СОВРЕМЕННЫЕ ТЕХНОЛОГИИ ЗАЩИТЫ ИНФОРМАЦИИ

Абдуллаев Эльвин Ахмед оглы

студент, Северный (Арктический) федеральный университет имени М.В. Ломоносова РФ, г. Архангельск

Лыткина Елена Александровна

научный руководитель, канд. техн. наук, доцент, Северный (Арктический) федеральный университет имени М.В. Ломоносова РФ, г. Архангельск

MODERN INFORMATION SECURITY TECHNOLOGIES

Elvin Abdullaev

Student of the Northern (Arctic) Federal University named after M.V. Lomonosov, Russia, Arkhangelsk

Elena Lytkina

Scientific supervisor, Candidate of technical sciences, associate professor, Russia, Arkhangelsk

Аннотация. В статье автор обозначает, что современные технологии защиты информации играют ключевую роль в обеспечении безопасности данных и защите конфиденциальности в условиях стремительно развивающегося цифрового мира, и, подчеркивает важность комплексного подхода к информационной безопасности.

Abstract. In the article, the author points out that modern information security technologies play a key role in ensuring data security and protecting privacy in the rapidly developing digital world, and emphasizes the importance of an integrated approach to information security.

Ключевые слова: информационная безопасность, защита данных, сетевой трафик, данные, устройство, соединение, современные технологии.

Keywords: information security, data protection, network traffic, data, device, connection, modern technologies.

Современные технологии информационной безопасности играют ключевую роль в обеспечении безопасности данных и защите конфиденциальности в быстро развивающемся цифровом мире. С ростом количества кибератак и утечек данных возрастает потребность в эффективных методах защиты информации. Существует множество технологий и подходов, которые помогают минимизировать риски и обеспечить безопасность данных.

Одной из важнейших технологий защиты информации является шифрование. Шифрование данных используется для защиты конфиденциальной информации от несанкционированного доступа. Современные алгоритмы шифрования, такие как AES (Advanced Encryption Standard) и RSA, обеспечивают высокий уровень безопасности за счет использования сложных математических вычислений. Например, AES используется для шифрования данных на устройствах и в сетях, что помогает защитить информацию при передаче и хранении. RSA, в свою очередь, часто используется для обеспечения безопасной передачи данных и аутентификации пользователей.

Еще одним важным аспектом информационной безопасности является использование технологий аутентификации и контроля доступа. Биометрическая аутентификация, такая как распознавание отпечатков пальцев, лица или радужной оболочки глаза, становится все более популярной [1]. Эти методы обеспечивают высокий уровень безопасности, поскольку основаны на уникальных биометрических данных пользователей, которые сложно подделать. Одним из примеров использования биометрической аутентификации является Apple Face ID, который позволяет пользователям разблокировать свои устройства и совершать безопасные платежи.

Виртуальные частные сети (VPN) также играют важную роль в защите информации. VPN создают безопасное соединение между устройствами и серверами, позволяя скрыть пользовательский трафик и данные о местоположении. Это особенно важно при использовании общедоступных сетей Wi-Fi, где данные могут быть легко перехвачены злоумышленниками. Например, NordVPN предоставляет услуги VPN, которые позволяют пользователям безопасно пользоваться Интернетом и защищать свои данные от киберугроз.

Технологии защиты от вредоносного ПО также занимают важное место в современном ландшафте информационной безопасности. Антивирусное и антишпионское программное обеспечение помогает обнаруживать и устранять вредоносные программы, такие как вирусы, троянские кони и шпионское ПО. Примером может служить антивирусное программное обеспечение Касперского, которое обеспечивает комплексную защиту от различных типов киберугроз и предоставляет регулярные обновления для борьбы с новыми видами вредоносного ПО.

Современные технологии информационной безопасности также включают в себя системы обнаружения и предотвращения вторжений (IDS/IPS). Эти системы отслеживают сетевой трафик и анализируют его на предмет подозрительной активности [2]. При обнаружении угрозы IDS/IPS может автоматически принять меры для предотвращения атаки. Например, Snort — популярный инструмент обнаружения вторжений, который используется для мониторинга сетевого трафика и обнаружения аномалий.

Криптографические протоколы, такие как SSL/TLS, обеспечивают безопасную передачу данных в Интернете. Они используются для защиты информации, передаваемой между веб-сайтами и пользователями. Протоколы SSL/TLS шифруют данные, что делает невозможным их перехват злоумышленниками. Например, URL-адрес веб-сайтов с безопасным соединением начинается с «https», что указывает на наличие сертификата SSL/TLS.

Защита данных в облачных сервисах также является важным аспектом современной информационной безопасности. Поставщики облачных услуг, такие как Amazon Web Services (AWS) и Microsoft Azure, предлагают широкий спектр инструментов защиты данных, включая шифрование, управление ключами и многоуровневую аутентификацию. Эти инструменты помогают обеспечить безопасность данных при хранении и передаче в облаке.

Использование технологий блокчейн также становится все более популярным для обеспечения безопасности данных. Блокчейн — это распределенный реестр, обеспечивающий прозрачность и неизменность данных. Это делает блокчейн особенно полезным для защиты данных в финансовых транзакциях, управлении цифровыми активами и других областях. Примером является использование блокчейна в таких криптовалютах, как Биткойн, где каждое изменение данных записывается и проверяется сетью участников, предотвращая возможность мошенничества.

Современные технологии информационной безопасности включают в себя и средства обеспечения безопасности мобильных устройств. Мобильные устройства часто становятся объектом кибератак, поэтому важно использовать надежные методы безопасности, такие как шифрование данных, управление устройствами и защита от вредоносного ПО. Например, Mobile Device Management (MDM) позволяет администраторам управлять мобильными устройствами, обеспечивая защиту данных и контроль над установкой приложений [3].

Одним из новейших подходов к информационной безопасности является использование искусства венного интеллекта (ИИ) и машинного обучения. Эти технологии позволяют анализировать большие объемы данных и выявлять аномалии, которые могут свидетельствовать о наличии киберугроз. Например, системы на основе ИИ могут автоматически обнаруживать и блокировать подозрительную активность, такие как проверка сертификата или распространение патентного ПО. Компания Darktrace использует ИИ для Диптихов и защиты сетей от киберугроз в первое время.

Также важно упомянуть технологии защиты данных на уровне физической занятости. Охрана серверных помещений, использование биометрических замков и систем видеонаблюдения позволяют предотвратить несанкционированный доступ к оборудованию. Эти меры являются важной частью комплексного средства защиты информации и помогают защитить данные от физической угрозы.

В заключение важно отметить, что современные технологии защиты информации играют решающую роль в обеспечении безопасности данных и конфиденциальности в цифровую эпоху. Шифрование, аутентификация, VPN, антивирусное ПО, IDS/IPS, SSL/TLS, облачные технологии, шкаф, защита мобильных устройств, ИИ и защита изображений — все эти методы и инструменты поддерживают разнообразные киберугрозы и обеспечивают безопасность информации. С развитием технологий и форм кибератак важно постоянно совершенствовать методы защиты данных и адаптироваться к новым вызовам в сфере информационной безопасности.

Список литературы:

1. Борлакова М.А., Болатов М.Х. Современные методы и средства защиты информации// Вестник Академии знаний. 2023. №1 (54).

2. Трофимова Н.О. Современные технологии обеспечения информационной безопасности // Экономика и социум. 2016. №9 (28).

3. Столлингс В. Криптография и защита сетей: принципы и практика. 3 - е изд. - М.: Вильямс, 2002. - 671 с.