ИССЛЕДОВАНИЯ ЧЕЛОВЕКА И СОЦИАЛЬНЫХ СИСТЕМ

УДК 343.98

Ахметов А.Р., студент, Набережночелнинский институт ФГАОУ ВО «Казанский (Приволжский) федеральный университет»

РОСТ КИБЕРПРЕСТУПНОСТИ В РОССИЙСКОЙ ФЕДЕРАЦИИ: ДЕТЕРМИНАНТЫ И МЕРЫ ПРОТИВОДЕЙСТВИЯ

Аннотация: Статья посвящена исследованию детерминант и мер противодействия роста киберпреступности в Российской Федерации. В материале рассматриваются меры, которые принимаются современной пассивной, бюрократизированной и инертной российской правоохранительной системой, столкнувшаяся с чрезвычайно гибким и умным противником, влияние которого долгое время не принималось во внимание. Автором было выявлено, что применяемые меры по борьбе с киберпреступностью носят запоздалый характер и являются ответом на уже совершенные преступления, поэтому возникает острая необходимость применять сформированные в результате исследования эффективные методы борьбы, требующие иной подход, отличный от традиционных стратегий, применяемых в отношении других преступлений.

Ключевые слова: киберпреступность, детерминанты, ИТ-специалисты, меры противодействия, законодательство, правоохранительная система.

В современном мире развитие и использование информационно-телекоммуникационных систем стало неотъемлемой частью жизни каждого, охватывая все аспекты человеческой жизнедеятельности, где информация является ключевым активом, защита данных и систем становится всё более критической. Однако параллельно с этим ставится принципиальный вопрос об актуальном состоянии преступности в Российской Федерации в поле киберпространства, которая находится в постоянном движении, создавая новые возможности для совершения киберпреступлений и, следовательно, представляя угрозу для глобальных информационных сетей и общества в целом [1, С.24]. Непредсказуемость тенденций развития технологий в целом и киберпреступности в частности — непременно одна из важнейших вызовов

для человечества, которая затрудняет прогнозирование процесса цифровизации и попытки урегулирования общественных отношений в ней. В этой связи, особое значение принадлежит обеспечению национальной безопасности Российской Федерации [2], включающей в себя государственную, правовую, общественную, экономическую, экологическую, энергетическую и личную безопасность.

Актуальность исследования обусловлена тем, что за последние семь лет в РФ киберпреступность, согласно статистике и опубликованных данных Министерства внутренних дел Российской Федерации (далее – МВД РФ), демонстрирует колоссальный шестикратный рост. В 2017 году подобных преступлений было 90 тыс., в 2018 году – 121 тыс., в 2019 году – 294,4 тыс., в 2020 году – 510,3 тыс., в 2021 году – 517,7 тыс., в 2022 году – 522 тыс., в 2023 году – 676,9 тыс. В январе-июне текущего года количество зарегистрированных в Российской Федерации киберпреступлений составило 368,7 тыс., что на 409,7% превышает показатели преступности в 2017 году [3]. Вдобавок, в 2022–2023 годах Российская Федерация столкнулась с новой волной киберпреступности, которая исходит преимущественно из-за рубежа и нацелена не только на граждан, но и на объекты критической инфраструктуры. Учитывая давление со стороны недружественных стран, сложившуюся на международной геополитической карте ситуацию, специфику российского законодательства и глобальный рост киберпреступности, модернизация российской правоохранительной системы становится всё более актуальной задачей. Последние несколько лет показали, что правоохранительная система с методами и подходами прошлого века неэффективна в борьбе с вызовами XXI века, включая киберпреступность.

Проблема заключается в том, что российская громоздкая и инертная система принятия и исполнения решений не отвечает вызовам со стороны киберпреступности – очень быстрого и адаптивного врага, который быстро находит уязвимости этой системы и активно их эксплуатирует. Кроме этого, одним из основных трендов в сфере киберпреступлений за последние годы

является увеличение количества случаев социальной инженерии. Действительно, в последнее время наблюдается смещение акцента с технологий на людей — самых уязвимых участников системы, поскольку каждому человеку свойственно ошибаться, испытывать когнитивные искажения или эмоции. Применение социальной инженерии в этом контексте можно рассматривать как мотив и повод для использования естественных слабостей людей.

