СЛУЖБА ПРОБАЦИИ РЕСПУБЛИКИ УЗБЕКИСТАН. КИБЕРБЕЗОПАСНОСТЬ-ОСНОВА ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ ЗАЩИТЫ,ВИДЫ ИНФОРМАЦИОННЫХ УГРОЗ.

Старший инспектор службы пробации
Министерства внутренних дел Республики Узбекистан
старший лейтенант ***Собирова Диёра Рустам қизи***

Аннотация: В данной статье регламентируется актуальность кибербезопастности, а именно то, что защищенность сетей передачи данных, является одной из самых необходимых вещей как в обычной жизни каждого из нас, так и в политической жизни стран мира. Обеспечение качественной передачи информации, обеспечение безопасности, предотвращение кибер-атак, нарушения сети, улучшение программного обеспечения является основной целью каждого при предотвращении киберпреступности.

Ключевые слова: кибербезопасность, кибер-атака, сеть, угроза, программа,информация,передача данных, социальная сеть, искусственный интеллект.

Annotatsiya: Ushbu maqola kiberxavfsizlikning dolzarbligini tartibga soladi, ya'ni ma'lumotlar uzatish tarmoqlari xavfsizligi har birimizning oddiy hayotimizda ham, dunyo mamlakatlari siyosiy hayotida ham eng zarur narsalardan biridir. Axborotning yuqori sifatli uzatilishini ta'minlash, xavfsizlikni ta'minlash, kiberhujumlar, tarmoq uzilishining oldini olish, dasturiy ta'minotni takomillashtirish asosiy hisoblanadi.

Kalit so’zlar : kiberxavfsizlik, kiberhujum, tarmoq, tahdid, dastur, axborot, ma’lumotlar uzatish, ijtimoiy tarmoq, sun’iy intellekt..

Abstract: This article regulates the relevance of cybersecurity, namely that the security of data transmission networks is one of the most necessary things both in the ordinary life of each of us and in the political life of countries around the world. Ensuring high-quality transmission of information, ensuring security, preventing cyber-attacks, network disruptions, improving software is the main goal of everyone in preventing cybercrime.

Key words: cybersecurity, cyber attack, network, threat, program, information, data transfer, social network, artificial intelligence.

Введение

Кибербезопасность (ее иногда называют компьютерной безопасностью) – это совокупность методов и практик защиты от атак злоумышленников для

компьютеров, серверов, мобильных устройств, электронных систем, сетей и данных. Кибербезопасность находит применение в самых разных областях, от бизнес-сферы до мобильных технологий. В этом направлении можно выделить несколько основных категорий.[1]

Целью написания данной статьи является изучение актуальных проблем киберпреступности, с которыми сталкиваемся ежедневно, необходимость улучшения кибербезопасности, а также меры пресечения угроз и преступлений в данной области.

Киберпреступность - это преступная деятельность, осуществляемая через компьютеры и/или интернет. К киберпреступности могут относиться ситуации, когда компьютер является центром деятельности: такие правонарушения, как компьютерные атаки, фишинг, спам и разработка вирусов.[2]

Необходимо отметить, что за последние несколько лет кибер-атаки стали по своей форме и виду сложными, несмотря на то, что эксперты разрабатывают новые способы и инструменты для защиты. В статье рассмотрим какие угрозы существуют, что можно сделать чтобы повысить безопасность и какими сайтами желательно воспользоваться для получения гарантированной безопасной передачи данных.

Разработчики различных программ, сайтов, социальных сетей, браузеров, как правило, предусматривают множество механизмов защиты, в целях предотвращения различных угроз и атак.

В качестве примера можно рассмотреть, как разработчики браузеров внедряют sandbox-технологии, защиту от фишинга и вредоносного ПО, блокировку отслеживающих скриптов и трекеров, просмотр с шифрованием DNS и другое[3].

И так мы рассмотрели лишь на примере браузера, исходя из него выявляется основная проблема, которая заключается в том, что многие угрозы обходят стандартные механизмы защиты, оставаясь невидимыми до момента атаки.

Какие виды угроз известны на сегодняшний день? Далее рассмотрим несколько вариантов сетевых атак, о которых многие даже не знают.

