УДК 349

ПРОТИВОДЕЙСТВИЕ КИБЕРПРЕСТУПНОСТИ В РОССИЙСКОЙ ФЕДЕРАЦИИ И МИРОВОМ ПРОСТРАНСТВЕ: СОВРЕМЕННЫЕ ТЕНДЕНЦИИ

В. С. Сахаров

Научный руководитель: Г. П. Лозовицкая, профессор, д.ю.н., доцент

ФГБОУ ВО "РЭУ им. Г.В. Плеханова", РЭУ им. Г.В. Плеханова,

г. Москва, Россия

Аннотация*:* Данная научная статья посвящена исследованию проблемы киберпреступности в Российской Федерации и в мировом пространстве. В работе рассматриваются основные виды киберпреступлений, а также методы борьбы с ними, используемые правоохранительными органами РФ и других стран. Анализ проводится на основе данных о количестве зарегистрированных случаев киберпреступлений за последний период времени. В результате работы было выявлено, что эффективность борьбы с киберпреступностью напрямую зависит от уровня развития информационных технологий и законодательства в данной области. Однако необходимость постоянного повышения компетенции специалистов-экспертов является ключевой задачей для успешной борьбы с этим видом преступности как на государственном уровне, так и на международном уровне

Ключевые слова: киберпреступность, компьютерные технологии, данные, экономика, бизнес.

Countering cybercrime in the Russian Federation and in the global space: current trends

V. S. Sakharov

Scientific supervisor: G. P. Lozovitskaya, Professor, Doctor of Sciences, Associate Professor

PLEKHANOV Russian University of Economics, PLEKHANOV

Russian University of Economics, Moscow, Russia

Abstract: This scientific article is devoted to the study of the problem of cybercrime in the Russian Federation and in the global space. The paper examines the main types of cybercrimes, as well as methods of combating them used by law enforcement agencies of the Russian Federation and other countries. The analysis is carried out on the basis of data on the number of registered cases of cybercrime over the last period of time. As a result of the work, it was revealed that the effectiveness of the fight against cybercrime directly depends on the level of development of information technologies and legislation in this area. However, the need to constantly improve the competence of expert specialists is a key task for the successful fight against this type of crime both at the state level and at the international level

Keywords: cybercrime, computer technology, data, economy, business.

Кибербезопасность в современном мире приобрела глобальный характер, а кибератаки становятся все более сложными и масштабными. В системе гражданского и уголовного правосудия компьютерная криминалистика помогает обеспечить целостность цифровых доказательств, представленных в судебных делах. Целью данного исследования является разработка научно обоснованных предложений и рекомендаций по внедрению инструментов для криминалистического исследования компьютерных средств и систем в борьбе с киберпреступностью. Актуальность данного исследования обусловлена необходимостью внедрения активных способов защиты и борьбы с киберпреступностью. Для достижения цели исследования были использованы методологические принципы и подходы юридической науки.

Объектом исследования являются общественные отношения, возникающие при осуществлении информационных процессов по производству, сбору, обработке, накоплению, хранению, поиску, передаче, распространению и потреблению компьютерной информации, а также в других областях, где используются компьютеры, компьютерные системы и сети.

Предмет исследования - особенности уголовных правонарушений в области использования электронных вычислительных машин (ЭВМ), систем и компьютерных сетей и телекоммуникационных сетей, и противодействия киберпреступности.

Одним из основных вопросов является рассмотрение юрисдикции киберпреступности, поскольку цифровой мир не имеет четко определенных границ и географических зон. По этой причине принцип гражданства обычно используется для определения юрисдикции, например, это может быть связано с гражданством правонарушителя (принцип активной личности) или гражданством жертвы (принцип пассивной личности). Что объединяет большинство стран, так это то, что интернет-провайдеры обязаны хранить пользовательские данные и предоставлять их следователям по запросу. Некоторые страны устанавливают юрисдикцию даже за преступление, совершенное в другом государстве, если оно затронуло интересы и безопасность страны за рубежом (принцип защиты). В исследовании рассматривается опыт России через призму мирового опыта противодействия киберпреступности.

