УДК 004.056

ЗАЩИТА ЦИФРОВОЙ ИНФОРМАЦИИ

Шидловский Николай Анатольевич
Студент,
ТИ(ф)ФГАОУ ВО «СВФУ им М.К. Аммосова» в г. Нерюнгри

Зарипова Мария Юрьевна
Ст. преподаватель,
ТИ(ф)ФГАОУ ВО «СВФУ им М.К. Аммосова» в г. Нерюнгри

В статье рассматривается актуальная проблема защиты цифровой информации в современном обществе. В ней подчеркивается важность защиты как личной, так и организационной информации, утечка которой может привести к серьезным негативным последствиям, включая финансовые потери, репутационный ущерб и даже полный развал предприятия. Также описываются различные виды цифровой информации и анализируются основные методы ее защиты. Представлен краткий обзор ключевых аспектов защиты информации предоставляя читателю базовые знания о важности этой проблемы и основных методах обеспечения информационной безопасности в современном мире.

Ключевые слова: защита, брандмауэры, цифра, цифровая информация**,** аутентификация, кибербезопасность, пароль, антивирусные программы, двухфакторная аутентификация, криптография, 2FA, блокчейн, IPS, IDS, электронная подпись.

*****

Защита информации, в том числе цифровой – важная часть современного общества. Информация может быть, как личной, маловажной, так и информацией организационной, которая имеет огромную важность и ценность. Любая утечка, кража важной для организации информации может привести к негативным последствиям, будь то убытки, потеря клиентов, ухудшение репутации или даже полному развалу предприятия. Аналогично утечка личной информации приведет к серьезным последствиям: разглашению конфиденциальных данных, шантажу и т. д.

Цифровая информация – это разновидность информации в электронном виде, являющаяся объектом права и участвующая в гражданском и торговом обороте, фиксация, хранение и передача которой обеспечиваются исключительно цифровыми (информационными) технологиями, при этом она технологически едина (неделима) и не обладает материально выраженными характеристиками.

Рассмотрим виды цифровой информации: цифровое телевидение, компьютер, смартфон, данные, хранящиеся на дисках и в облачных сервисах. Сюда также можно добавить цифровую валюту, токены (криптовалюты), электронную подпись, аккаунты и даже дезоксирибонуклеиновая кислота (ДНК человека) – это естественную форму хранения цифровых данных. Хотя цифровые сигналы обычно ассоциируются с двоичными электронными системами, цифровая информация появилась давно. Например, письменный текст, использующий алфавит, счеты, маяк также являются формами цифровой информации.

Существует огромное множество способов защиты информации в зависимости от ее типа и вида. Рассмотрим одни из самых основных видов защиты информации:

1. Использование двухфакторной аутентификации (2FA) в приложениях и сервисах, которые ее поддерживают. Используется во многих электронных ресурсах. 2FA – это дополнительный уровень защиты ваших данных и вашего аккаунта. При ее использовании после ввода логина и пароля от аккаунта на каком-либо ресурсе пользователю потребуется ввести код из смс, отправленный на номер мобильного телефона или почту владельца аккаунта, либо код, сгенерированный в специальном

приложении. Кроме данных видов подтверждения могут использоваться и другие, к примеру, отпечаток пальца или Face ID (лицевая биометрия).

2. Использование надежных паролей. Пароль должен быть сложным, уникальным. Часто к паролям относят такие требования как: наличие заглавных и прописных букв, соблюдение определенной длины пароля (часто больше 12 символов), наличие цифр, использование в пароле специальных символов таких как «!;%:.></?\» и т п. Кроме того, пароли нельзя нигде записывать и передавать третьим лицам.

3. Регулярная проверка и использование антивирусного программного обеспечения. Один из лучших способов защиты от вирусов: троянов, шпионов – это установка антивирусного программного обеспечения, которое будет предупреждать вас об возможной опасности. Например, на компьютерах с операционной системой Windows 10 можно использовать встроенный антивирус Microsoft Defender, либо приобрести другое антивирусное программное обеспечение.

