УДК 004

ЗАЩИТА ИНФОРМАЦИИ В КОМПЬЮТЕРНЫХ СЕТЯХ

Андрей Алексеевич Хохлов
студент
garlic142@gmail.ru
Наталия Владимировна Пчелинцева
старший преподаватель
natas79@mail.ru
Владислава Михайловна Ворошилова
студент
voroshilova.vladislava@inbox.ru
Алла Борисовна Лыкова
студент
lukovaalla3@gmail.com
Мичуринский государственный аграрный университет
г. Мичуринск, Россия

Аннотация. В статье уделяется внимание защите информации в сети Интернет. Рассматриваются основные проблемы утечки информации в руки злоумышленников и механизмы достижения максимально безопасного пользования данными.

Ключевые слова: данные, защита, информация, информационная безопасность, аутентификация, несанкционированный доступ.

На сегодняшний день самой развитой системой передачи, хранения и обмена информацией служит компьютерная сеть. Вопрос в обеспечении безопасности данных занимает важное место в современном мире, поскольку численность и масштабы киберпреступлений увеличиваются с каждым днем. В октябре 2021 года компания Check Point Software Technologies сообщила результаты анализа актуальных киберугроз по всему миру. Анализ показал, что число кибератак в 2021 году выросло на 40% по сравнению с 2020 годом. В России количество атак увеличилось на 54% [1].

Операционные системы защищены новейшими системами защиты, которые позволяют противодействовать множеству внешних угроз. Но даже самые защищенные системы не идеальны и также могут дать сбой, тем самым подставив под удар всю хранимую информацию.

Вся информационная безопасность построена на обеспечении условий, показанных на рисунке 1.

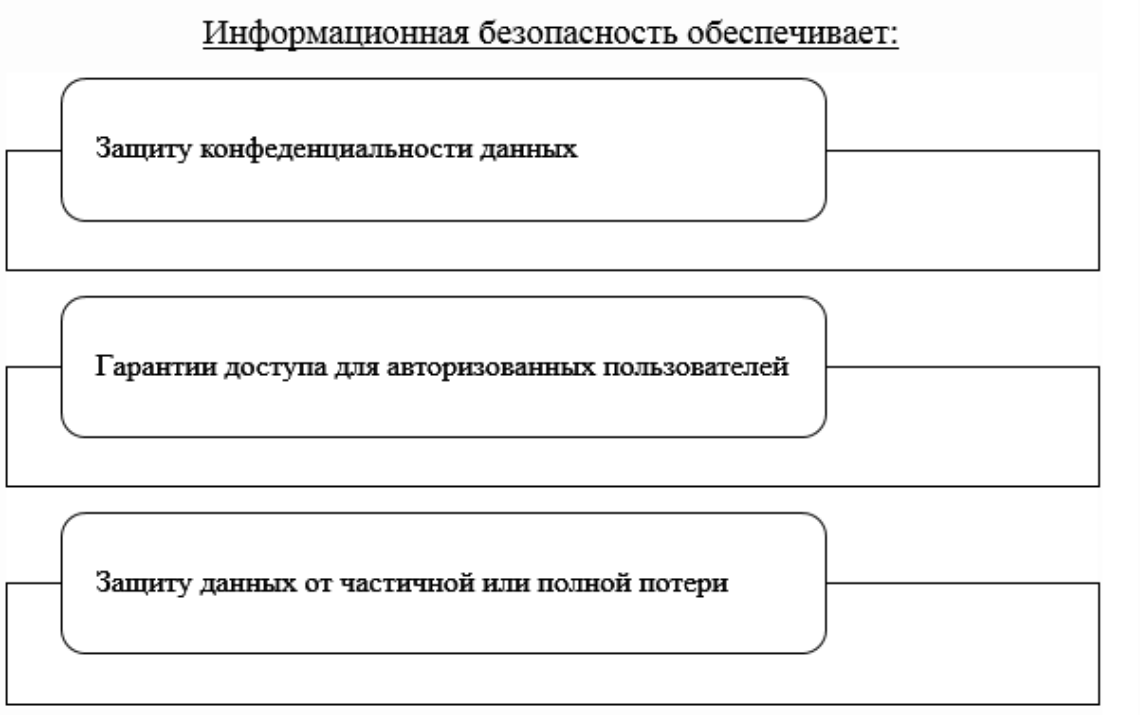

Рисунок 1 – Условия, обеспечивающие информационную безопасность

Если же брать банковскую или правоохранительную систему, то здесь стоит говорить о более совершенном уровне защиты, нежели чем у простых пользователей интернета.