Предлагается шире использовать компьютерные криминалистические методы исследования в борьбе с киберпреступностью. Авторы обнаружили отсутствие нормативного механизма для регулирования кибербезопасности, сбора и использования цифровых доказательств и нормативной базы для международного сотрудничества. К выявленной необходимости в укреплении международного сотрудничества и в разработке соответствующей политики и законодательных инициатив в области безопасности и сетевых и информационных систем, совершенствовании законодательства в области противодействия киберпреступности.

Киберпреступность уже стала очень прибыльным видом бизнеса, который не связан с высоким риском. В конце концов, доходы от киберпреступности могут превышать миллионы долларов. Вот почему сегодня

киберпреступность является проблемой номер один в мире. Ее решению уделяется большое внимание, используются программы сотрудничества между специальными органами многих стран [10, с. 103]. В связи с этим необходимо внедрять активные способы защиты от киберпреступности и борьбы с ней. По мнению экспертов, одним из факторов, влияющих на уровень информационной безопасности, являются облачные решения: 54% респондентов заявили, что планируют перейти на облачные технологии в течение двух лет [4, с. 48].

Киберпреступники используют множество методов - кражу личных данных с целью получения прибыли и шантажа, утечку данных, распределенный отказ в обслуживании и атаки вредоносных программ на медицинские устройства и интеллектуальные транспортные средства [12, с. 7] [7, с. 71] [9, с. 94].

Кибератаки могут оказать значительное социально-экономическое воздействие как на глобальные компании, так и на отдельных лиц. Поэтому киберпреступники должны быть идентифицированы немедленно, а высококачественные доказательства атак должны быть доступны в зале суда [8, с. 11248]. В то же время киберпреступников очень трудно идентифицировать, что постоянно создает дополнительные риски для бизнеса, является серьезной проблемой, которую правительства многих стран не могут решить [3, с. 26].

Криминалистическая особенность киберпреступлений заключается в том, что их расследование и выявление невозможно без использования компьютерных технологий. Существует потребность в точном, быстром реагировании и поиске, записи, изъятии и сборе доказательств в электронной форме, а также в оперативных и следственных мерах [10, с. 50]. Для предотвращения киберпреступности и борьбы с ней необходимо систематически готовить квалифицированных специалистов, способных защищать интересы государства.

В связи с постоянным ростом киберпреступлений и цифровых преступлений цифровое криминалистическое расследование уже стало

профессией и научной сферой деятельности [1, с. 155]. Хотя область цифровой криминалистики в настоящее время хорошо зарекомендовала себя, ее исследовательское сообщество можно считать относительно новым по сравнению со смежными областями традиционной криминалистики и компьютерных наук [2, с. 244]. Цифровое судебно-медицинское расследование включает в себя множество процессов цифрового расследования, включая идентификацию, хранение, анализ, документирование и представление цифровых доказательств. Эти процессы должны осуществляться надежно и законно, чтобы выдержать проверку в судах. Во всем мире многие учреждения полагаются на цифровые носители информации [5, с. 10]. В настоящее время информация обрабатывается, хранится и обменивается с использованием этих носителей. Поскольку использование цифровых носителей для хранения данных быстро расширяется, наблюдается соответствующий рост компьютерных преступлений и кибермошенничества [6, с. 220]. Этот рост усугубил проблемы, стоящие перед правоохранительными органами и силами безопасности по всему миру. Факторами, влияющими на рост угроз в киберпространстве, являются: активное установление и наращивание возможностей для кибервлияния ведущими государствами; развитие организационных структур этих государств, увеличение количества подразделений и их состава, задействованных в системе кибербезопасности мира.

