БОРЬБА С КИБЕРПРЕСТУПНОСТЬЮ

Инагамова Мафура Мухторхонова - *доцент Ташкентского Государственного Университета*
Кенисов Жантас Амангельди улы - *студент 2-курса Ташкентского Государственного Транспортного Университета*

Аннотация: В статье изучены основные моменты развития внедрения информационно-коммуникационных в Узбекистане. Комплексная программа «Цифровой Ташкент». Киберпреступность. Кибербезопасность. Обозначены нормативно-правовые основы законодательства уголовной ответственности преступлений. Рассмотрены меры, принимаемые государством для пресечения данного деяния. Изучен вопрос об актуальности данной проблемы и меры по безопасности граждан. Приводится мировой опыт по решению данной глобальной проблемы.

Ключевые слова: Киберпреступность, Фишинг, Кибершпионаж, Кибермошенничество, Киберкража, Законность, Искусственный интеллект, Мониторинг, Защита данных.

Киберпреступность - это сфера преступной деятельности, связанная с использованием информационных и коммуникационных технологий (ИКТ) для совершения преступлений. Киберпреступники могут направлять свои атаки на компьютерные системы, сети, устройства, а также на людей и организации. Вот некоторые ключевые аспекты киберпреступности:

1. Типы киберпреступлений:

-Фишинг: Злоумышленники маскируются под доверенные источники, чтобы обмануть людей и получить доступ к их личной информации.

-Вредоносные программы: Распространение и использование вирусов, троянов, шпионских программ и других вредоносных кодов.

-Кибершпионаж: Атаки на государственные, корпоративные или индивидуальные системы с целью получения конфиденциальной информации.

-ДДоС-атаки: Завал веб-сайтов или сетей путем перегрузки их трафиком.

-Кибермошенничество: Мошенничество, включающее в себя финансовые аспекты, часто с использованием интернета.

2. Мотивации киберпреступников:

-Финансовая выгода: Кража денег, банковских данных или вымогательство.

-Шпионаж: Политические или корпоративные интересы.

-Активизм: Осуществление атак в рамках политических или идеологических убеждений.

-Развлечение: Некоторые киберпреступники атакуют просто для развлечения и вызова хаоса.

3. Последствия:

-Потери данных: Кража или уничтожение ценных данных.

-Финансовые потери: Ущерб бизнесам и частным лицам.

-Нарушение конфиденциальности: Утечка личной информации.

-Угрозы безопасности: Возможность воздействия на критическую инфраструктуру.

4. Противодействие:

-Кибербезопасность: Разработка и применение технологий и стратегий для защиты от киберугроз.

-Законодательство: Введение и совершенствование законов, регулирующих киберпреступность.

-Международное сотрудничество: Совместные усилия стран и международных организаций в борьбе с киберугрозами.

Общество сталкивается с постоянной эволюцией киберпреступности, и защита от нее требует постоянного совершенствования технологий и стратегий безопасности. В современном мировом контексте киберпреступления представляют собой одну из наиболее серьезных и динамично развивающихся угроз. С увеличением зависимости общества от цифровых технологий киберпреступники активно адаптируются, создавая новые и более сложные методы атак.

Киберпреступления охватывают широкий спектр деятельности, включая кражу личных данных, финансовые махинации, шпионаж, кибершпионаж, взломы корпоративных сетей и многие другие аспекты. Эти атаки могут иметь различные масштабы, начиная от индивидуальных случаев до массированных кибератак на государственные инфраструктуры.

Одной из ключевых особенностей киберпреступлений является их трансграничный характер: киберпреступники могут действовать из любой точки мира, а их атаки часто нацелены на объекты в других странах. Это создает сложности в сфере правоприменения и подчеркивает необходимость международного сотрудничества в борьбе с этой угрозой.

С учетом постоянного развития технологий и их все более важной роли в нашей повседневной жизни, проблема киберпреступлений требует постоянного внимания, инициатив по укреплению кибербезопасности и разработки эффективных международных стратегий противодействия этой глобальной угрозе.

Киберпреступления имеют высокую актуальность в Узбекистане, так как страна, подобно многим другим, сталкивается с растущим влиянием цифровой трансформации.

Киберпреступления могут оказать серьезное воздействие на экономику Узбекистана, в том числе через кибермошенничество, кражу финансовых данных и атаки на банковские системы.

В Ташкенте в 2022 году было совершено 4332 преступления в сфере информационных технологий, что в 40 раз превышает показатель 2020 года, когда правоохранители зафиксировали 106 подобных фактов. Такую статистику привели сотрудники Главного управления внутренних дел столицы на брифинге, посвященном кибербезопасности.

Если сравнивать с данными за 2021 год, то в прошлом году число киберпреступлений возросло в два раза — с 2281 до 4332. Из них 2747 — киберкражи, 625 — кибермошенничество, 874 — правонарушения, связанные с распространением наркотиков через интернет.

