4. Техника для проверки подлинности денег/ Ресурс для IT-специалистов «Хабр» [Электронный ресурс]. – Режим доступа: https://habr.com/ru/post/185806/. – Дата доступа: 01.03.2023.

УДК 343.985.7:343.3/.7:004

КИБЕРПРЕСТУПНОСТЬ И КИБЕРКОНФЛИКТ В СОВРЕМЕННОМ МИРЕ

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

Не зря говорят, что XXI век – век активного пользования Интернетом. Всемирная паутина позволяет различным компаниям, учёным, организациям повысить эффективность труда. А также обеспечивает обмен идеями и информацией среди всех людей, находящихся на дальних расстояниях. Однако вместе с появлением Интернета в нашу жизнь вошли и такие понятия, как «киберпреступность», «кибератака», «кибероружие» и иные понятия с приставкой «кибер». Из-за резкого роста числа пользователей информационно-телекоммуникационных технологий, компьютеров и компьютерных сетей большинство людей уязвимы в киберпространстве. И в настоящее время киберпреступность, а именно преступления в киберпространстве, быстро стала серьёзной, опасной, чреватой значительными последствиями мировой проблемой. Нарушение кибербезопасности, кража данных и интеллектуальной собственности не знают границ, а атаки киберпреступников становятся всё более частыми и изощрёнными.

Киберпреступность происходит в пространстве, называемом виртуальным или информационным, содержащем данные о людях, фактах, событиях и процессах, которые перемещаются в локальных и глобальных компьютерных сетях или хранятся в памяти реальных или виртуальных устройств. Данный вид преступности отличается от всех остальных тем, что противоправные деяния обладают высокой степенью секретности, характеризующейся анонимностью и шифрованием. Можно добавить, что одной из самых главных особенностей является нахождение преступника и жертвы на расстоянии, протяжённость которого может достигать нескольких тысяч километров.

Киберпреступность – угроза безопасности? К несчастью, да. Появление глобальной сети открыло широкие возможности преступному миру для выхода на новый уровень, на котором виртуальное пространство широко используется злоумышленниками для совершения противоправных деяний.

Тем не менее, даже противоправная деятельность является одним из признаков этапа развития общества, и зарождение, развитие и распространение киберпреступлений и кибепреступности – это часть новейшей истории человечества, а не отдельного государства.

Отмечая и географическое распределение пользователей сети Интернет, можно говорить, что около 90% населения Европы, 55% населения Азии, 37% населения Африки, 95% населения Северной Америки и 73% населения Южной Америки являются пользователями Интернета. [1]

Также примечательным является и время, затрачиваемое на пользование Интернетом. В среднем, по миру оно составляет 6 часов и 42 минуты каждый день. На основе указанных показателей возможно сделать вывод о проникновении информационного пространства в значительную часть человеческой жизнедеятельности. Общественная опасность рассматриваемой проблемы признана на международном уровне.

На современном этапе киберпреступления в зависимости от последствий и масштаба можно разделить на две категории: киберпреступления на поражение компьютерных и информационно-телекоммуникационных систем государственных органов, международных организаций, крупных предприятий, государственных реестров, объектов критической инфраструктуры и других; киберпреступления индивидуального действия, направленные на завладение имуществом или информацией определённого лица, группы лиц или предприятия. [5]

Кроме того, хакеры могут атаковать пользователя через Интернет с помощью социальной инженерии. Суть данного способа получения конфиденциальной информации состоит в том, что правонарушитель взламывает учётную запись пользователя и получает доступ к конфиденциальной информации под различными предлогами, часто с согласия жертвы.

К довольно распространённому виду социальной инженерии относится вид мошенничества, при котором клиента под предлогами каких-либо маркетинговых акций уговаривают перевести деньги за товар, после чего продавец безвозвратно пропадает. Иной сценарий кибермошенников – отправка SMS-сообщений о том, что карта заблокирована и для её разблокировки необходимо позвонить по определённому номеру телефона. Для защиты от кибермошенников желательно соблюдать ряд правил: в случае оплаты услуг через сеть Интернет лучше использовать дополнительную карту, на которую легко можно будет переводить небольшие суммы денег (в случае компрометации данных такую карту достаточно просто заблокировать), а также рекомендуется регулярно проверять состояние банковских счетов. [2]

С каждым годом всё актуальней становится проблема, связанная с распространением вредоносных программ на мобильных устройствах. Сегодня

мобильный телефон не просто устройство связи, а необходимое почти для каждого человека ежедневно. Он помогает владельцу обеспечить доступ к любой информации через глобальную сеть, производить фото- и видеосъёмку, хранить данные, в том числе банковские конфиденциальные данные, которые могут быть считаны с помощью вирусов и затем использованы злоумышленниками для хищения денежных средств. А количество вирусов для мобильных устройств с каждым годом стремительно растёт. Однако всем известная установка только антивируса не обеспечивает необходимого уровня защиты, данную проблему нужно решать комплексной настройкой и изучением основ безопасности, к примеру, открывать вложения только от известных вам отправителей, всегда проверять их на наличие вирусов.