В то же время негосударственные ресурсы активно вовлекаются в деятельность по обеспечению кибербезопасности; активная разработка кибероружия и осуществление с его использованием определенных действий в киберпространстве; возрастающие возможности для скрытного осуществления кибератак и кибероперациий противоборствующими сторонами; усиление влияния государств на национальные информационные пространства других государств, сетевой трафик посредством доступа к глобальным информационным сетям; активное развитие информационных технологий в

глобальном масштабе, в том числе в интересах киберзащиты, кибервлияния, проведения кибероперациий в целом .

Внутренними факторами, которые ограничивают способность государства противостоять негативному воздействию в киберпространстве, являются:

- неразвитость, моральное и физическое устаревание, уязвимость к незаконному воздействию существующей информационной инфраструктуры, информационных и телекоммуникационных сетей и систем;
- активное внедрение и использование в государстве информационных технологий (систем, продуктов) иностранного происхождения, которые не гарантируют надлежащего уровня безопасности использования и трудно поддаются контролю;
- сложность разграничения военной и гражданской критической инфраструктуры государства в киберпространстве;
- возможность негосударственных субъектов и отдельных пользователей осуществлять незаконное кибервлияние в киберпространстве и сложность их обнаружения;
- нарушение процедуры обмена информацией с ограниченным доступом в области обороны, установленной национальным законодательством;
- недостаточное нормативно-правовое регулирование деятельности субъектов кибербезопасности государства;
- недостаточность ввиду растущего объема задач как количественного, так и качественного состава сил (подразделений) субъектов кибербезопасности государства, так и квалифицированных специалистов для укомплектования штатов.

Все вышесказанное требует формирования и внедрения в государстве единого комплексного подхода к дальнейшему развитию и функционированию национальной системы кибербезопасности, который должен определять

(конкретизировать) ее цель, принципы, направления, основные задачи, процедуры создания и функционирования необходимых организационных структур, подготовки кадров и управления вооруженным противостоянием в киберпространстве, другие вопросы кибербезопасности государства.

Существует четыре основных типа киберпреступности:

преступления против конфиденциальности, целостности и доступности компьютерных данных и систем - незаконный доступ, незаконный перехват, вмешательство в данные, системное вмешательство, злоупотребление устройством;

преступления, связанные с компьютерами - контрафакция, мошенничество, связанное с компьютерами;

правонарушения, связанные с контентом - правонарушения, связанные с детской порнографией;

правонарушения, связанные с нарушением авторских и смежных прав.

С развитием Интернета киберпреступность набирает обороты. Киберпреступность обошлась мировой экономике более чем в 1 триллион долларов в 2020 году - чуть более 1% мирового ВВП. По сравнению с 2018 годом этот показатель увеличился более чем на 50%. Киберпреступность приобрела особый размах во время карантина, когда работа, покупки и встречи выходили в Интернет.

Результаты исследования безопасности ИТ-облака Microsoft, проведенного аналитической компанией IDC в Центральной и Восточной Европе, свидетельствуют о том, что в связи с вынужденным переходом большинства компаний на удаленную работу значительно увеличилось количество уязвимостей и формирование новых рисков.

По данным FintechNews, пандемия вызвала всплеск кибератак в августе 2020 года. В частности, количество атак на банки увеличилось на 238%, а 80% компаний в мире столкнулись с ростом активности преступников. По мнению исследователей, международные кибератаки и объемы данных растут

беспрецедентными темпами, что создает трудности для экспертов по безопасности и правоохранительных органов, расследующих киберпреступности.

Для анализа необходимо видеть всю картину преступности в Интернете. Ниже мы приводим данные о киберпреступности, обновленные данными за 2021 год, - от ежегодных нарушений и плотности до последствий киберпреступности, затрат и наиболее часто преследуемых лиц по возрастным группам.

Рисунок 1. Глобальная тепловая карта утечки данных

Рассматривая общее количество взломов в 2022 году, мы видим, что в 87,3% проанализированных нами стран плотность взломов ниже, чем в среднем по миру (50 утечек учетных записей электронной почты на 1000 пользователей Интернета). Это показывает, что хакеры нацелены на одни страны больше, чем на другие.