В современности со стороны преступного сообщества происходит постоянное тестирование новых преступных схем и их распространение на большое количество потенциальных жертв. В таких обстоятельствах правоохранительные органы, законодательство и информационные ресурсы не всегда успевают адаптироваться к новым способам мошенничества. Эта проблема подчёркивает необходимость разработки комплексного подхода к постоянной и результативной профилактике киберпреступлений.

В этой связи, несмотря на довольно широкую законодательную базу, которая включает в себя Доктрину информационной безопасности Российской Федерации, федеральные законы «Об информации, информационных технологиях и о защите информации», «О персональных данных», «О техническом регулировании» и пр., на законодательном уровне лишь поднимаются вопросы о важности решения проблем в сфере борьбы с киберпреступностью, не воплощая закрепленную в них политику государства в полном объеме. Тем не менее, потенциал может быть реализован благодаря повышению эффективности расследования киберпреступлений правоохранительными органами, а также усилению мер по предотвращению киберпреступлений: в некоторых случаях предупреждение киберпреступления будет более целесообразным, нежели устранение его последствий. Представляется, что решения можно разбить на несколько ключевых мер и методов:

Во-первых, необходимо провести более масштабную, глубокую и системную работу с населением по повышению осведомлённости, цифровой грамотности и образованности.

Во-вторых, выполнить модернизацию правоохранительных органов, которые оказались не готовы к быстрому переходу преступности в цифровой сектор. Здесь важно указать на то, что в соответствии с Указом Президента Российской Федерации от 30 сентября 2022 г. № 688 было создано Управление МВД РФ по организации борьбы с противоправным использованием информационно-коммуникационных технологий. В свою очередь это не должно приостанавливать процесс подготовки высококвалифицированных ИТ-специалистов, а напротив уделять особое внимание на совершенствование обучения сотрудников, формированию компетенций у каждого сотрудника и выпускника ведомственных образовательных организаций, закрывая кадровый голод.

В-третьих, провестим более тесное международное сотрудничество, необходимость которого вытекает из трансграничной сущности киберпреступности.

В-четвертых, решить проблему нехватки высококвалифицированных специалистов важно как для российской IT-индустрии в целом, чтобы создавать надёжные и защищённые цифровые системы, так и для правоохранительных органов для успешного расследования преступлений и проведения превентивных мероприятий. В 2022 году российское государство столкнулось с масштабной, серьёзной волной отъезда квалифицированных кадров, в том числе и ИТ-специалистов [4, С.238].

В-пятых, выделить дополнительное финансирование на проекты по борьбе с киберпреступностью, поскольку в настоящее время в правоохранительных органах прослеживается проблема, где система материального поощрения не позволяет привлекать и удерживать перспективных, квалифицированных специалистов, которые бы позволяли быстро раскрывать и своевременно пресекать преступления.

В-шестых, эффективное и оперативное сотрудничество правоохранительных органов, банков и операторов связи для блокировки мошеннических сайтов и номеров.

В-седьмых, совершенствование российского законодательства в сфере информационных технологий. Так, в нынешних реалиях прослеживается необходимость «полного обновления норм, регулирующих сеть «Интернет Действующие уголовные нормы, которые определяют ответственность за такие преступления, не адаптированы к новым видам преступных действий в сфере информационно-коммуникационных технологий [5, С.101]. Существует необходимость детально проработать национальное законодательство и международные акты, предусматривающие ответственность за совершение киберпреступлений [6, С.320].

В-восьмых, необходимо обеспечить более активную поддержку российских стартапов и инициатив в сфере информационной безопасности, которая выражается в интеграции российской коммерческой экспертизы с государственными структурами и правоохранительными учреждениями.

