопасности собственных сведений, не соблюдают и не подразумевают о правилах использования профилями в сети. Главной причиной взломов, как отмечают специалисты, является невнимательность и неграмотность пользователей. Чтобы обезопасить персональные данные нужно прибегнуть к информационной безопасности.

Под информационной безопасностью (ИБ) следует понимать защиту интересов субъектов информационных отношений.

Защита информации - это комплекс мероприятий, направленных на обеспечение информационной безопасности.

Информационная безопасность делится на следующие виды:

- защита корпоративной сети;
- защита корпоративной электронной почты;
- антивирусная защита;
- защита от DDoS;
- защита от утечки информации.

Знание возможных угроз, а также уязвимых мест защиты, которые эти угрозы обычно эксплуатируют, необходимо для того, чтобы выбирать наиболее экономичные средства обеспечения безопасности.

Угроза информационной безопасности — совокупность условий и факторов, создающих опасность нарушения информационной безопасности. [1]

Попытка осуществления угрозы называется «атакой», а тот, кто осуществляет эту попытку, называется «злоумышленником».

Одним из таких угроз информационной безопасности является хакерская атака.

Хакерская атака — это комплекс действий, направленных на поиск уязвимостей в цифровых системах, например на компьютерах, смартфонах, планшетных устройствах или даже целых компьютерных сетях.[2]

Очень часто хакеры используют взломанные профили для того, чтоб перепродать пароли, рассылать спам, для вымогательства и др. Личные сведения также могут быть получены мошенниками, которые практикуют "фишинг" - пользователь, сам того не понимая и не подозревая, скидывает, свою персональные данные, даже не догадываясь о возможных последствиях. Одной из наибольших опасностей может быть хищение ваших паролей, или логинов с целью входа в онлайн-банк и дальнейшей кражи средств. Также для сбора данных могут быть использованы вредоносные программы. Поэтому очень важно всегда быть внимательным и ответственно относиться к вопросам безопасности.

Для повышения защиты своих социальных сетей, нужно понять на какие виды делится хакерская атака и как с ними бороться.

Виды кибератак:

1. Атаки MitM.

Иными словами - атака с перехватом.

Она возникает, когда хакер пытается перехватить связь между двумя сторонами (веб-сервером и пользовательским браузером), чтобы наблюдать за жертвой, похитить личные сведения либо учетные данные, передаваемые согласно по сети.

Для предотвращения таких атак при доступе к сети из незащищенной общедоступной точки доступа Wi-Fi прибегают к виртуальной частной сети (VPN), обеспечивающая безопасное соединение с шифрованием данных.

2. Отказ в обслуживании(Dos, Ddos).

Атаки такого типа перегружают системы, сайты трафиком для нарушения или прекращения их обслуживания, чтобы сделать его неприступным для посетителей. В результате перегруженного сервера сайт не может отвечать на запросы пользователей и прекращает свою работу.

Для предотвращения именно таких атак необходимо уменьшить трафик с помощью CDN, балансировщика нагрузки, масштабируемых ресурсов

3. Парольные атаки.

В этом типе кибератаки хакер пытается взломать пароль пользователя. Есть много разных способов для взламывания пароля, в том числе атака грубой силы, атака по словарю, атака по радужной таблице, заполнение учетных данных, распыление паролей, атака кейлоггера.

Для предотвращения взлома паролей рекомендуется настроить функцию блокировки учетной записи при авторизации, которая автоматически блокирует доступ к устройству, веб-сайту или приложению после определенного количества попыток ввода неверного пароля.

4. Вредоносное ПО.

Вредоносное ПО - это такие виды программного обеспечения, которые выполняют вредоносные задачи на устройстве с целью получения злоумышленником личных или других ценных данных, прерывания работы системы, вымогательства у жертвы денежных средств.

Вредоносное ПО активируется и заражает компьютер после его загрузки.

