– Автоматическая система выявления запрещенных товаров.

Перечисленные области применения искусственного интеллекта в деятельности таможен способствуют повышению доверия к таможенной системе, так как фактор человеческих ошибок будет отсутствовать. Однако во многих случаях вмешательство лиц таможенного дела будет необходимо.

В настоящее время технологии автоматизации искусственного интеллекта значительно помогают ускорять процессы в таможенном деле. Существует множество перспектив развития данных технологий в ближайшем будущем, которые уже находятся в активной разработке. [3]

Современные технологии таможенного дела стремительно развиваются, что требует особых знаний должностных лиц таможенных органов во многих аспектах. Следовательно, слаженная работа сотрудников таможенного дела и разработчиков искусственного интеллекта является необходимым условием при переходе к автоматизации таможенных процессов.

Литература

1. Андреева Е.И., Катунин В.А., Караулова А.Н. Перспективы таможенного декларирования и таможенного контроля товаров с использованием облачных технологий // Вестник экономической интеграции. 2014. № 10 (79). С. 35–42.

2. Сомов Ю.И., Аникин С.Н., Нажимов Р.А., Позднякова К.Е. Актуальные вопросы применения искусственного интеллекта в деятельности таможенных органов // Ю.И. Сомов, С.В. Новиков. Вестник Российской таможенной академии. 2021. № 3. С. 16-18.

3. Федотова Г.Ю. Практические проблемы процессов цифровизации в таможенной сфере. / Сборник трудов научно-практической конференции с международным участием. Под редакцией А.В. Бабкина. 2019. С. 124-129.

КИБЕРПРЕСТУПНОСТЬ И КИБЕРКОНФЛИКТЫ В СОВРЕМЕННОМ МИРЕ

Лозовик К.В., Гаро В.А.
Научный руководитель: ст. преподаватель Ковалькова И.А.
Белорусский национальный технический университет

В наши дни киберпреступления создают множество проблем для общества. С резким увеличением числа пользователей информационно-телекоммуникационных технологий, а также компьютеров и компьютерных сетей, многие люди оказались в уязвимом положении в киберпространстве. Это явление стало особенно актуальным в последние годы, когда доступ к интернету стал более простым и повсеместным.

Киберпреступность – это незаконная деятельность, которая осуществляется при помощи компьютерных технологий или интернета. Обычно это делает один человек или небольшая группа, для получения незаконного доступа к информации, кражи данных, вымогательства или нанесения материального ущерба. В результате, киберпреступность, охватывающая широкий спектр преступлений, таких как хакерские атаки, кража личных данных, финансовые мошенничества и распространение вирусов, быстро превратилась в серьёзную и опасную проблему, которая может иметь значительные последствия для общества в целом. По данным различных исследований, киберпреступность ежегодно наносит ущерб в миллиарды долларов, и эта цифра продолжает расти. Важно понимать, что киберугрозы могут исходить не только от отдельных злоумышленников, но и от организованных группировок, которые действуют на международном уровне. Это требует от правительств и частных компаний совместных усилий для разработки эффективных стратегий защиты и реагирования на кибератаки. [1]

Киберпреступники используют всё более сложные методы, чтобы обойти системы безопасности, что делает защиту данных и информации крайне важной задачей для организаций и отдельных пользователей. Например, фишинг, при котором злоумышленники пытаются обманом заставить пользователей раскрыть свои личные данные, стал одной из самых распространённых форм киберпреступлений. Злоумышленник как бы «подсаживает» жертву на крючок, отправляя письма от крупного и уважаемого сервиса зайти на сайт, но по ссылке, как правило, загружается поддельный веб-сайт, который внешне похож на оригинальный, но принадлежит злоумышленнику. Сайт запросит логин и пароль, при их вводе хакер получает их и потом, зная их, он сможет легко под видом вашей учётной записи зайти на настоящий веб-сайт и в итоге украсть ваши личные данные или денежные средства. Пример фишингового сайта можно видеть на Рисунке 1.

