БОРЬБА С КИБЕРПРЕСТУПНОСТЬЮ И ЕЕ ЗНАЧЕНИЕ ДЛЯ ОБЩЕСТВА

Беликова Елена Геннадьевна
старший преподаватель
УО «Брестский государственный
технический университет»

Аннотация: В наши дни киберпреступления создают множество проблем для общества: личных, финансовых и даже становятся угрозой национальной безопасности. Только за последние несколько лет были украдены данные с сотен миллионов кредитных карт и десятков миллионов страховых свидетельств. В Беларуси за 2023 год было зафиксировано 10 тысяч киберпреступлений, из них 90% это мошенничество и хищение денежных средств: как собственных накоплений граждан, так и кредитных ресурсов.

Ключевые слова: Кибербезопасность, мошенничество, хищения денежных средств, вирусы, киберпреступления.

THE FIGHT AGAINST CYBERCRIME AND ITS IMPORTANCE TO SOCIETY

Belikova Elena Gennadievna

Abstract: Nowadays, cybercrimes create many problems for society: personal, financial, and even become a threat to national security. In the last few years alone, data from hundreds of millions of credit cards and tens of millions of insurance certificates have been stolen. In Belarus, 10,000 cybercrimes were recorded in 2023, of which 90% are fraud and embezzlement of funds: both citizens' own savings and credit resources.

Key words: Cybersecurity, fraud, embezzlement of funds, viruses, cybercrimes.

За первую половину 2023 года мошенники украли через СБП 1,3 млрд рублей, 16,25% от всех похищенных за этот период средств.

Центробанк начал отдельно отслеживать этот канал краж денег с начала года. Всего мошенники украли за полгода у банковских клиентов более 8 млрд рублей, это на 33% больше, чем за тот же период годом ранее.

Взломы случаются благодаря ошибкам и уязвимостям в аппаратном и программном обеспечении, но гораздо чаще благодаря случайным действиям людей, которые пользуются этими программами.

Киберпреступниками бывают разные люди с совершенно разной мотивацией, среди них есть международные террористы и подростки, желающие похвастаться перед сверстниками. Также существуют киберпреступники, которые могут быть спонсированы государствами или преступными организациями и занимаются кражей финансовых данных, шпионажем или проведением кибератак на крупные организации или правительства.

Киберпреступность имеет серьезные последствия для общества. Она может привести к финансовым потерям, утечке личной информации, нарушению конфиденциальности и доверия, а также повреждению репутации компаний и организаций.

Борьба с киберпреступностью требует сотрудничества и координации между правительствами, компаниями и организациями. Это включает обмен информацией о новых угрозах, совместная разработка стратегий и планов действий, а также сотрудничество в области правоохранительной деятельности для выявления и наказания киберпреступников.

В целом, борьба с киберпреступностью является сложной задачей, требующей постоянного внимания и инноваций. Однако, совместными усилиями мы можем создать более безопасное и защищенное цифровое пространство.

Возникновение вируса. Вирус – это обычная программа, которая устанавливается на компьютер непреднамеренно и приносит вред пользователю и компьютеру. Он может быть передан через зараженные файлы, электронные письма или при посещении зараженных веб-сайтов. Как только вирус попадает на компьютер, он начинает размножаться и распространяться, заражая другие файлы и системы.

Вирусы могут иметь различные цели и последствия. Некоторые вирусы могут украсть личную информацию пользователя, такую как пароли или данные банковских карт. Другие вирусы могут нанести вред системе, удаляя или изменяя файлы, вызывая сбои или замедление работы компьютера.

Как вирус заражает компьютер. Современный уровень развития автоматизированных систем обработки информации позволяет увеличить скорость передачи данных и совершать множественные преступления без особых финансовых и временных затрат.

Существуют несколько способов внедрения вируса в компьютер, например злоумышленник, может убедить вас установить вирус под видом полезной программы. Так же возможно, что в программном обеспечении вашего компьютера есть уязвимости. Попав на ваш компьютер, вирус может красть и удалять важные файлы, перехватывать контроль над другими программами, а иногда даже удаленно управлять вашим компьютером.

При помощи вирусов хакеры могут захватить миллионы компьютеров по всему миру и сделать из них цифровую армию «BotNet», с помощью которой можно атаковать и отключать веб-сайты. Такая распределенная атака называется «Отказ в обслуживании» или «DDOS». Она действует при помощи намеренной поломки одного или нескольких корпоративных устройств.

