КИБЕРПРЕСТУПНОСТЬ КАК УГРОЗА МЕЖДУНАРОДНОЙ БЕЗОПАСНОСТИ

И. Э. Жадан[1], Л. Н. Мамаева[2]

[1]*Саратовский национально-исследовательский государственный университет им. Н. Г. Чернышевского, Россия*
[2]*Социально-экономический институт СГТУ им. Ю. А. Гагарина, Саратов, Россия*
E-mail: inga645@bk.ru, l.mamaeva2014@yandex.ru

Научная статья раскрывает такую важную и актуальную на сегодняшний день тему как киберпреступность, и какую угрозу она несет в международном масштабе. Отмечается, что развитие цифровых технологий и активное их использование во всех областях хозяйственной деятельности привело к стремительному распространению киберпреступности и ее появлению в перечне глобальных угроз. В научной статье предлагаются решения проблем экономической безопасности.

CYBERCRIME AS A THREAT TO INTERNATIONAL SECURITY

I. E. Жадан, L. N. Mamaeva

The scientific article reveals such an important and relevant topic as cybercrime, and what threat it poses on an international scale. It is noted that the development of digital technologies and their active use in all areas of economic activity has led to the rapid spread of cybercrime and its appearance in the list of global threats. The scientific article offers solutions to the problems of economic security.

Глобальное освоение новых цифровых технологий и активная цифровизация бизнес-процессов, внедрение цифровых технологий в работу промышленных предприятий, государственных органов и финансовых учреждений, а также активное их использование людьми в повседневной жизни, приводит к росту угроз, связанных с утечкой информации и открывает новые возможности перед киберпреступниками [1.С.58]. На современном этапе киберпреступность наносит значительный ущерб как отдельным гражданам, организациям и предприятиям во всем мире, так и экономикам различных государств в целом и с развитием информационных технологий этот ущерб будет продолжать расти.

В 2019 году кибератаки и незаконная деятельность хакерских групп стали одной из главных угроз международной кибербезопасности. Разрушительный потенциал кибератак становится все более очевиден, особенно в области геополитических угроз. Особое внимание стоит уделить рискам, связанным с массовой утечкой данных, которые усиливают влияние кибератак на глобальную экономику. Киберпреступность наносит не только прямой ущерб бизнесу и экономике, но и сдерживает развитие инноваций.

Одной из причин ускоренного роста киберпреступности являются техно-

логические тренды. К 2022 году к глобальной сети Интернет будет подключен 1 трлн устройств. К 2023 году у 80% людей появится аватар в цифровом мире. При этом более 50% трафика домохозяйств в 2014 году будут потреблять умные устройства и бытовая техника.

Растущие угрозы целостности данных подрывают доверие к ранее надежным системам и могут причинить физический и материальный ущерб в случае повреждения критической инфраструктуры.

Ежегодно эксперты Международного союза электросвязи (International telecommunication Union) при ООН составляют рейтинг стран по уровню кибербезопасности под названием «Глобальный индекс кибербезопасности» (Clobal Cybersecurity index). Глобальный индекс кибербезопасности основывается на исследованиях 195 стран мира. При составлении рейтинга эксперты принимали во внимание пять показателей:

1. Наличие правовых систем и структур, занимающихся вопросами кибербезопасности и киберпреступлений
2. Технические возможности в области кибербезопасности
3. Существование институтов координации политики и стратегий развития кибербезопасности на государственном уровне
4. Наличие научно-исследовательских, образовательных и подготовительных программ, а также сертифицированных специалистов и госучреждений, способствующих наращиванию потенциала в сфере информационной безопасности.
5. Наличие партнеров, механизмов сотрудничества и систем обмена информацией.

По результатам отчета Глобального индекса кибербезопасности за 2017 год 1-е место занял Сингапур, 2-е место США, 3-е место Малайзия. Россия в этом рейтинге находится на 11 месте.

Сингапур и Малайзия находятся в Азиатско-Тихоокеанском регионе, где, по данным Всемирного экономического форума, киберпреступность и кибератаки входят в пятерку основных бизнес-рисков. США также входит в число стран, уделяющих особое внимание проблеме кибербезопасности и уступает лишь Сингапуру. Однако инфраструктура в США все же уязвима перед киберпреступностью, которая по данным Всемирного экономического форума рассматривается в качестве главного бизнес-риска на территории Северной Америки, а именно крупномасштабных кибератак или воздействия вредоносных программ, вызывающих крупные экономические убытки, геополитическую напряженность или повсеместную потерю доверия к сети Интернет.

Согласно данным компании Positive Technologies, которая специализируется на разработке программного обеспечения в области информационной безопасности, самой атакуемой страной за 2018 год является США (41% всех атак), на втором месте находится Россия – 10% и на третьем месте – Великобритания 7 5). В целом атакам подвергались не менее 26 стран мира.