Особенно выделяется одна страна — Россия, где утечек учетных записей электронной почты почти в 17 раз больше, чем в среднем по миру. Чтобы представить это в перспективе, 8 из 10 российских интернет-пользователей

были взломаны в 2022 году. На втором месте Франция, где взломаны 3 из 10 пользователей.

В целом, мы видим, что хакеры гораздо реже нападают на развивающиеся страны:

На континентальном уровне самые низкие показатели взломанных учетных записей электронной почты в Африке и Азии (23 взломанных аккаунта на 1000 пользователей Интернета).

В Европе самый высокий уровень взломов: в 2022 году взломали каждого пятого европейского интернет-пользователя. Это число более чем в 4 раза превышает среднемировой показатель. Океания занимает второе место с 1 из 8 взломанных пользователей Интернета.

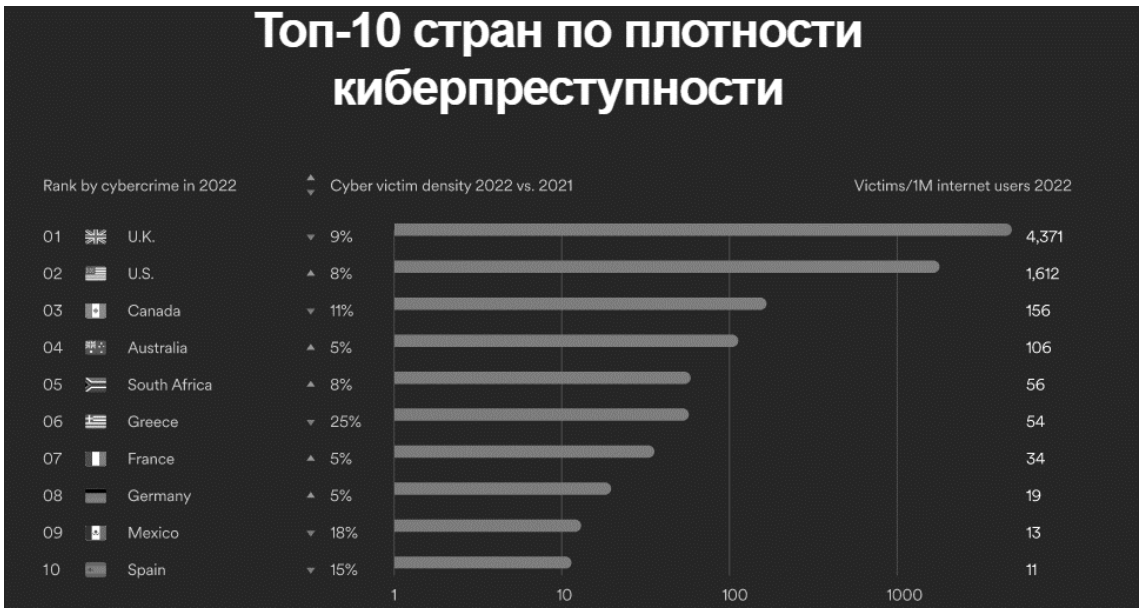

Рисунок 2. Топ-10 стран по плотности киберпреступности

На этом графике показаны десять стран, которые сообщили о самой высокой плотности киберпреступности (число жертв киберпреступлений на 1 млн пользователей Интернета). В рейтинг были включены только страны, данные по которым были в обоих отчетах ФБР (2022 и 2021).

Третий год подряд в этом десятилетии Великобритания возглавляет список по плотности киберпреступности с 4371 жертвой на 1 млн пользователей Интернета (хотя и с падением на 8,6% по сравнению с 2021 годом). Фактически, топ-4 те же, что и годом ранее, остальные составляют

США, Канада и Австралия. Хотя ни в одной из десяти стран не наблюдалось значительного увеличения числа жертв киберпреступлений, в США зафиксирован самый высокий показатель - около 8%. В отличие от этого, в четырех странах наблюдалось снижение более чем на 10%, при этом в Греции наиболее значительное снижение составило около 25%.