Для защиты устройства от такого типа атак устанавливают антивирусные программы, популярные из которых – Eset NOD32, Антивирус Касперского, Avast!, Symantec Norton Anti-Virus, McAfee VirusScan и др. Антивирусы замечают вирусные программы, предупреждают о возможных и скрытых угрозах во всплывающем окне и удаляют их.

Чтобы обеспечить информационную безопасность государство ведет постоянную борьбу против внутренних и внешних угроз информационного пространства страны. В результате сформулированы базовые принципы и основные меры информационной безопасности, которые должны обеспечить:

- целостность данных – защиту от сбоев, ведущих к потере информации, а также неавторизованного создания или уничтожения данных;
- конфиденциальность информации и одновременно ее доступность для всех авторизованных пользователей [3].

Для того чтобы обезопасить личную информацию, специалисты советуют повышать компьютерную грамотность и следовать нескольким важным требованиям.

1. Нельзя переходить по сомнительным ссылкам.

При переходе вы можете занести вредоносное ПО в свой компьютер, которое предоставит хакерам ваши данные.

Чтобы не подвергаться к риску, старайтесь заходить на сайты с хорошей репутацией.

2. Скачивание фальшивого антивирусного ПО.

Довольно каждый пользователь сталкивался с всплывающими предупреждениями о том, что ваш компьютер окажется под угрозой, если вы немедленно не скачаете бесплатное антивирусное ПО. Этого ни в коем случае нельзя делать, ведь один клик мыши по этой ссылке может заблокировать использование на компьютере защитных решений.

3. Использование слабых паролей.

Пароли могут быть легко угаданы злоумышленником, если не принять мер предосторожности. Ваш пароль должен содержать и цифры, и знаки препинания, и заглавные и строчные буквы. Избегайте использования каких-либо слов или комбинаций слов, имен и т.д. Лучше всего использовать пароль, каждый символ которого соответствует какому-то слову. Обычно следует иметь различные пароли для различных учетных записей, но не в таком количестве, чтобы вы не смогли запомнить их. [4]

4. Хранение всех своих паролей в системе.

Это ни в коем случае нельзя делать, потому что если вашу систему взломают, то у злоумышленников будет доступ ко всем вашим паролям и они смогут проникнуть в другие ваши данные.

Для обеспечения защиты персональных данных следует предпринимать следующие меры.

1. Нужно зашифровать всю важную информацию.
2. Использовать антивирусные программы и вовремя их обновлять.
3. Не скачивать подозрительные приложения.
4. Использовать протокол HTTPS.
5. Ставить надежные пароли.
6. Включить двойную аутентификацию.

Надо понимать, что никто не застрахован от кибератак и утечки информации. Чтобы не попасться на взлом злоумышленников и обеспечить безопасность своих данных, необходимо придерживаться вышеизложенных элементарных мер предосторожности при работе с персональным компьютером и сети интернет. Нужно помнить, если вы стали жертвой мошенников, обязательно принимайте необходимые меры, иначе ваши личные сведения могут быть использованы в самых различных целях.

1. Википедия https://ru.m.wikipedia.org/wiki/Угрозы_информационной_безопасности
2. Хакерские атаки <https://ru.malwarebytes.com/hacker/>
3. Белов Е. Б., Лось В. П. Основы информационной безопасности. М. : Горячая линия : Теле- ком, 2006.
4. Скембрей Д., Мак-Клар С. Секреты хакеров. Безопасность Microsoft Windows Server – Hacking Exposed Windows Server – М.: «Вильямс», 2007. – С. 512.

Вавилов В.А.

Асимптотический анализ RQ-системы с вызываемыми и возвратными заявками в случайной среде

*Национальный исследовательский Томский государственный университет
(Россия, Томск)*

doi: 10.18411/trnio-11-2021-37

Аннотация

В работе предложена математическая модель RQ-системы с вызываемыми и возвратными заявками в случайной среде, моделируемой цепью Маркова с непрерывным