Многие сегодня рискуют стать жертвой скимминга, представляющего собой кражу данных карты при помощи специального считывающего устройства (скиммера). Злоумышленники копируют всю информацию с магнитной полосы карты (имя держателя, номер карты, срок окончания её действия, CVV- и CVC-код), могут узнать ПИН-код с помощью мини-камеры или накладок на клавиатуру, установленных на банкоматах. Стать жертвой скимминга можно не только снимая наличные, но и оплачивая покупки в торговых точках. К примеру, для копирования данных официанты, кассиры, служащие гостиниц могут использовать переносные скиммеры или устройства, прикреплённые к терминалу. [4]

Для защиты от скимминга банкиры рекомендуют использовать карты только в заслуживающих доверия торговых точках и интернет-магазинах. При оплате товаров в ресторанах, магазинах и т. д. следует не выпускать карту из вида, а деньги снимать в банкоматах, расположенных на охраняемой территории. [1]

Несмотря на то, что единый глобальный акт, который регламентировал бы порядок противодействия киберпреступлениям, пока ещё не выработан, международное сообщество предпринимает меры по борьбе с киберпреступлениями. В частности, недавно были подписаны договоры о кибербезопасности между Россией и Китаем, Китаем и США, Китаем и Великобританией, где в рамках этих документов государства обязуются не только сотрудничать, но и не допускать атаки друг на друга. [3]

Киберпреступность безусловно становится опасностью XXI века, а следовательно, кибербезопасность по значимости становится наряду с физической безопасностью, ведь не важно сколько сантиметров толщина стальной двери в хранилище, если она открывается с помощью компьютерной системы.

Литература

1. Торчков, Б.А. Анализ преступных деяний, совершенных в банковскоӗ сфере с использованием интернет технологий/ Б.А. Торчков, Л.А. Бураева // Пробелы в российском законодательстве, 2017. – No 5.– С. 211-212.

2. Бураева Л.А. Актуальные проблемы защиты информации в коммуникационных системах на современном этапе / Л.А. Бураева, Т.М. Шигонов. // Сборник материалов II Международноӥ научно-практическоӗ конференции. 2017. – С. 211-213.

3. Бураева Л.А. Мировоӥ опыт противодействия экстремизму и терроризму в глобальном информационном пространстве // Теория и практика общественного развития, 2015.

4. Словарь банковских терминов [Электронный ресурс]. – Режим доступа: https://www.banki.ru/wikibank. – Дата доступа: 30. 03. 2023.

5. Ковалькова, И. А. Киберугрозы, с которыми сталкиваются пользователи сети. // Информационные технологии в политических, социально-экономических и технических системах [Электронный ресурс] : материалы научно-практической конференции, 22 апреля 2022 года / Белорусский национальный технический университет, Факультет технологий управления и гуманитаризации ; редкол.: Г. М. Бровка (пред. редкол.) [и др.] ; сост. А. В. Садовская. – Минск : БНТУ, 2022. – С. 267-270.

УДК 001.83

БЕЛОРУССКО-КИТАЙСКОЕ НАУЧНО-ТЕХНИЧЕСКОЕ СОТРУДНИЧЕСТВО

Пшеничная Д.А.
Научный руководитель: ст. преподаватель Галай Т.А.
Белорусский национальный технический университет

Мир является свидетелем беспрецедентной волны глобализации, поскольку страны стремятся интегрировать свои экономики и общества друг с другом. В этом контексте международное научно-техническое сотрудничество становится все более важным аспектом глобализации. В последние годы Беларусь и Китай уделяют приоритетное внимание сотрудничеству в области науки и технологий как средству достижения взаимной выгоды и содействия устойчивому развитию своих экономик.

Белорусско-китайское научно-техническое сотрудничество является важным направлением сотрудничества двух стран в области науки и технологий. Это сотрудничество охватывает широкий спектр областей, включая