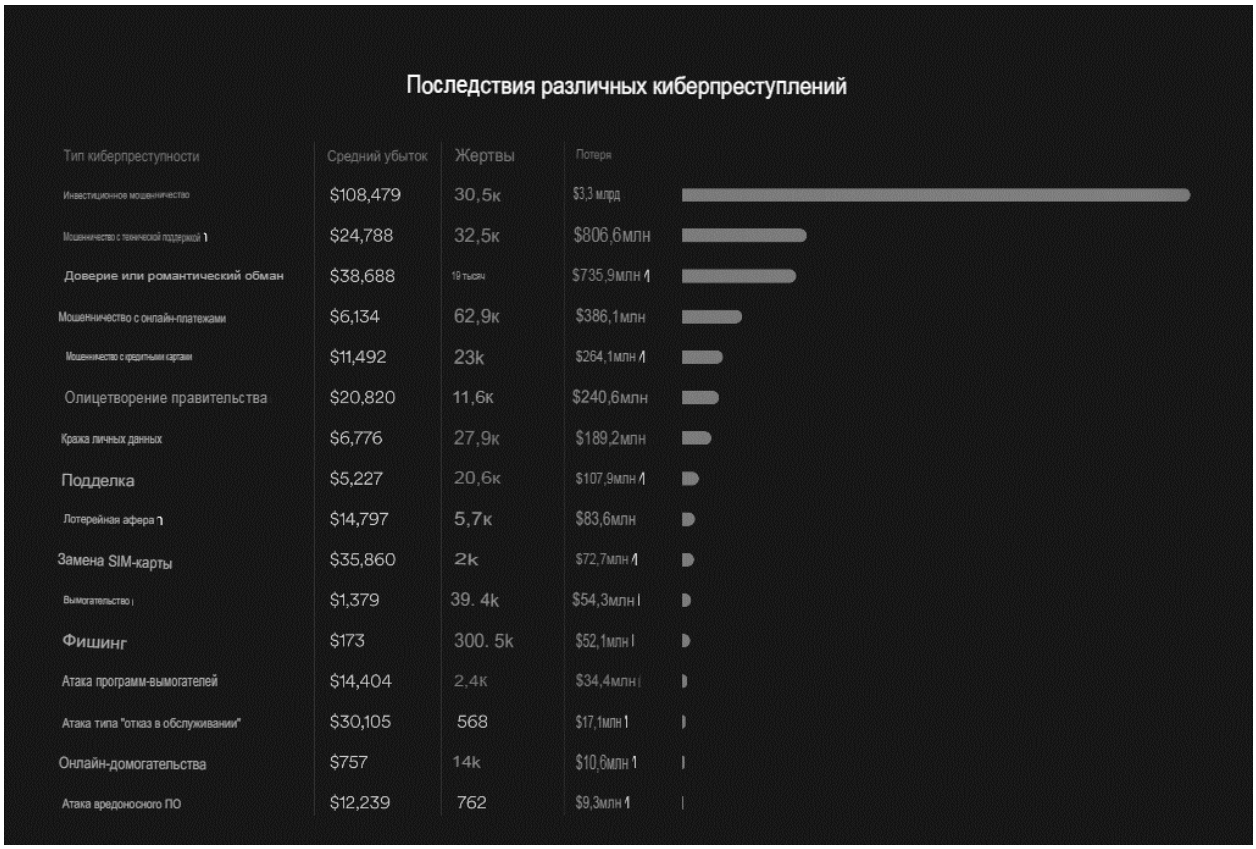

Рисунок 3. Последствия различных киберпреступлений

Существует большое несоответствие в типах киберпреступлений, которые обычно затрагивают людей. Например, фишинг третий год подряд в этом десятилетии продолжает оставаться наиболее распространенным киберпреступлением. В 2022 году насчитывалось в общей сложности 300 497 жертв фишинга. Или, другими словами, каждый второй человек, попавшийся на онлайн-преступление, стал жертвой фишинговой атаки.