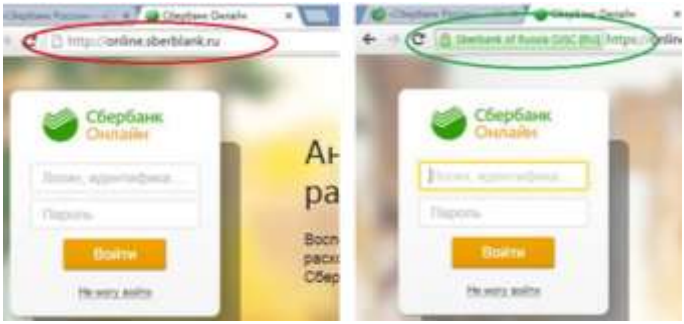

Рисунок 1. Пример фишингового сайта.

Также ещё одной разновидностью кибератак является распределённая атака «отказ в обслуживании» или DDOS(Distributed Denial-of-Service). При такой атаке хакер перегружает веб-сайт большим количеством запросов. Они идут одновременно с разных компьютеров. Их цель – искусственно перегрузить целевой сервер или сеть таким количеством запросов, что он перестаёт нормально функционировать и становится недоступен для законных пользователей. Злоумышленники выбирают цели, исходя из различных мотивов. Финансовая выгода – одна из главных причин. Атаки на онлайн-банки и платёжные системы могут быть предприняты для кражи данных пользователей или вымогательства денег. График процентного соотношения направления атак изображён на Рисунке 2.

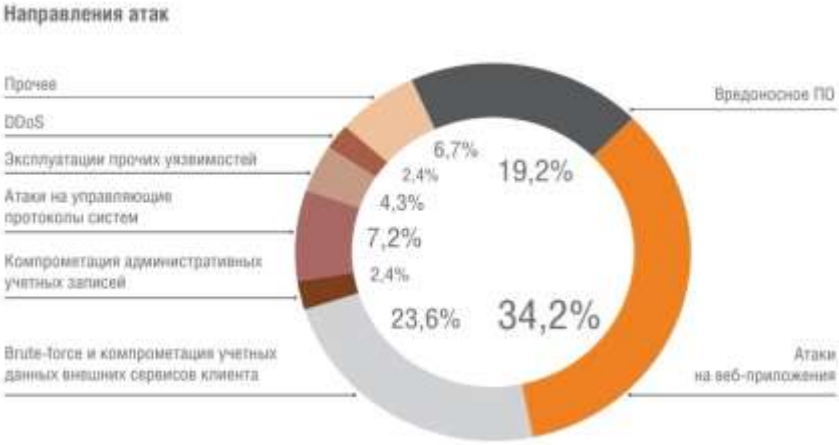

Рисунок 2. График процентного соотношения направления атак.

Киберконфликты – это более широкое явление, часто связанное с политическими, идеологическими или геополитическими мотивами. Суть заключается в использовании киберпространства для проведения атак на государства, организации или отдельных лиц с целью нанесения ущерба странам или отдельным регионам. Такие конфликты могут проявляться в виде кибератак на важные объекты, например, энергетические сети, финансовые учреждения.

Вот некоторые ключевые отличия:

• Причины: Киберпреступность – желание получить выгоду, корысть; киберконфликт – разногласия в политических, идеологических, геополитических вопросах.

• Участники: Киберпреступность – отдельные лица, группы, организованные преступные сообщества; киберконфликты – государства, негосударственные субъекты, хакерские группировки, действующие по заказу государств.

• Масштабы: Киберпреступность – обычно ограничена конкретными жертвами; киберконфликты – могут затрагивать целые страны и регионы.

• Цели: Киберпреступность – получение финансовой выгоды, кража данных, саботаж; киберконфликты – дестабилизация, подрыв доверия, нанесение политического или экономического ущерба.

• Последствия: Киберпреступность – финансовые потери, утечка данных, нарушение работы систем; киберконфликты – широкомасштабные сбои в работе инфраструктуры, политическая нестабильность, международные конфликты.