В ГУВД подчеркнули, что количество фактов мошенничества и краж денег с банковских карт увеличилось «в связи с развитием современных технологий».

С учетом сложившейся ситуации в августе прошлого года в структуре столичного управления внутренних дел создали отдел по борьбе с преступностью в сфере информационных технологий. За короткий период специалистами был проведен ряд профилактических мероприятий по предупреждению киберпреступлений.

Однако на брифинге не уточнили, как изменилась динамика киберпреступлений после начала работы отдела. Хотя известно, что за первые семь месяцев 2022 года по всей республике было заведено 1812 уголовных дел по факту мошенничества и краж с пластиковых карт.

В свою очередь, сотрудник центра кибербезопасности МВД Узбекистана Саидкамол Содиков признал, что в последние годы количество правонарушений в сфере информационно-коммуникационных технологий увеличилось в несколько раз и составляет наибольшую часть от общего числа преступлений.

Согласно данным, озвученным представителем министерства:

☞ 34% киберпреступлений основаны на получении мошенниками секретного кода банковской карты в рамках предложений финансовой помощи, оформления онлайн-кредита или выигрыша в игре;

☞ 22% — это выманивание денег у потерпевшего в виде авансового платежа по какому-либо договору;

☞ 17% — получение пин-кода и номера карты «лже-сотрудниками банка» или платежных систем;

☞ 14% — получение секретных данных через торговые онлайн-площадки;

☞ 9% — мошенничество через финансовые интернет-биржи.

Также были зарегистрированы преступления, когда злоумышленники просили предоставить им коды для подтверждения отправки средств на благотворительность и оплату затрат на умру (паломничество в Мекку).

В сентябре прошлого года сообщалось, что власти Узбекистана намерены ужесточить наказание за хищение денег с банковских карт. В частности, планировалось увеличить сумму штрафа, а также повысить максимальный срок лишения свободы за подобное преступление — с пяти до восьми лет.

Президент подписал Закон от 15.04.2022 г. №ЗРУ-764 «О кибербезопасности». Закон состоит из 8 глав и 40 статей.

В Законе используются такие понятия, как киберпреступность, киберпространство, киберугроза, кибербезопасность, киберзащита, кибератака.

Также определены основные принципы обеспечения кибербезопасности, к которым относятся:

-Законность;

-Приоритет защиты интересов личности, общества и государства в киберпространстве;

-Единый подход к регулированию сферы кибербезопасности;

-Приоритет участия отечественных производителей в создании системы кибербезопасности;

-Открытость Республики Узбекистан к международному сотрудничеству в обеспечении кибербезопасности.

Противодействие киберпреступлениям требует комплексного подхода, включая технические, организационные и правовые меры.

Вот несколько предложений:

1.Кибербезопасность:

-Антивирусное и антишпионское программное обеспечение: Регулярное обновление и использование современных средств защиты.

-Брандмауэры и интранет-системы: Защита сетей от несанкционированного доступа.

2.Обучение персонала:

-Создание культуры безопасности: Обучение сотрудников базовым принципам безопасности в интернете и на рабочем месте.

-Симуляции фишинга: Проведение тренировок для распознавания и предотвращения атак фишинга.

3.Регулярные аудиты безопасности:

-Проверки уязвимостей: Регулярное сканирование и анализ систем для выявления потенциальных уязвимостей.

-Мониторинг сетевой активности: Отслеживание подозрительной активности в сети.

4.Создание и соблюдение политик безопасности:

-Установление строгих паролей и двухфакторной аутентификации: Защита доступа к системам и данных.

-Ограничение прав доступа: Предоставление минимально необходимых прав для сотрудников.

5.Защита данных:

-Регулярные резервные копии: Систематическое создание резервных копий данных для быстрого восстановления после атаки.

-Шифрование данных: Защита конфиденциальной информации шифрованием.

6.Законодательство и сотрудничество:

-Строгие законы о киберпреступлениях: Создание и совершенствование законов для наказания киберпреступников.

-Международное сотрудничество: Обмен информацией и совместные действия для противодействия трансграничным киберугрозам.

7.Инновации в технологиях безопасности:

-Искусственный интеллект и аналитика данных: Использование современных технологий для обнаружения и предотвращения кибератак.

Противостоять киберпреступлениям требует постоянного обновления стратегий и технологий, так как угрозы постоянно эволюционируют.

Список литературы:

1. https://fergana.media/news/129278/
2. https://nuz.uz/obschestvo/1246386-v-uzbekistane-vyroslo-kolichestvo-kiberprestuplenij.html
3. https://lex.uz/ru/docs/5960609
4. Закон Республики Узбекистан о Кибербезопасности от 17.03.2022