Однако за каждое киберпреступление приходится платить разную цену. Жертвы фишинга в среднем теряли наименьшую сумму денег (173 доллара на жертву), в то время как люди, ставшие жертвами инвестиционного мошенничества , потеряли больше всего (108 479 долларов на жертву).

Другим хорошим примером является подмена SIM-карт, которая впервые появилась в отчете о преступлениях в Интернете. 2026 жертв сообщили, что в 2022 году они подверглись нападениям, что привело к финансовым потерям в общей сложности на 72,7 миллиона долларов в результате преступления. Получается, что в среднем потери на одну жертву составляют 35 860 долларов — один из самых высоких показателей в списке.

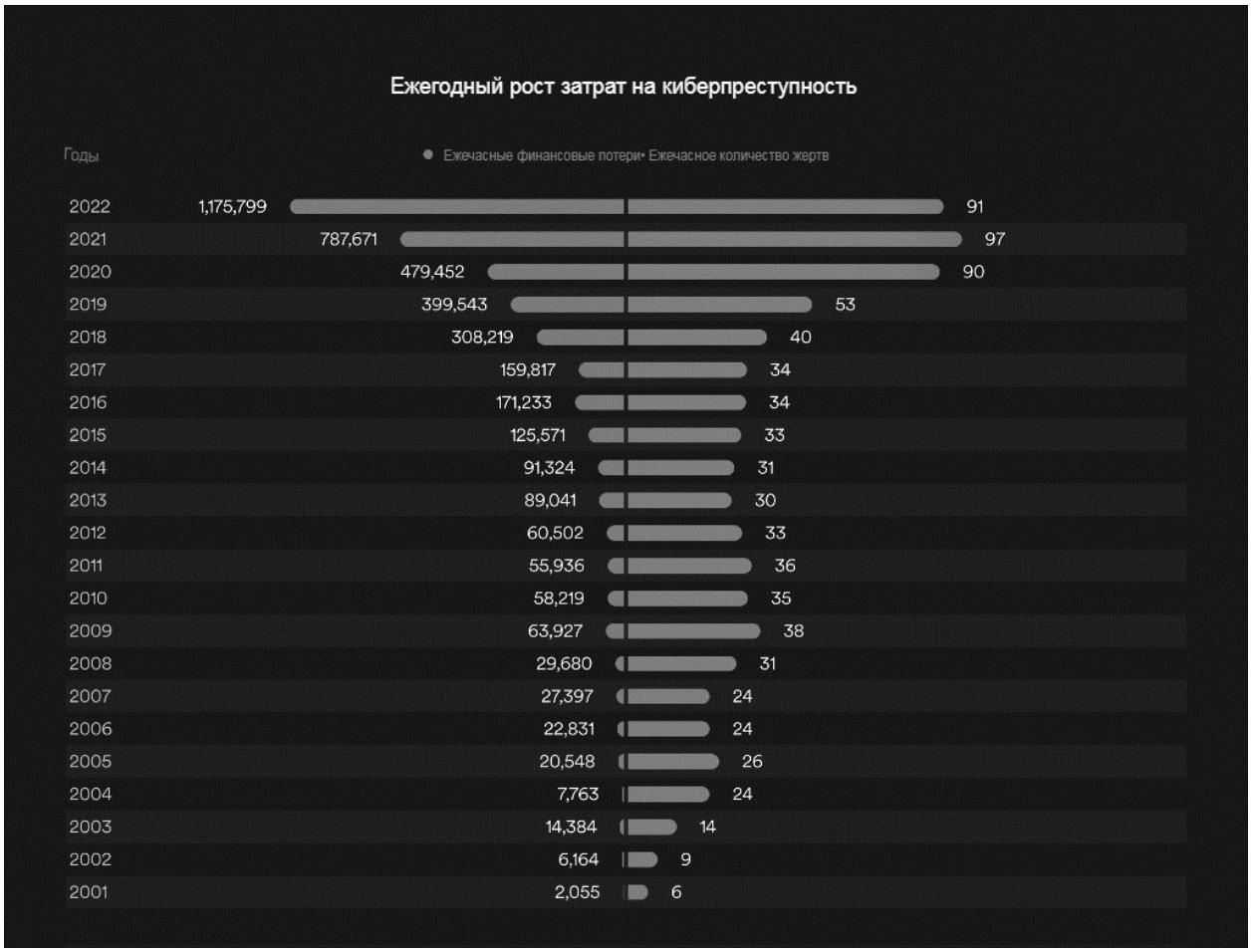

Рисунок 4. Ежегодный рост затрат на киберпреступность

Киберпреступность постоянно растет. С 2001 года число жертв онлайн-преступлений увеличилось в 16 раз (с 6 до 91 жертвы в час), а финансовые потери выросли более чем в 570 раз (с 2000 до почти 1,2 миллиона долларов потерь в час). В общей сложности жертвами киберпреступности стали по меньшей мере 7 303 267 человек и убытки в размере 36,4 миллиарда долларов за 22-летний период.

Мы также видим, что показатели киберпреступности идут рука об руку с глобальными событиями:

2009 год, год после Великой рецессии, привел к увеличению финансовых потерь в результате киберпреступлений на 115% (с 260 миллионов долларов в 2008 году до 560 миллионов долларов в 2009 году).

В 2020 году, в первый год пандемии COVID-19, число жертв киберпреступлений выросло на 69% по сравнению с 2019 годом (с 467 тыс. до 792 тыс. жертв киберпреступлений в год). Это был самый высокий рост числа жертв киберпреступлений, зафиксированный с 2001 года.

На фоне резкого роста цен и достижения пика инфляции в большинстве стран мира в 2022 году финансовые потери от киберпреступности в этом году также достигли рекордного уровня в 10,3 миллиарда долларов - почти 50%—ный рост по сравнению с 6,9 миллиарда долларов в 2021 году. Увеличение ежегодных убытков на 3,4 миллиарда долларов было самым высоким за это столетие.

