Имамутдинов Роман Арсенович,
курсант 222 учебной группы,
Филиал Военного учебно-научного центра военно-воздушных сил
«Военно-воздушной академии имени профессора
Н.Е. Жуковского и Ю.А. Гагарина» в г. Челябинске

Ефанов Георгий Дмитриевич,
курсант 222 учебной группы,
Филиал Военного учебно-научного центра военно-воздушных сил
«Военно-воздушной академии имени профессора
Н.Е. Жуковского и Ю.А. Гагарина» в г. Челябинске

Научный руководитель:
Попов Юрий Леонидович,
доцент 1 кафедры тактики,
Филиал Военного учебно-научного центра военно-воздушных сил
«Военно-воздушной академии имени профессора
Н.Е. Жуковского и Ю.А. Гагарина» в г. Челябинске
кандидат исторических наук, доцент, профессор АВН

ПЕРСПЕКТИВЫ РАЗВИТИЯ ЗАЩИТЫ ИНФОРМАЦИИ

Аннотация: в нашей статье рассматриваются перспективы развития защиты информации, ее непосредственное улучшение ввиду добавления новых технологий и смены информационных источников.

Ключевые слова: информация; угроза; защита; угроза; данные; технологии; управление; аутентификация; кибербезопасность; система.

Перспективы развития защиты информации – это динамичная и многогранная область, которая постоянно развивается под влиянием технологического прогресса, новых угроз и меняющихся потребностей бизнеса и общества. Вот некоторые ключевые направления и перспективы:

Искусственный Интеллект (ИИ) и Машинное Обучение (МО) – включает в себя четыре аспекта: автоматизация обнаружения угроз, адаптивную защиту, анализ поведения пользователей и прогнозирование угроз. Автоматизация обнаружения угроз подразумевает собой, что ИИ и МО используются для анализа больших объемов данных, выявления аномалий и автоматического обнаружения потенциальных угроз в режиме реального времени. Это помогает сократить время реагирования на инциденты и повысить точность обнаружения. Адаптивная защита включает в себя системы безопасности на основе ИИ которые могут адаптироваться к меняющимся угрозам и автоматически корректировать параметры защиты. Анализ поведения пользователей значит что, ИИ может анализировать поведение пользователей, выявлять отклонения от нормы и предупреждать о возможных внутренних угрозах. Прогнозирование угроз имеет в виду, что ИИ может использоваться для прогнозирования будущих угроз на основе анализа исторических данных и текущих тенденций [1].

Блокчейн – это настоящая одноранговая сеть, снижающая зависимость от разного рода посредников. Это повышает эффективность процессов и уменьшает возможность ошибок при вводе данных, а также снижает плату за транзакции. Включает в себя три аспекта: безопасность данных, управление идентификацией и доступом и защита от DdoS-атак.

Безопасность данных: блокчейн может использоваться для хранения и управления данными таким образом, что их невозможно изменить или подделать. Это особенно важно для защиты конфиденциальной информации, такой как финансовые транзакции и медицинские записи.Управление идентификацией и доступом: блокчейн может использоваться для создания децентрализованных систем управления идентификацией и доступом, что повышает безопасность и прозрачность.Защита от DDoS-атак: блокчейн может использоваться для создания устойчивых к DDoS-атакам систем [2].

Квантовая криптография – метод защиты коммуникаций, основанный на принципах квантовой физики. В отличие от традиционной криптографии, которая использует математические методы, чтобы обеспечить секретность информации, квантовая криптография сосредоточена на физике, рассматривая случаи, когда информация переносится с помощью объектов квантовой механики.Включает два аспекта: защита от квантовых компьютеров и квантовое распределение ключей. Защита от квантовых компьютеров: с развитием квантовых компьютеров существующие методы шифрования становятся уязвимыми. Квантовая криптография предлагает новые методы шифрования, которые устойчивы к атакам квантовых компьютеров. Квантовое распределение ключей (QKD): QKD использует законы квантовой механики для безопасного обмена ключами шифрования [3].

Биометрия – автоматическое распознавание индивидов, основанное на их поведенческих и биологических характеристиках. Включает в себя два аспекта: усиление аутентификации и непрерывная аутентификация. Усиление аутентификации: биометрические методы аутентификации (отпечатки пальцев, распознавание лиц, сканирование радужной оболочки глаза) становятся все более распространенными и точными. Они могут использоваться для усиления защиты от несанкционированного доступа к системам и данным. Непрерывная аутентификация: биометрия может использоваться для непрерывной аутентификации пользователей, что позволяет выявлять подозрительную активность в режиме реального времени.