Наибольшее число атак направлено на государственные учреждения, на них пришлась каждая пятая атака, что составило – 20 %. Предпосылками для

этого может служить обостренная как внешняя, так и внутренняя политическая обстановка многих стран. Социальные сети, поисковые системы, интернет-магазины и онлайн-сервисы стали целью каждого девятого нападения – 11%. Немного лучше ситуация в финансовой отрасли – на банки пришлось 9 % всех инцидентов. Далее следует сфера образования 8 %. Медицинские учреждения и сфера услуг по 7 %, промышленные компании 5 % и оборонные предприятия 3 %.

Растущей тенденцией является использование кибератак против критической информационной инфраструктуры и стратегических секторов экономики. Ландшафт угроз критической инфраструктуры продолжает усложняться за счет хакерских групп. Далее в научной статье приведен перечень наиболее активных APT-групп, а также география их деятельности.

Следует отметить, что хакерские группы сегодня это профессиональные и высокоорганизованные структуры с вертикальной структурой управления.

Появление криптовалют и активное развитие блокчейн-проектов привело к изменению ландшафта угроз для криптовалютного рынка и появлению новых схем для кражи криптовалют и взлома торговых площадок. Большинство мошеннических схем, используемых для хищения криптовалют, аналогичны тем. Что используются на традиционных рынках. Особое внимание хакеры уделяют атакам на ICO-проектам. Около 56 % средств, похищенных в ходе ICO, были похищены в ходе фишинговых атак. Несомненно, блокчейн-технологии меняют привычную логику и отбрасывают необходимость в посредниках, но как мы можем наблюдать они в свою очередь несут и множества угроз [3.С.54].

Если в 2017 году ущерб мировой экономики от киберпреступлений составил 600 млрд долларов США, в 2018 году 1,5 трлн долларов США, то уже в 2019 году – 2,5 трл долларов. К 2022 году, по прогнозу Всемирного экономического форума, сумма планетарного ущерба от кибератак вырастет до 8 трл долларов США. [4.С.54].

В последнее время мы можем наблюдать возникновение нового вида преступности – организованной киберпреступности, которое заставляет экономических агентов и государство выделить основные задачи по предотвращению киберугроз в следующих направлениях: безопасность информационных систем; защита персональных данных; защита рабочей среды, технологий и инструментов.

Особое внимание стоит уделить вопросу кибервойн. Кибератаки становятся поводом для политических спекуляций и как следствие, причиной международных конфликтов.

Основные подходы связаны со строительством инфраструктуры борьбы с киберпреступностью на международном уровне, образованием, технологическим совершенствованием ИТ-программного обеспечения и аппаратного обеспечения, регулированием, использованием финансов и страхования, поддержкой средств массовой информации и созданием кибер- преступления awareculture.

Следует отметить, что в данном вопросе невозможно противостоять ки-

берпреступности силами одной страны, необходима консолидация усилий не только на национальном, но и на международном уровне, а также принятия международных правил поведения в киберпространстве. В связи с этим возникает необходимость в создании наднациональных институтов, регулирующих киберпространство и глобальную сеть Интернет.

Также необходимо сократить разрыв между практикой и законодательством в информационной сфере. Данный разрыв во многом связан со стремительным развитием информационных технологий и затянутой практикой разработки и применения нормативно-правовых актов.

Для обеспечения кибербезопасности как на уровне государства, так и на международном уровне необходимо выработать системный подход включающий в себя не только повышение осведомленности относительно существования рисков в киберпространстве, создание национальных структур, занимающихся вопросами кибербезопасности, но и установление необходимых взаимоотношений между отраслями экономики, а также сотрудничество между членами мирового сообщества

СПИСОК ЛИТЕРАТУРЫ

1. *Жадан И. Э., Мамаева Л. Н.* Влияние кибербезопасности на национальную безопасность России // Материалы X Международной научно- практической конференции, СГНИУ имени Н.Г. Чернышевского. 2019. 235 с.

2. *Мамаева Л. Н., Гребенщиков Н. А.* Блокчейн как новый этап развития цифровой экономики // Экономическая безопасность и качество. 2018. № 4 (33).

3. *Мамаева Л. Н., Лазарева В. А., Рыбакова К. С., Кирюхина М. В*. Безопасность финансовой системы в рамках появления криптовалюты // Экономическая безопасность и качество. 2018. № 1 (30).

4. *Лавров С. В.* Глобальные проблемы кибербезопасности и международные инициативы России по борьбе с киберпреступностью // Внешнеэкономические связи. 2020. [Электронный ресурс]. URL: https://statya-ministra inostrannykh-del-rossiyskoy-federatsii-s-v-lavrova-problemy-kiberbezopasno/ (дата обращения: 01.10.2020).