Создание безопасной среды для хранения данных достигается путем обработки критической информации. В свою очередь критическая информационная инфраструктура (КИИ) – это система ключевых сфер жизнедеятельности государства и общества в целом, основанная на информационных системах и телекоммуникативных сетях, максимально отвечающая требованиям задач любого уровня скрытности, от служебного до коммерческого.

Также не стоит забывать и обращать свое внимание на временное отсутствие доступа к аккаунту или перебои в работе, это может быть вызвано несанкционированным доступом к данным.

Основные проблемы в процессе защиты информации:

1. Несанкционированный доступ: скачивание пиратского ПО, работа с посторонними файлами.
2. Неправильное сохранение и разрешение доступа к архивам.
3. Ошибки технического штата и пользователей сетевого ресурса: случайное искажение, либо уничтожение информации, некорректное пользование программными продуктами.
4. Нарушения работы системного оборудования: сбои в жестком диске, системе архиваций, нарушение функционирования серверов и так далее.
5. Уничтожение информации и намеренное скачивание программ без разрешения пользователя: вирусы, скаченные вместе с файлами с неизвестных сайтов, ошибки в системе безопасности.

Все вышеперечисленные проблемы требуют незамедлительного устранения источника проблемы и усиления системы безопасности, использование антивируса.

Для полной конфиденциальности разработаны дополнительные средства защиты информации:

1. Аппаратные (антивирусные программы, брандмауэры, устройства шифрования протоколов).

2. Программные (сетевой мониторинг, архивация данных, идентификация и аутентификация пользователя, управление доступом).

3. Административные (ограничение доступа в помещения, разработка планов действий при ЧС и стратегии безопасности компании).

Комбинация данных методов несет в себе большую эффективность, чем каждый из них отдельно [2].

Одним из самых простых и легких вариантов защиты данных является использование антивируса. В задачи системы антивируса входит недопущение к данным несанкционированного пользователя или сторонней программы Подобные программы обнаруживают вирусы на стадии скачивания и предупреждают об этом пользователя, но если же вирус попал на компьютер, то проверка позволит обнаружить его и удалить. Оптимальным для сохранения системных сведений будет использование комбинации программного и аппаратного барьера. Чаще всего это специализированные платы для борьбы с вирусами.

Одной из главных задач по защите информации является запрет несанкционированного доступа. С этой целью в операционных системах используется такие функции как запрос разрешения на открытие или изменение того, или иного файла, документа. Причины утечки информации:

1. Оставшийся открытый доступ после разрешенного запроса.
2. Предоставления данных третьим лицам.
3. Взлом системы безопасности.
4. Несвоевременное сканирование системы на наличие вирусов.
5. Ввод данных на сайтах с похожим адресом.
6. Программные ловушки.

С целью защиты информации проводят целый ряд организационных мероприятий, которые заключаются, прежде всего, в ограничении доступности зданий и офисов, где проводится работа с информацией. Все носители информации, журналы регистрации и учета необходимо хранить в закрытых сейфах. При передаче секретных сведений по

каналам связи лучше использовать криптографическое кодирование. Нужно следить за тем, чтобы все отработанные устройства и носители, содержащие ценные данные, были вовремя уничтожены.

К организационно-техническим средствам защиты можно отнести устройства независимого блока питания для системы обработки ценных файлов, оснащение входных дверей кодовыми замками и использование ЖК или плазменных дисплеев с высокочастотным излучением электромагнитных импульсов. Кроме того, отправляя оргтехнику в ремонт, нужно стереть все имеющиеся данные.

Технические защитные средства будут включать в себя постоянную охрану помещения, содержащих в себе ценную информацию, а также в экстренном случае блокировку информации и использование защитных ключей.

Способы защиты информации:

1. Шифрование с помощью криптографии. Эта технология делает документ нечитаемым, и доступ к данным можно получить только использую ключ. Работает криптография за счет двух понятий – это алгоритм, создающий кодировку и ключ, позволяющий расшифровать информацию.

