«М.А. Гендельманның 110 жылдығына арналған «Сейфуллин оқулары – 19» халықаралық ғылыми-практикалық конференциясының материалдары = Материалы международной научно-практической конференции «Сейфуллинские чтения – 19», посвященной 110 - летию М.А. Гендельмана» - 2023.- Т. II, Ч.I.- С. 340-344.

**УДК 004.056**

# КИБЕРБЕЗОПАСНОСТЬ КАК СОВРЕМЕННАЯ ТЕХНОЛОГИЯ ЗАЩИТЫ ИНФОРМАЦИИ

*Байдильдин М., студент 1 курса*
*Молдабекова А.Ж., старший преподаватель*
*НАО «Казахский агротехнический исследовательский университет им. С.Сейфуллина, г. Астана*

В настоящее время предметом современных информационно-коммуникационных технологий является информация. Область информационно-коммуникационных технологий позволяет осуществлять процессы сбора, хранения, передачи и использования различной информации, способов ее обработки, доставки, получения и использования.

В современном мире информационно-коммуникационные технологии применяются в различных областях профессиональной деятельности, научной и практической работе, для самообразовательных и других целей. Информационные науки связаны со сбором, хранением и анализом данных. Развитие технологий привело к созданию огромных объемов данных, и информационные науки стали играть важную роль в управлении и анализе этих данных.

Год за годом в мире становится все больше угроз и происходит все больше утечек данных. Чаще всего утечке данных подвергаются медицинские и государственные учреждения или организации из сферы розничной торговли. В большинстве случаев причина – действия преступников. Некоторые организации привлекают злоумышленников по понятной причине – у них можно украсть финансовые и медицинские данные. Однако мишенью может стать любая компания, ведь преступники могут охотиться за данными клиентов, шпионить или готовить атаку на одного из клиентов. Очевидно, что масштаб киберугроз будет расширяться, следовательно, глобальные расходы на решения по кибербезопасности будут увеличиваться. По прогнозам Gartner, в целом расходы на кибербезопасность в мире достигнут $188,3 млрд в 2023 году, а к 2026 году превысят $260 млрд. Правительства разных стран борются с преступниками, помогая организациям внедрять эффективные методы кибербезопасности.

В Концепции кибербезопасности (Киберщит Казахстана), утвержденной постановлением Правительства Республики Казахстан от 30 июня 2017 года №

407 под кибербезопасностью понимаются состояние защищенности информации в электронной форме и среды ее обработки, хранения, передачи (электронных информационных ресурсов, информационных систем и информационно-коммуникационной инфраструктуры) от внешних и внутренних угроз, то есть информационная безопасность в сфере информатизации[1].

В современном цифровом мире кибербезопасность стала важнейшим аспектом современных технологий. В связи с растущей зависимостью от Интернета и увеличением использования электронных устройств потребность в кибербезопасности как никогда высока. Кибербезопасность относится к практике защиты электронных устройств, сетей и конфиденциальной информации от несанкционированного доступа, кражи и повреждения. В данной статье рассматривается важность кибербезопасности, типы киберугроз и меры, которые можно предпринять для защиты от кибератак.

По мнению автора, на сегодняшний день кибербезопасность жизненно важна для частных лиц, предприятий и правительств. В последние годы кибератаки стали более частыми и изощренными. Киберпреступники могут украсть конфиденциальную информацию, такую как номера кредитных карт и личную идентификационную информацию, и использовать ее для мошеннических действий. Предприятия также могут пострадать от кибератак, которые могут привести к потере доходов и ущербу для их репутации. Правительства сталкиваются со значительной угрозой национальной безопасности, когда их компьютерные системы подвергаются взлому, что может привести к краже конфиденциальной информации и нарушению работы критической инфраструктуры.

Киберугрозы бывают разных форм. Взлом — один из самых распространенных видов кибератак. Хакеры используют свои технические навыки для получения несанкционированного доступа к компьютерным системам и сетям. Они могут украсть конфиденциальную информацию или получить контроль над устройствами для запуска более серьезных атак.

Вредоносное ПО — еще одна форма кибератаки, которая становится все более распространенной. Вредоносное ПО — это вредоносное программное обеспечение, которое может заражать компьютеры и красть данные, нарушать работу компьютерных систем или даже контролировать устройства. Вредоносное ПО может попасть на компьютеры через вложения электронной почты, загрузки или другие действия в Интернете.

Фишинг — это тип атаки с использованием социальной инженерии, когда злоумышленник выдает себя за надежный источник, например банк или поставщик услуг электронной почты, для получения конфиденциальной информации от жертвы. Фишинговые атаки могут принимать различные формы, включая электронные письма, телефонные звонки и даже текстовые сообщения.

Используя разные формы киберугроз, хакеры за кибератаки на информационную информацию привлекаются у уголовной ответственности.

