Лукьянова Надежда Владимировна
студентка
Калашникова Елена Борисовна
канд. ист. наук, доцент

ФГБОУ ВО «Самарский государственный
экономический университет»
г. Самара, Самарская область

DOI 10.21661/r-541342

КИБЕРПРЕСТУПНОСТЬ – КРИМИНАЛЬНАЯ УГРОЗА СОВРЕМЕННОГО МИРА

Аннотация*: в статье анализируются наиболее актуальные проблемы киберпреступности в банковской сфере. Методология исследования – анализ научной литературы по заданной проблеме, а также практического отечественного опыта.*

Ключевые слова*: киберпреступность, информационные технологии, банковская сфера, латентность, инструменты, эффективность, финансы.*

Мы живем в условиях, когда компьютер и другие информационные технологии используются во всех сферах общественной жизни, и, казалось бы, делают нашу жизнь и проще, и интереснее. Но заменяя человека телекоммуникациями, люди не могли представить, что создают для себя огромную угрозу. Именно с развитием информационного общества зарождается новый вид преступлений – киберпреступность.

Киберпреступность зародилась посредством глобализации информационных технологий, главные качества которых – легкость в использовании, анонимность, доступность и экономия времени.

С развитием информационных технологий увеличивается число преступлений в виртуальном пространстве. Однако, выявить достоверную картину

Content is licensed under the Creative Commons Attribution 4.0 license (CC-BY 4.0)

состояния киберпреступности ни то, чтобы на общемировом уровне, даже на государственном невозможно, поскольку она обладает высокой латентностью.

Для противодействия мошенничеству финансово-кредитные учреждения должны регулярно изучать положение безопасности своих каналов связи, а также обеспечивать безопасность своих электронных устройств.

Жертвами киберпреступников могут стать не только отдельные люди, но и целые государства. В принципе, ситуация в стране и отношение населения к этой проблеме, зависит от отношения государственных органов к мошенничеству и злоумышленникам. Но чтобы противостоять этой опасности необходимо сотрудничество международных организаций для защиты финансов и банковских систем.

Проблема киберпреступности заключается в масштабности её распространения. Вместе с глобализацией технологий и информации происходит распространение проблемы на мировом уровне. Поэтому вытекающим следствием из этого становится невозможность ограничить распространение преступности в рамках одного государства, а требует значимых исследований и выработки международных соглашений – от понятийного аппарата до унифицированного законодательства. Взаимодействие на национальном, региональном и международном уровне – это по мнению многих исследователей лучшее решение в борьбе против киберпреступности.

Но повышенный интерес к созданию международного законодательства с целью ликвидации дистанционных преступлений, не означает что Правительство не должно предпринимать никаких мер по борьбе с этой проблемой во внутренней политике. Из отчёта международной компании Group-IB в 2018 года мы видим, что в России ежегодно 1–2 банка становятся жертвами киберпреступников. Ущерб, нанесенный одной хакерской атакой, составляет примерно 132 млн руб.

Но России удалось снизить ущерб от киберпреступников путём создания специальной группы реагирования на чрезвычайные ситуации. Так, в 2017 году ущерб, приносимый стране мошенниками, составил 4,7 млрд руб., что составило

Содержимое доступно по лицензии Creative Commons Attribution 4.0 license (CC-BY 4.0)

на 0,8 млрд. руб. меньше, чем в предыдущем году. По мимо этого, российские финансово-кредитные учреждения пересмотрели свою политику в области кибербезопасности, были вынуждены выделить больше инвестиций на разработку и внедрение средств, обеспечивающие защиту от информационных преступлений. Таким образом, преступления, связанные с распространением вирусов на компьютеры крупных компаний, стали не под силу всем хакерам, что вынуждало менять тактику осуществления своих схем и это привлекало их интерес.

Актуальным и наиболее успешным вариантом осуществления финансовых краж в современном обществе, где человечеству присуще такие качества как наивность, тяга к выгоде, неграмотность, считается – рассылка сообщений абонентам, которые якобы содержат заманчивые предложения, но на самом деле, открыв такое предложение, человек подвергает своё устройство активизации вирусов. Такие вирусы имеют различные формы действия, ярким примером служит – автоматическое списание определенной суммы денег у абонента, а иногда даже данное сообщение рассылается по всем контактам, и выгода хакеров, соответственно, умножается в разы. Пик такого финансового мошенничества пришелся на 2018 г., тогда вирусы похищали денежные средства клиентов, если у них на телефоне был установлен мобильный клиент банка.

Киберпреступность не поддаётся контролю со стороны должных органов, поэтому бороться с ней достаточно сложно, порой даже невозможно. В отчаянной борьбе за существование кибербезопасности необходимо создание соответствующих актов на региональном уровне, что невозможно предпринять без мирового сотрудничества. Осуществление политики в данном направление было бы некорректно и бесполезно без создания новых актов или внесения поправок в существующее национальное законодательство страны в этой же сфере отношений. Это делается для того, чтобы не было пробелов и противоречий в национальном и международном праве. Государство должно быть в постоянной боевой готовности для обеспечения быстрого реагирования на развитие компьютерных технологий и принятия соответствующих мер. В настоящее время в формировании международной стратегии борьбы с киберпреступностью

Content is licensed under the Creative Commons Attribution 4.0 license (CC-BY 4.0)

задействованы более сорока стран мира, и процесс этот обещает быть достаточно долгим. Однако, несмотря на все сложности, очевидно, что международному сообществу необходимо прийти к решению проблем унификации законодательства. В противном случае, с учетом выхода за пределы отдельного государства, такого явления как киберпреступность, определенные несоответствия в законодательстве и не подчинённость виртуальных преступлений уголовной политики позволят лицам, совершившим общественно опасные действия, избегать ответственности, поскольку расследование преступлений и преследование правонарушителей в развитом обществе всё ещё представляет некие затруднения.

Список литературы

1. Калашникова Е.Б. Актуальные проблемы киберпреступности в банковской сфере // Институт стратегических исследований. – 2019.

2. Курушин В.Д. Компьютерные преступления и информационная безопасность / В.Д. Курушин, В.А. Минаев. – М., 2018.

3. Калашникова Е.Б. Основные механизмы, используемые при отмывании преступных доходов, полученных от кибердеятельности / Е.Б. Калашникова, М.А. Архипов// Аллея Науки. – 2018 – №11 (27).

4. Немов М.В. Киберпреступность как новая криминальная угроза // Эпоха науки. – 2017.

5. Простосердов М.А. Экономические преступления, совершаемые в киберпространстве, и меры противодействия им. – 2016.

Содержимое доступно по лицензии Creative Commons Attribution 4.0 license (CC-BY 4.0)