Схемы шифровки: симметричная (один ключ для отправителя и получателя) и асимметричная (ключ открытого доступа).

2. Использование электронно-цифровой подписи, содержащей уникальный ключ (номер) человека.

3. Аутентификация пользователей. Самый распространённый способ защиты данных в сети. Сервер принимает запрос на получение информации, передает его другому серверу, который отвечает за аутентификацию, и только после проверки пользователь получает доступ.

Разумно использовать одноразовый вход в систему, ведь даже при получении кода третьими лицами, доступ при повторном входе в профиль будет невозможен, так как потребуется ввести новый код доступа.

4. Защита брандмауэрами. Все крупные корпорации подключены к сети, что делает её уязвимой для утечки данных. Для защиты от утечек используют

брандмауэры или по-другому сетевые экраны. Они разделяют трафик на несколько потоков и обозначают обмен данными из одного потока в другой. После проверки каждого пакета он решает, пропускать его или нет.
Зависит это от алгоритма, прописанного в правила брандмауэра [3].

Брандмауэр состоит из нескольких элементов:

1. Пакетный – фильтрация происходит за счет маршрутизатора;
2. Прикладной – блокирует доступ к отдельным сетевым ресурсам.

Стоит также отметить защищенный протокол HTTPS – это безопасный протокол передачи данных, который шифрует их с помощью криптографических протоколов SSL и TLS, т.е. цифровыми подписями сайта. Перед установкой защищённого соединения, протокол сначала запрашивает у центра сертификации подлинность документа, а после проверки устанавливает соединение и начинается обмен данными. Он является расширенной версией протокола HTTP (HyperText Transfer Protocol), использующегося для передачи гипертекста (с перекрестными ссылками) и с одним большим недостатком - незащищённостью. Данные с помощью этого протокола передаются в незащищённом виде, и злоумышленник может получить к ним доступ [4].

Подводя итоги, стоит сказать, что порой простые упущения в системе безопасности могут нанести большой ущерб, как компании, так и отдельному пользователю. Даже простые меры предосторожности: установка антивируса, настройка разрешений, скачивание приложений с официальных сайтов, обращения внимания на адрес ссылки сайта поможет в несколько раз снизить риск утечки информации и потери доступа к ним.

Список литературы:

1. Гущина А.А., Пчелинцева Н.В., Шацкий В.А. Применение искусственного интеллекта в обеспечении безопасности данных // В сборнике: Инженерное обеспечение инновационных технологий в АПК. материалы Международной научно-практической конференции. Мичуринск-наукоград РФ. 2021. С. 79-81.

2. Корелина А. Ученые научили искусственный интеллект определять сарказм в постах пользователей. / СекретФирмы. – URL: https://secretmag.ru/technologies/uchyonye-nauchili-ii-opredelyat-sarkazm-v-postakh-polzovatelei.htm

3. Мамедов Р. Защита персональных данных в социальных сетях // Information Security / ITsec.Ru. – URL: http://www.itsec.ru/articles2/pravo/zaschita-personalnyh-dannyh-v-sotsialnyh-setyah/

4. Ярославцева К.А., Пчелинцева Н.В., Чепраков И.В., Картечина Н.В. Этические проблемы цифровых технологий// В сборнике: Инженерное обеспечение инновационных технологий в АПК. Материалы Международной научно-практической конференции. Под общей редакцией И.П. Криволапова. Мичуринск-наукоград. 2022. С. 255-258.

UDC 004

INFORMATION PROTECTION IN COMPUTER NETWORKS

Andrey Al. Khokhlov
student
garlic142@gmail.com
Natalia V. Pchelintseva
Senior Lecturer
natas79@mail.ru
Vladislava M. Voroshilova
student
voroshilova.vladislava@inbox.ru
Alla B. Lykova
student
lukovaalla3@gmail.com
Michurinsk State Agrarian University

Michurinsk, Russia

Annotation. The article focuses on the protection of information on the Internet. The main problems of information leakage into the hands of intruders and mechanisms for achieving the most secure use of data are considered.

Keywords: data, protection, information, information security, authentication, unauthorized access.

Статья поступила в редакцию 03.05.2024; одобрена после рецензирования 13.06.2024; принята к публикации 27.06.2024.

The article was submitted 03.05.2024; approved after reviewing 13.06.2024; accepted for publication 27.06.2024.