4. Криптография – шифрование информации от незаконного использования с использованием криптографического алгоритма и ключа. Цель криптографии заключается в блокировании несанкционированного доступа к информации от людей или компаний путем шифрования содержания сообщений. Основной процесс криптографии заключается в зашифровке информации отправителем и ее передаче получателю, который может расшифровать данные с помощью определённого ключа или правил дешифровки. Не имея ключа или правил, адресат видит зашифрованные данные в виде неопознанного файла или бессвязного набора символов, что делает их не возможными для понимания. Кроме того, криптография обеспечивает целостность информации, гарантируя адресату и ремитенту уверенность в том, что в процессе передачи данных сообщение не подвергалось изменениям.

5. Работа только с защищенными, проверенными сетями интернет (Wi-Fi). Сети могут быть небезопасными и представлять угрозу для конфиденциальности и безопасности ваших данных. Бесплатные сети часто используются хакерами для перехвата вашей информации, которая включает в себя личные данные, пароли и банковские реквизиты. Кроме того, подключение к открытым сетям может быть опасным из-за возможности подключения к поддельным точкам доступа, созданным хакерами для отслеживания онлайн-активности. Рекомендуется использовать защищенные сети с шифрованием данных, например, с защитой WPA или WPA2, чтобы обезопасить вашу информацию от несанкционированного доступа.

6. Регулярное обновление используемых программ. Нередко обновление приложений не происходит автоматически. Поэтому стоит следить за появлением новых версий программного обеспечения. В новых версиях часто улучшаются функции, устраняются слабые места, через которые хакеры могут получить доступ к вашим данным.

7. Скачивание и использование нелегальных программ. Не стоит скачивать и использовать на своем персональном компьютере программы с торрентов и непроверенных сайтов, данные программы могут оказаться программами-троянами. Помимо этого, пиратское программное обеспечение нарушает закон о защите авторского права и может повлечь за собой административную или даже уголовную ответственность. Вместо скачивания и использования нелегальных программ следует приобретать программы только у официальных и надежных источников, либо можно воспользоваться другими, бесплатными программными продуктами с открытым и безопасным исходным кодом.

8. Применение брандмауэра для фильтрации нежелательного трафика. Брандмауэр представляет собой встроенный инструмент в операционной системе Windows, который управляет доступом к персональному компьютеру и сетевым ресурсам. Он ограничивает внешним соединениям доступ к компьютеру и регулирует передачу данных между сетями. Работая на уровне операционной системы брандмауэр способен блокировать определённые порты для исходящих и входящих соединений. Однако важно понимать, что брандмауэр – не является защитой от всех угроз в интернете. С некоторыми видами опасностей он не справится. Также он может защитить компьютер от шпионского программного обеспечения, взлома, вирусов и атак типа

(DDoS-атак), при которых множество компьютеров одновременно перегружают систему запросами. От некоторых атак и брандмауэр не сможет уберечь, например, от угроз уже присутствующих на компьютере, от входящего трафика через VPN и от некоторых сложных типов вирусов. Поэтому важно использовать все доступные инструменты безопасности в комплексе – только так вы сможете максимально защитить своё устройство и данные хранящиеся на нем.

9. Использование электронной подписи. Электронная подпись – это часть документа, позволяющая подтвердить подлинность документа через криптографические алгоритмы. Обеспечивая тем самым невозможность подделки и целостность передаваемой информации. Подпись содержит в себе несколько видов ключей, одни из которых, открытый и закрытый, открытый ключ называют сертификатом, а закрытый – криптографической частью. Уже некоторое время электронная подпись стала частью портала «Госуслуги», а также приложения «Госключ». В данных сервисах она используется для онлайн подачи заявлений, подачи услуг, получения справок и многого другого.

10.Применение блокчейн технологий. Блокчейн – это технология децентрализованного хранения данных, где информация разделена на блоки (на англ. block), каждый из которых связан с предыдущим, образуя цепочку (на англ. chain). Изменение данных в предыдущих блоках является крайне ресурсоёмким и практически невозможным, поэтому все, что попадает в блокчейн, остается неизменным. Эта технология используется, например, в здравоохранении, где организации хранят в блокчейне медицинские карты пациентов.

