ТЕХНОЛОГИИ СНИЖЕНИЯ РИСКОВ КИБЕРПРЕСТУПНОСТИ, СОВЕРШЕНСТВОВАНИЯ СТАНДАРТОВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

М. А. Тренина

Белорусский государственный университет, пр. Независимости, 4, 220030, г. Минск, Беларусь, mariatren@mail.ru
Научный руководитель – И. Н. Бородавка

В век цифровых технологий информационная безопасность становится критически важным аспектом современного общества. Киберпреступность представляет собой все более значительную угрозу, поэтому разработка и усовершенствование мер защиты является насущной необходимостью.

Ключевые слова: киберпреступность; информационная безопасность; Интернет угрозы.

В современном мире информационные технологии занимают центральное место в бизнес-процессах и взаимодействии людей. Однако, развитие информационных технологий также приводит к росту угроз кибербезопасности, что требует постоянного совершенствования технологий и стандартов информационной безопасности.

Теоретические аспекты изучения явления киберпреступности и способов борьбы с ней

Глобализация информационных технологий открывает неограниченные возможности для воздействия на человека и общество. Это включает в себя возникновение и развитие новых форм преступности – преступности в сфере высоких технологий.

Киберпреступление – это незаконное использование компьютеров или сетей с целью совершения преступных действий. Хакеры, отдельные лица или организации могут быть участниками таких преступлений. Личные данные пользователей и их финансовые средства, хранящиеся на электронных устройствах, могут быть объектами незаконных действий [4].

Киберпреступность охватывает широкий спектр деяний, четкое разграничение которых затруднено. Тем не менее, среди основных видов можно выделить [2]:

1. Финансовые преступления
2. Вредоносное программное обеспечение (ВПО)
3. Кибероружие

Состояние киберпреступности на сегодняшний день

Состояние кибербезопасности в мире сегодня является крайне напряженным. Киберпреступления стали все более распространенными

и разнообразными, а атаки стали более умными и сложными для обнаружения и предотвращения.

Первое киберпреступление в Беларуси было зафиксировано в 1998 году, когда хакер использовал вредоносную программу для несанкционированного доступа к конфиденциальным данным клиентов интернет-провайдера [3].

В течение всего 2023 года было зарегистрировано более 10 000 случаев киберпреступлений. Причем примерно 9 тысяч из них связаны с мошенничеством в сфере финансов. Общая динамика показателей киберпреступности за 2015–2023 гг. в Беларуси представлена на диаграмме (рис. 1).

Рис. 1. Динамика показателей киберпреступности за 2015–2023 гг. в Беларуси

Если говорить о мировом масштабе проблемы, то последствия от кибератак становятся все более внушительными. Впечатляющая динамика количества киберпреступлений в мире за период 2000–2021 с прогнозом на 2031 г. также представлена на диаграмме (рис. 2).

Анализ современных методов борьбы с киберпреступностью

Существует широкий спектр методов, которые можно использовать для борьбы с киберпреступностью. Выбор конкретного подхода зависит от уникальных особенностей каждой организации или компании [1].

1. IDS (системы обнаружения вторжений)
2. Использование механизмов шифрования данных.
3. Искусственный интеллект (ИИ).
4. Использование механизмов мониторинга утечек данных.

5. Многофакторная аутентификация (MFA).
6. Кодирование данных.
7. Системы для резервного копирования и восстановления данных.
8. Обучение и повышение осведомленности пользователей.

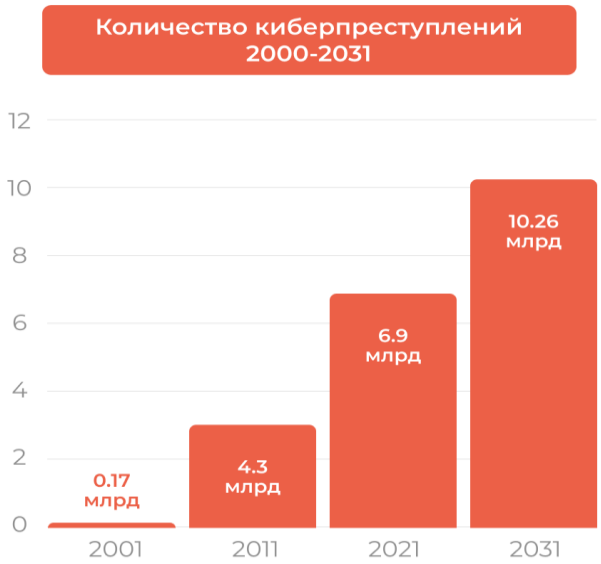

Рис. 2. Динамика количества киберпреступлений в мире за период 2000-2021, прогноз на 2031 г.

Тестирование эффективности антивирусных программ

С целью выявления эффективного решения для защиты личной информации было проведено тестирование трех ведущих антивирусов в мире: Kaspersky Lab, Norton 360 Antivirus, BitDefender.

В ходе тестирования было выявлено, что Bitdefender и Kaspersky продемонстрировали себя как наиболее эффективные антивирусные программы, обладающие передовыми технологиями обнаружения и блокировки вредоносных угроз. Они показали высокую скорость работы, относительно низкое влияние на производительность системы и широкий спектр дополнительных функций для обеспечения безопасности. С другой стороны, Norton немного отстает от Bitdefender и Kaspersky в эффективности работы, однако все равно представляет собой надежное решение для защиты от киберугроз.

Рекомендации по защите конфиденциальности в киберпространстве

В процессе написания статьи был составлен краткий список советов по обеспечению безопасности в интернете, включающий следующие пункты:

1. Использование сильных паролей.
2. Своевременное обновление антивирусного ПО.

3. Внимательное отношение к незнакомым сайтам и ссылкам.

4. Наблюдение за конфиденциальностью в социальных сетях.

5. Соблюдение осторожности при подключении к открытым сетям Wi-Fi.

6. Защита от онлайн-слежки.

7. Отключение онлайн-сохранения паролей в браузере.

8. Внимательное отношение к установке приложений и скачиванию файлов.

9. Перед завершением работы выход из всех аккаунтов и выключение компьютера.

10. Хранение личные данные в тайне.

Соблюдение этих простых мер поможет обеспечить вашу безопасность в онлайн-сфере.

Таким образом, развитие информационных технологий также приводит к росту угроз кибербезопасности, что требует постоянного совершенствования технологий и стандартов информационной безопасности. Масштабы киберпреступности становятся настолько внушительными, что игнорирование этой проблемы уже невозможно.

Существует множество методов и технологий, которые могут использоваться для повышения уровня безопасности информации и их эффективность. Однако, применение технологий информационной безопасности не ограничивается только внедрением современных технологий. Также необходимо уделять внимание организации процесса работы с информацией, обучению персонала правилам безопасности и контролю за их соблюдением.

Библиографические ссылки

1. *Веремейчик Р. М.* Исследование применения методов защиты информации и борьбы с киберпреступностью [Электронный ресурс]. URL: https://na-journal.ru/6-2023-informacionnye-tekhnologii/5845-issledovanie-primeneniya-metodov-zashchity-informacii-i-borby-s-kiberprestupnostyu (дата обращения: 27.03.2024).

2. *Кочкина Э. Л.* Определение понятия «киберпреступление». отдельные виды киберпреступлений. С. 162-169.

3. Следственный комитет Республики Беларусь [Электронный ресурс]. URL: https://sk.gov.by. (дата обращения: 25.03.2024).

4. *Шогенов З. А.* Уголовное право // Образование и право. № 8. 2022. С. 292–297.