Киберпреступность и киберконфликты представляют серьезную опасность для безопасности национальной и международной сфер. Государства вынуждены вкладывать средства и силы в кибербезопасность и развивать свои возможности в области кибероборoны. Это приводит к созданию новых стратегий и идей, направленных на защиту от кибератак и киберугроз. [3]

Современные тенденции:

1. Увеличение числа атак: За последние годы наблюдается рост кибератак на государственные и частные учреждения.

2. Новые технологии: Развитие ИИ и Интернета вещей усложняет борьбу с киберпреступностью.

3. Правительственные меры: Многие страны разрабатывают национальные стратегии кибербезопасности.

В условиях современного, быстро меняющегося цифрового мира киберпреступность и киберконфликты становятся все более актуальными и серьезными темами. Для борьбы с этими угрозами необходимы совместные усилия международного сотрудничества, включая сотрудничество между государствами, развитие технологий безопасности и повышение осведомленности пользователей о киберугрозах.

Для борьбы с киберпреступностью и киберконфликтами необходим определенный подход, который включает:

Развитие правовой базы: Формирование и улучшение законодательства в области кибербезопасности.

Укрепление защиты в кибербезопасности: Инвестиции в защитные технологии, улучшение компьютерной грамотности населения и сотрудников организаций.

Международное сотрудничество: Совместные усилия государств для обмена данных, координации действий по борьбе с киберпреступностью и предотвращению киберконфликтов.

Развитие кибербразведки: Оперативное и своевременное обнаружение и недопущение кибератак.

Повышение осведомленности: Обучение граждан методам защиты от киберугроз. [2]

Таким образом, киберпреступность становится не только индивидуальной проблемой, но и глобальной угрозой, требующей комплексного подхода и активного участия всех заинтересованных сторон. Образование и повышение осведомленности пользователей о киберугрозах также играют ключевую роль в защите от киберпреступлений, поскольку большинство атак начинается с простых ошибок, таких как клик на подозрительную ссылку или использование слабых паролей.

Литература

1. Айков Д.В. Компьютерные преступления. Руководство по борьбе с компьютерными преступлениями / Д. Айков, К. Сейгер, У. Фонсторх. - М.: Мир, 2014.- 351 с.

2. Вехов В. Б. Компьютерные преступления: способы совершения и раскрытия / В.Б. Вехов; Под ред. акад. Б.П. Смагоринского. - М.: Право и закон, 2014.- 182 с.

3. Киберпреступность — определение, классификация интернет угроз. [Электронный ресурс].

ЭЛЕКТРОННО-ЦИФРОВАЯ ПОДПИСЬ (ЭЦП) И ЕЕ НАЗНАЧЕНИЕ

Муравейко А.А., Климович А.А.
Научный руководитель: ст. преподаватель Ковалькова И.А.
Белорусский национальный технический университет

Электронно-цифровая подпись (ЭЦП) – это аналог собственноручной подписи, представленный в электронном виде. ЭЦП используется для подтверждения подлинности и целостности электронных документов.

Получить ее вправе каждый субъект хозяйствования на возмездной основе. Для этого нужно записаться в Национальный центр электронных услуг. Если же у субъекта хозяйствования уже был ключ, сертификат можно продлить. В этом случае посещать НЦЭУ уже не обязательно, заявку можно подать и оплатить удаленно, а сформированный файл обновленного ключа пришлют в облаке.[1]

Одно из главных преимуществ ЭЦП - придание электронным документам юридической значимости, равной бумажным документам с собственноручной подписью. Это позволяет использовать электронные документы в судебных разбирательствах и других официальных процедурах. ЭЦП также обеспечивает конфиденциальность, защищая информацию от несанкционированного доступа и позволяя шифровать данные для безопасной передачи по открытым каналам связи.

В бизнес-среде ЭЦП значительно оптимизирует процессы, ускоряя подписание и обмен документами, а также сокращая расходы на бумажный документо-