Атаки нулевого дня. Уязвимости, о которых не знают даже разработчики, — идеальное оружие для хакеров. Например, в 2023 году эксплойт в движке Chrome V8 позволял запускать произвольный код через PDF-файлы. Такие «дыры» могут месяцами оставаться открытыми, пока их не закроют патчем.

Загрузка вредоносов. Посещение поддельного сайта или даже легитимного ресурса с рекламным баннером может привести к автоматической

[1] https://www.kaspersky.ru/resource-center/definitions/what-is-cyber-security
[2] https://www.rahmanravelli.co.uk/ru/
[3] https://securitymedia.org/info/slezhka-fishing-i-utechki-naskolko-bezopasny-populyarnye-brauzery.html

загрузке майнера, шпионского ПО или ransomware. Браузеры блокируют часть таких сценариев, но методы вроде «drive-by download» все еще работают.

Фишинг. Современные фишинговые страницы копируют интерфейс банков, соцсетей и даже двухфакторной аутентификации. Браузеры учатся распознавать поддельные SSL-сертификаты, но AI-генераторы вроде **WormGPT или FraudGPT** создают сайты-двойники, которые обманывают даже ИИ-фильтры.[4]

Повышение знаний в области кибербезопасноти для обеспечения безопасности и сохранения конфеденциальности информации является необходимым не только, медийным личностям, но и всем остальным, так как день за днем цифровизация всех деятельностей страны выходит на новый уровень. На сегодняшний день при присвоении информации путем искусственного интеллекта совершаются разного рода правонарушения, влекущие за собой разной тяжести последствия.

Всеобщим достижением является то, что на ровне с развитием распространения различных угроз, также разрабатываются, прогрессируют различные меры по обеспечению защиты программ, сетей, социальных аккаунтов и так далее. В последние годы концепция активной защиты (хэк бэк) притягивает все больше внимания к себе, набирая популярность в сфере информационной безопасности как проактивный метод защиты. Данный подход предполагает не только защиту от атак, но предусматривает также и ответные действия, направленные на нейтрализацию грозы, в том числе путем воздействия на инфраструктуру злоумышленников. Однако такие методы вызывают споры о легальности, этичности и возможных последствиях. В некоторых странах использование данного метода является нарушение закона.

Справедливо отметить, что ежегодно растет количество инцидентов ИБ и компьютерных атак. Обнаружение программных и аппаратных уязвимостей происходит с нарастающей скоростью, расширяя масштаб угроз. Техники злоумышленников становятся сложнее, а ход их действий продолжает совершенствоваться. При этом важно отметить, что технологии и методология со стороны защиты развиваются с той же интенсивность, что и угрозы, эксперты -защитники бьются над тем, чтобы обнаруживать хакеров на самых ранних звеньях.

Таким образом, на сегодняшний день каждый из нас должен повышать своё правовое сознание в области кибербезопасноти, так как все сферы деятельности переходят на новый уровень циврофизации, даже дети с ранних лет начинают пользоваться компьютерными технологиями, социальными сетями. В

[4] https://securitymedia.org/info/slezhka-fishing-i-utechki-naskolko-bezopasny-populyarnye-brauzery.html

целях предотвращения роста преступлений в данной сфере, а также обеспечения индивидуальной и виктимологической профилактики правонурушения.

Список использованной литературы:

1. Конституция Республики Узбекистан – 01.05.2023г.
2. Ш.М.Мирзиёев. “Янги Ўзбекистон стратегияси”. Т. Издательство “O’zbekiston”. 2021. С.464;
3. Уголовный Кодекс Республики Узбекистан от 01.04.1995 № 2012-XII [Электронный ресурс] - http://fmc.uz/legisl.php?id=k_ug – Дата доступа 18.12.2023;
4. Уголовно-исполнительный Кодекс Республики Узбекистан от 01.10.1997г. [Электронный ресурс]- https://lex.uz/docs/163627 - Дата доступа 18.12.2023;
5. Закон “О профилактике правонарушения” от 14 мая 2014 года ЗРУ№371 [Электронный ресурс]- https://lex.uz/docs/2387359 -Дата доступа 26.01.2022