Секция «Обеспечение финансовой безопасности России: финансовые расследования в цифровой экономике»

Киберпреступления в России: тенденции развития и возможности предотвращения

Научный руководитель – Кузовлева Нина Федоровна

Гречишкина Алиса Дмитриевна

Студент (специалист)

МИРЭА - Российский технологический университет, Институт комплексной безопасности и специального приборостроения, Кафедра «Экономическая безопасность», Москва, Россия

E-mail: alisagrechishkina@gmail.com

Самым распространенным типом киберпреступности являются киберпреступления экономического характера, поскольку обусловлены получением финансовой выгоды, например, от воровства денежных средств со счетов организации и утечки корпоративной информации с целью перепродажи данных конкурентам.

С начала 2022 года, по словам главы МВД России Владимира Колокольцева, сумма ущерба от IT-преступлений в России составила 65 млрд рублей. Отмечается, что эта сумма на 20% больше той, что была в 2021 году. Возможный ущерб от киберпреступности в 2022 году оценивается в 165 млрд рублей [6].

В 2022 году в России было зафиксировано около 510 тыс. преступлений с использованием информационных технологий против 10 тыс. в 2014 году. Речь идет о более чем 50-кратном росте числа ИТ-преступлений [8].

В 2022 году по данным «Ростелеком-Солар» на российские компании было совершено 911 тыс. хакерских атак [9], 65% которых имели целенаправленный характер. Жертвами подобных атак стали госучреждения, медицинские учреждения, промышленные компании, IT-компании и др.

По данным Генпрокуратуры России в общем объеме киберпреступлений почти половину составили случаи мошенничества (48%). Причем, если число краж с банковских карт сократилось на 28%, количество мошенничеств с электронными денежными средствами выросло на 4,4%.

Вместе с тем, необходимо отметить, что в 2021 году Россия заняла пятое место в рейтинге кибербезопасности, получив 98,06 балла из 100 возможных и разделив данную позицию с ОАЭ и Малайзией. В 2018 году Россия находилась лишь на 28 месте [7].

Уязвимость российских компаний перед хакерами связана с нехваткой ИТ-специалистов для обеспечения полноценной защиты, импортозамещением значимых систем и переходом на продукты типа OpenSource.

В Российской Федерации отсутствует Концепция кибербезопасности на уровне государства. В 2010 году был разработан проект концепции – создать государственный механизм защиты и ужесточить ответственность за киберпреступления, а также обеспечить приоритет отечественных IT-компаний [1].

Проект концепции подразумевает трехуровневую систему защиты в этой сфере:

- на уровне государства должны решаться вопросы правового регулирования, координация действий участников процесса;
- на уровне бизнеса необходимо обеспечивать надежность наиболее важных объектов инфраструктуры, соответствие государственным стандартам;

- на уровне общества должны решаться вопросы повышения уровня цифровой грамотности населения и участия в оценке компетенции государства и бизнеса.

Документ не был принят по следующей причине: термин "кибербезопасность" используется в западных странах. В России принято понятие "информационная безопасность" в таких нормативно-правовых актах как Стратегия национальной безопасности Российской Федерации и Доктрина информационной безопасности Российской Федерации. Документы определяют информационную безопасность как «состояние защищённости личности, общества и государства от внутренних и внешних информационных угроз», где вопросы безопасности информационных технологий, действий в киберпространстве являются одним из уровней обеспечения защиты от киберугроз [2].

Понятие "информационная безопасность" шире понятия "кибербезопасность", к тому же, между этими терминами имеется принципиальное различие. Кибербезопасность – это защита коммуникационных каналов (в частности интернета) и аппаратуры, информационная безопасность распространяется и на контент. Руководствуясь понятием "информационная безопасность", Россия к угрозам относит действия, совершаемые "с целью подрыва политической, экономической систем другого государства, психологическую обработку населения" [4].

В России должна быть принята Концепция кибербезопасности, поскольку киберугрозы продолжают иметь место и совершенствоваться. Кроме того, в Российской Федерации не сформирован категориальный аппарат в сфере кибербезопасности, отсутствует системный подход к решению вопросов повышения грамотности населения в области информационной безопасности. Вместе с тем, киберпреступления определяются как общественно опасные действия, совершенные в информационно-телекоммуникационной сфере посредством применения информационно-коммуникационных технологий [3].

Для борьбы с киберпреступлениями в экономической сфере необходимо:

- принятие общесистемных мер по обеспечению кибербезопасности;
- дальнейшее развитие нормативно-правовой базы обеспечения кибербезопасности;
- обеспечение реального инвестирования в современные системы защиты данных;
- подготовка кадрового потенциала в сфере обеспечения кибербезопасности;
- организация внутреннего и международного взаимодействия по проблемам кибербезопасности;
- формирование и развитие культуры безопасного поведения в киберпространстве[5].

Только путем совместных усилий государства, бизнеса и общества можно добиться эффективного противодействия киберпреступности и обеспечить дальнейшую цифровизацию экономики Российской Федерации.

Источники и литература

1) Концепция стратегии кибербезопасности Российской Федерации. Проект. http://council.gov.ru/media/files/41d4b3dfbdb25cea8a73.pdf (дата обращения: 15.01.2024)

2) Бородакий Ю.В., Добродеев А.Ю., Бутусов И.В. Кибербезопасность как основной фактор национальной и международной безопасности XXI века (часть1) https://docs.yandex.ru/docs/view?tm=1706037494&tld=ru&name=Kiber_Bezop_-– (дата обращения: 23.01.2024)

3) Клишков В.Б., Стебенева Е.В. Киберпреступность: понятие, признаки, основные направления противодействия. Вестник Нижегородского университета им. Н.И. Лобачевского, 2022, № 4, с. 106–114 http://www.unn.ru/pages/e-library/vestnik/19931778_2022_-_4_unicode/14.pdf (дата обращения 15.01.2024)

4) Концепция кибербезопасности разошлась с государственной стратегией https://www.kommersant.ru/doc/2355154?ysclid=lrqsiqedl0415509127 (дата обращения 15.01.2024)

5) Тихонова А. В. Информационные технологии и безопасность // Перспективы развития информационных технологий. 2013. №12. URL: https://cyberleninka.ru/article/n/informatsionnye-tehnologii-i-bezopasnost (дата обращения: 23.01.2024)

6) Потенциальный ущерб от киберпреступности в 2022 году оценили в 165 млрд рублей. Об этом сообщает "Рамблер" https://news.rambler.ru/sociology/48152500/?utm_content=news_media&utm_medium=read_more&utm_source=copylink (дата обращения: 15.01.2024)

7) Global Cybersecurity Index 2020 https://num.radiosit.ru/indexes/globalnyy-indeks-kiberbezopasnosti-2020.html?ysclid=lrpa8p9ga6874385212 (дата обращения: 15.01.2024)

8) Число киберпреступлений в России https://www.tadviser.ru/index.php/%D0%A1%D1%82%D0%B0%D1%82%D1%8C%D1%8F:%D0%A7%D0%B8%D1%81%D0%BB%D0%BE_%D0%BA%D0%B8%D0%B1%D0%B5%D (дата обращения: 15.01.2024)

9) Число кибератак в России и в мире https://www.tadviser.ru/index.php/%D0%A1%D1%82%D0%B0%D1%82%D1%8C%D1%8F:%D0%A7%D0%B8%D1%81%D0%BB%D0%BE_%D0%BA%D0%B8%D0%B1%D0%B5%D (дата обращения 23.01.2024)