11. IPS и IDS-системы. Технологии предотвращения и обнаружения вторжений IPS и IDS-системы (от англ. соответственно Intrusion Prevention System и Intrusion Detection System) оказывают значительное влияние на безопасность данных. IDS-системы отслеживают сетевой трафик и выявляет необычную активность, которая указывает на возможное нарушение безопасности. Например, попытки взлома сети или атаки на серверы. IPS-системы в свою очередь не только фиксируют потенциальные угрозы безопасности, но и принимают активные меры для их нейтрализации. Например, при скачивании файла инструменты IPS-системы сначала проверят вредоносный файл или нет, а затем позволят пользователю скачать файл, если он не представляет опасности для компьютера. Иначе предупредят пользователя об угрозе и заблокируют скачивание, если файл является вредоносным. Кроме того, данные системы могут блокировать уникальные идентификаторы устройств (ip-адреса) представляющих опасность для пользователя.

Исходя из всего выше сказанного можно сделать вывод, что в современном мире невозможно обойтись без защиты цифровой информации, ведь она повсюду окружает нас, начиная от нашей личной информации, заканчивая информацией предприятий, организаций, государств.

Утечка, кража информации могут иметь негативные последствия. Для предотвращения таких последствий необходимо использовать способы защиты информации. Эти способы включают в себя: криптографию, блокчейн, технологии обнаружения и предотвращения вторжений, двухфакторную аутентификацию, использование надежных паролей и многие другие способы защиты важной информации. Только все эти методы в совокупности способны обеспечить достойный уровень безопасности личной информации или информации организаций и предприятий.

В настоящее время, когда информационные технологии развиваются довольно стремительно и с каждым днем растет не только количество способов защиты информации, но и количество хакеров, которые занимаются кражей конфиденциальной информации. Поэтому следует внедрять уже имеющиеся способы защиты информации и способствовать дальнейшему их развитию и улучшению.

Список использованных источников

1. Цымбал Федор Алексеевич ЗАЩИТА ЦИФРОВОЙ И АНАЛОГОВОЙ ИНФОРМАЦИИ // Столыпинский вестник. 2022. №4. URL: https://cyberleninka.ru/article/n/zaschita-tsifrovoy-i-analogovoy-informatsii (дата обращения: 05.05.2024).

2. Боярко, М. В. Сравнение методов защиты цифровой информации / М. В. Боярко, В. А. Ковтун, А. А. Ковтун // Актуальные аспекты развития науки и общества в эпоху цифровой трансформации: сборник материалов XII Международной научно-практической конференции, Москва, 05 декабря 2023 года. – Москва: Алеф, 2023. – С. 137-142. – EDN AMDHQY. (дата обращения: 04.05.2024).

3. Борисов, Р. С. Информатика : учебное пособие / Р. С. Борисов, А. С. Скотченко. – Москва : РГУП, 2023. – 334 с. – ISBN 978-5-00209-051-8. – Текст : электронный // Лань : электронно-библиотечная система. – URL: https://op.raj.ru/spo/1164-bor-skot-inf (дата обращения: 04.05.2024).

4. Прокопов, Д. С. Защита информации. Виды защиты информации / Д. С. Прокопов // Передовые инновационные разработки. Перспективы и опыт использования, проблемы внедрения в производство : сборник научных статей по итогам второй международной научной конференции, Казань, 30 марта 2019 года. – Казань: ООО «Конверт», 2019. – С. 133-134. – URL: https://elibrary.ru/item.asp?id=37355656 (дата обращения: 04.05.2024).

5. Балдов Дмитрий Валентинович, Петрова Светлана Юрьевна, Лебедев Александр Анатольевич ИСПОЛЬЗОВАНИЕ ТЕХНОЛОГИИ БЛОКЧЕЙН ДЛЯ ЗАЩИТЫ ДАННЫХ // International Journal of Open Information Technologies. 2021. №9. URL: https://cyberleninka.ru/article/n/ispolzovanie-tehnologii-blokcheyn-dlya-zaschity-dannyh (дата обращения: 23.05.2024).

PROTECTION OF DIGITAL INFORMATION

Shidlovsky N. A., Zaripova M. Y.

The article deals with the actual problem of digital information protection in modern society. It emphasizes the importance of protecting both personal and organizational information, the leakage of which can lead to serious negative consequences, including financial losses, reputational damage and even the complete collapse of the enterprise. It also describes various types of digital information and analyzes the main methods of its protection. A brief overview of the key aspects of information security is presented, providing the reader with basic knowledge about the importance of this problem and the main methods of ensuring information security in the modern world.

Keywords: protection, firewalls, digital, digital information, authentication, cybersecurity, password, antivirus programs, two-factor authentication, cryptography, 2FA, blockchain, IPS, IDS, electronic signature.