Из представленного анализа можно сделать вывод о том, что нынешнее состояние киберпреступности требует принятие необходимых мер для недопущения ухудшения ситуации. С массовым распространением электронной коммерции, онлайн-банкинга, удалённой работы и других видов активности в цифровой среде, использующих информационные технологии, преступники не могли не воспользоваться этими возможностями. Технологии, обеспечивающие анонимность, скрытие следов преступлений и подделку голоса или изображений, повышают вероятность совершения преступлений без негативных последствий для злоумышленников. Рост киберпреступности в России является результатом несовершенства законодательства перед лицом такого умного и адаптивного противника. Пассивная, забюрократизированная и инертная система столкнулась с чрезвычайно гибким и умным врагом, влияние которого долгое время

недооценивалось. Сегодня этот враг представляет серьёзную угрозу для самой системы.

Применяемые меры по борьбе с киберпреступностью носят запоздалый характер и являются ответом на уже совершенные преступления. Однако в борьбе с таким быстрым и адаптивным врагом такая стратегия заведомо проигрышна: когда законодатели обсуждают законопроекты по пресечению одной преступной схемы, преступники активно тестируют новые методы. В связи с этим предлагаем:

1)выделить дополнительное финансирование на проекты по борьбе с киберпреступностью;

2)решить проблему нехватки высококвалифицированных специалистов;

3)установить систему эффективного и оперативного сотрудничества правоохранительных органов, банков и операторов связи для блокировки мошеннических сайтов и номеров;

4)провести работу по совершенствованию российского законодательства в сфере информационных технологий;

5)выполнить полную модернизацию правоохранительных органов;

6)провести более масштабную, глубокую и системную работу с населением по повышению осведомлённости, цифровой грамотности и образованности.

Таким образом, для эффективной борьбы с таким противником требуется иной подход, отличный от традиционных стратегий, применяемых в отношении иных преступлений.

Список использованных источников

1. Баланов А.Н. Защита информационных систем. Кибербезопасность: учебное пособие / А.Н. Баланов. – Санкт-Петербург: Лань, 2024. – 280 с.

2. О Стратегии национальной безопасности Российской Федерации: указ Президента РФ от 02.07.2021 №400 // Собрание законодательства РФ. – 2021. – № 27 (часть II). – Ст. 5351.

3. Интернет-ресурс: Краткая характеристика состояния преступности в Российской Федерации [Заглавие с экрана] – URL: https://xn--b1aew.xn--p1ai/reports/item/41741442 (Дата обращения: 10.10.2024).

4. Швыряев П.С. Кадровая обеспеченность в сфере информационных технологий в России: проблемы и перспективы / П.С. Швыряев // Государственное управление. Электронный вестник. – 2023. – № 97. – С. 231-240.

5. Кобец П.Н. Правовые основы предупреждения киберпреступлений: отечественный и зарубежный опыт / П.Н. Кобец // Научный вестник Омской академии МВД России. – 2022. – № 2. – С. 101-105.

6. Долженко Н.И., Хмелевская И.Г. К вопросу о содержательных аспектах киберпреступности / Н.И. Долженко, И.Г. Хмелевская // Философия. Социология. Право. – 2020. – Том 45. – № 2. – С. 315-322.

Akhmetov A.R., student, Naberezhnye Chelny Institute, Kazan (Volga Region) Federal University.

THE RISE OF CYBERCRIME IN THE RUSSIAN FEDERATION: DETERMINANTS AND COUNTERMEASURES

Abstract: The article is devoted to the study of the determinants and measures to counter the growth of cybercrime in the Russian Federation. The article examines the measures that are being taken by the modern passive, bureaucratic and inert Russian law enforcement system, which is faced with an extremely flexible and intelligent opponent, whose influence has not been taken into account for a long time. The author revealed that the measures taken to combat cybercrime are belated and are a response to crimes already committed, therefore there is an urgent need to apply effective methods of combating formed as a result of the study, requiring a different approach from traditional strategies used in relation to other crimes.

Keywords: cybercrime, determinants, IT specialists, counteraction measures, legislation, law enforcement system.