Чаще всего зараженные технические средства реагируют на манипуляции хакеров кратковременными перебоями в работе, чего зачастую хватает для поражения инфохранилищ. При полном доступе к системе программисты либо сразу загружают нужные файлы на собственные носители, либо заражают систему вирусом, который делает это за них. Бэкдоры в этом случае хороши тем, что их активацию можно провести удаленно.

Другой вид такой атаки заключается в предумышленной блокировке аккаунтов на важных сайтах после неправильного подбора пароля и логина хозяином. В результате этого пользователь не может войти и бросает все попытки это сделать. Цель такой атаки – воздействовать на нервное состояние жертвы. Заметим, что целью DDOS-атак зачастую не служат кражи данных или денег. Напротив, здесь, прежде всего, целью является порча репутации и доброго имени конкурирующего предпринимателя с умыслом обелить собственную биографию. Многим хакерам проведение таких схем заказывают участники конкурентных войн.

Еще один способ, которым пользуются хакеры это рассылка множества писем, чтобы обманом получить от людей ценную личную информацию. Такая атака называется «Фишинг». Попадаются на такие аферы чаще всего простые люди, у которых добычей могут стать их финансы. Похищать могут

логины и пароли от соцсетей, номера и данные карт, коды доступа к интернет-банкам. Словом, все, что поможет завладеть деньгами. После этого жертва остается без денег, а аферисты исчезают. При ней злоумышленник подсаживает жертву как бы на крючок, отправляя письма якобы от крупного и уважаемого сервиса с просьбой зайти на сайт, но по ссылке загрузиться поддельный веб-сайт, который внешне похож на оригинал, но принадлежит злоумышленнику. Введя на поддельном сайте логин и пароль, вы добровольно отдаете их хакеру, после чего он использует полученные данные, чтобы зайти под вашей учетной записью на настоящий веб-сайт и украсть ваши личные данные или денежные средства.

Защита от киберпреступления. Киберпреступления могут иметь серьезные последствия, такие как утечка конфиденциальной информации, финансовые потери, нарушение работы критической инфраструктуры и даже угроза жизни людей.

Для борьбы с киберпреступностью необходимо принимать меры на разных уровнях. Во-первых, компании и организации должны улучшить свою кибербезопасность, обеспечивая защиту своих систем и данных. Это включает в себя использование сильных паролей, регулярное обновление программного обеспечения, установку антивирусных программ и обучение сотрудников основам кибербезопасности.

Во-вторых, правительства должны разрабатывать и внедрять законы и политики, которые обеспечат эффективное пресечение киберпреступлений и наказание виновных. Это включает в себя создание специализированных служб, которые будут заниматься расследованием и предотвращением киберпреступлений.

В-третьих, необходимо развивать международное сотрудничество в области кибербезопасности. Киберпреступления часто имеют трансграничный характер, поэтому совместные усилия стран могут быть эффективны в борьбе с этой угрозой. Разработка общих стандартов и соглашений поможет улучшить защиту данных и систем на международном уровне.

Киберпреступления являются серьезной проблемой, которая требует немедленного внимания и действий. Только совместными усилиями государств, компаний и общества в целом можно справиться с этой угрозой и обеспечить безопасность в киберпространстве.

Список литературы

1. Национальный правовой Интернет-портал Республики Беларусь [Электронный ресурс] / Нац. центр правовой информ. Респ. Беларусь. – Режим доступа: https://pravo.by/ – Дата доступа: 28.10.2023.

2. Информационно-поисковая система Эталон-online / Режим доступа: https://etalonline.by/ - Дата доступа: 28.10.2023.

3. Информационно-правовая система Нормативка.by / Режим доступа: https://normativka.by/ - Дата доступа: 31.10.2023.

4. Онлайн-сервис Ilex / Режим доступа: https://ilex.by/ - Дата доступа: 01.11.2023.

5. Экономическая газета [Электронный ресурс] / Режим доступа: https://neg.by/ Дата доступа: - 01.11.2023.

6. Интернет-статья [Электронный ресурс] / Режим доступа: https:// www.ptsecurity.com/ - Дата доступа: 01.11.2023.