Облачные технологии – модель обеспечения удобного сетевого доступа по требованию к некоторому общему фонду конфигурируемых вычислительных ресурсов, которые могут быть оперативно предоставлены и освобождены с минимальными эксплуатационными затратами или обращениями к провайдеру. Включает в себя три аспекта: безопасность облачной инфраструктуры, шифрование данных в облаке и управление доступом к облачным ресурсам. Безопасность облачной инфраструктуры: обеспечение безопасности облачной инфраструктуры является критически важным для защиты данных, хранящихся в облаке. Шифрование данных в облаке: использование шифрования для защиты данных, хранящихся в облаке, является обязательным условием для обеспечения конфиденциальности. Управление доступом к облачным ресурсам: строгий контроль доступа к облачным ресурсам помогает предотвратить несанкционированный доступ к данным.

Интернет вещей (IoT) – концепция сети передачи данных между физическими объектами, оснащёнными встроенными средствами и технологиями для взаимодействия друг с другом или с внешней средой. Включает в себя три аспекта: безопасность устройств IoT, шифрование данных, передаваемых устройствами IoT, обновление программного обеспечения устройств IoT. Безопасность устройств IoT: защита устройств IoT от взлома и кибератак является критически важной для предотвращения утечек данных и других инцидентов безопасности. Шифрование данных, передаваемых устройствами IoT: шифрование данных, передаваемых устройствами IoT, помогает защитить конфиденциальную информацию от перехвата [4]. Обновление программного обеспечения устройств IoT: регулярное обновление программного обеспечения устройств IoT помогает устранить уязвимости и повысить уровень безопасности.

Автоматизация и оркестрация безопасности – набор инструментов или служб, которые помогают интегрировать и автоматизировать задачи и процессы, связанные с безопасностью. Включает в себя два аспекта: SOAR и XDR. SOAR (Security Orchestration, Automation and Response): платформы SOAR позволяют автоматизировать процессы безопасности, такие как обнаружение угроз, реагирование на инциденты и расследование инцидентов. XDR (Extended Detection and Response): XDR объединяет данные из различных источников безопасности (endpoint, network, cloud) для более эффективного обнаружения и реагирования на угрозы [5].

Zero Trust Security – это концепция информационной безопасности, основанная на отсутствии доверия и политике минимума доступа, необходимого для выполнения задач. Включает в себя два аспекта: минимизация доверия и аутентификация и авторизация для каждого доступа. Минимизация доверия: модель Zero Trust Security предполагает, что никому нельзя доверять по умолчанию, даже если они находятся внутри сети организации. Аутентификация и авторизация для каждого доступа: каждая попытка доступа к ресурсам должна быть аутентифицирована и авторизована, независимо от того, откуда исходит запрос.

Повышение осведомленности и обучение – обучение сотрудников основам кибербезопасности: обучение сотрудников основам кибербезопасности помогает снизить риск фишинговых атак и других инцидентов, связанных с человеческим фактором. Повышение осведомленности о киберугрозах: повышение осведомленности о киберугрозах помогает пользователям принимать более обоснованные решения в области безопасности.

Подводя краткий итог, можно сделать вывод, что перспективы развития защиты информации тесно связаны с технологическим прогрессом и необходимостью противостоять новым угрозам. Развитие ИИ, блокчейна, квантовой криптографии и других технологий открывает новые возможности для защиты данных, но также требует от организаций постоянного обновления знаний и навыков в области кибербезопасности.

Список литературы:

1. Платонов А. В. Машинное обучение: учебное пособие для вузов / А. В. Платонов. – 2-е изд. – Москва: Издательство Юрайт, 2025. – 89 с.;

2. Цихилов А.А. Блокчейн: принципы и основы. – Москва: Издательство Альпина Про, 2019.;

3. Кронберг Д. А. Квантовая криптография учебное пособие / Д.А. Кронберг, Ю.И. Ожигов, А.Ю. Чернявский; МГУ им. М.В. Ломоносова, Фак. вычисл. математики и кибернетики. – Москва: МАКС Пресс, 2011;

4. Баланов А.Н. IoT-решения: принципы, примеры, перспективы. – Москва: учебное пособие для СПО, 2024;

5. Богданов В.В. Защита информации: учебное пособие – Москва: ООО Издательский Дом "Афина", 2021.