Комитетом по правовой статистике представлены показатели правонарушений, зарегистрированные в период с 2018 по 2022 года, представлены в диаграмме[2]:


Анализируя показатели, можно сделать вывод, что с 2018 года число зарегистрированных интернет-мошенничеств выросло даже в не в десять, а в несколько десятков раз. Число преступлений с использованием платежных карт выросло в 10 раз, число правонарушений в сфере кредитования — за 3 года в 14 раз.

Далее автор приводит статистику в различных сферах деятельности распределения киберинцидентов по метрикам (объектов атак, методов, последствий) и внутри категорий жертв киберпреступлений[3].


Какие же существует меры защиты от кибератак? Существует несколько мер, которые отдельные лица, предприятия и правительства могут принять для защиты от кибератак. Одним из наиболее важных является своевременное обновление программного обеспечения и операционных систем с помощью последних исправлений безопасности. Компании-разработчики программного обеспечения регулярно выпускают обновления, которые устраняют уязвимости в их продуктах, и отсутствие установки этих обновлений может сделать устройства и сети уязвимыми для атак.

Также важно использовать надежные пароли и включать двухфакторную аутентификацию, когда это возможно. Двухфакторная аутентификация добавляет дополнительный уровень безопасности, требуя от пользователя предоставить вторую форму идентификации, такую как код, отправленный на его телефон, в дополнение к его паролю[4].

Шифрование — еще один важный инструмент в борьбе с кибератаками, который представляет собой процесс преобразования конфиденциальных данных в код, который может быть расшифрован только авторизованными сторонами. Это помогает защитить данные от несанкционированного доступа и кражи.

Брандмауэры и антивирусное программное обеспечение также являются важными компонентами стратегии кибербезопасности. Брандмауэры — это программные или аппаратные устройства, которые отслеживают и контролируют сетевой трафик, а антивирусное программное обеспечение помогает обнаруживать и удалять вредоносные программы с устройств.

В дополнение к перечисленным техническим мерам кибербезопасность также зависит от образования и осведомленности. Отдельные лица и организации должны знать о распространенных киберугрозах и предпринимать шаги для своей защиты. Это включает осторожность при переходе по ссылкам в электронных письмах и сообщениях из неизвестных источников, избегание общедоступных сетей Wi-Fi и регулярное резервное копирование важных данных.

Для снижения вероятности киберугроз в Республике Казахстан необходимо принять комплексные меры, включающие в себя организационные, правовые, технические составляющие, а именно:

1 повышение осведомленности пользователей электронных информационных ресурсов, информационных систем и информационно-коммуникационной инфраструктуры;

2 мотивирование отечественных компаний, осуществляющих деятельность, связанной с обеспечением кибербезопасности, и повышение масштабности их деятельности до уровня государства;

3 увеличение доли отечественных средств защиты от киберугроз (кибератак);

4 усовершенствование нормативной правовой базы обеспечения кибербезопасности, в частности;

5 организация международных и региональных конференций, посвященных тематике информационной безопасности;

6 организация полигонов с типовыми киберугрозами на базе учебных заведений;

7 организация курсов повышения квалификации специалистов по кибербезопасности.

Таким образом, принятие нормативных правовых актов, регламентирующих порядок обеспечения кибербезопасности, является необходимым условием, но не достаточным.

Для получения полноценного результата требуется качественная проработка уполномоченными организациями путей и механизмов реализации указанных нормативных правовых актов.

Следует отметить, что даже при идеальных условиях реализации невозможно гарантировать защиту от всех видов (типов) киберугроз, так как они могут реализоваться в кибератаках по различным векторам.

## Список использованной литературы


1Израилов К.Е., Буйневич М.В., Котенко И.В., Десницкий В.А. Оценивание и прогнозирование состояния сложных объектов: применение для информационной безопасности [Текст] // Вопросы кибербезопасности.–2022.-№6(52).-С.2-21.-(https://cyberrus.com/ wp-content/uploads/ 2022/12/02-21-652-22_1. - Izrailov.pdf)

2Малик Т. Н. Кибербезопасность: проблемы и перспективы [Текст] // Молодой ученый. — 2021. — № 7 (349). — С. 10-12. (https://moluch.ru/archive/349/78602/) (дата обращения: 20.02.2023)

3Шаповаленко О. Д., Бедрий Д. И. Обзор современного состояния кибербезопасности [Текст] // Международный журнал информационных и коммуникационных технологий.-2021.- №3. - С.18-26. (https://moluch.ru/archive/349/78602/) (дата обращения: 17.02.2023)

4Jiaqi Sun. Computer Network Security Technology and Prevention Strategy Analysis [Текст] // Procedia Computer Science. Volume 208. 2022. (https://www.sciencedirect.com/ science/article/pii/S1877050922015204) (дата обращения: 26.02.2023)