Таким образом, основными проблемами в борьбе с киберпреступностью являются следующие:

- изменения в парадигмах современных юридических наук, что требует разработки предложений по,,внедрению лучших,,практик нормативно-правовой базы передовых стран мира, взаимодействия международных, интеграционных и национальных правовых систем для обеспечения противодействия киберпреступности;
- необходимость усиления правоохранительной деятельности, которая обновляет применение, по мере необходимости, существующих положений внутреннего законодательства и международного права в отношении преступлений, совершаемых в Интернете;
- вопросы постоянного совершенствования внутреннего законодательства - с целью криминализации актов киберпреступности и предоставления правоохранительным органам процессуальных полномочий для

расследования предполагаемых преступлений в соответствии с надлежащими процессуальными гарантиями, принципами неприкосновенности частной жизни, гражданских свобод и прав человека;

- запрос на разработку внутреннего процессуального законодательства - в соответствии с развитием технологий, обеспечение правоохранительных органов соответствующим оборудованием для борьбы с киберпреступностью;
- необходимость разработки механизмов государственно-частного партнерства в борьбе с киберпреступностью, в том числе посредством законодательства и каналов диалога, для содействия сотрудничеству между правоохранительными органами, поставщиками услуг связи и научными кругами в целях углубления знаний и повышения эффективности мер по борьбе с киберпреступностью;
- необходимость наращивания потенциала (технического, интеллектуального, кадрового, коммуникационного и т.д.) в целях повышения эффективности расследований, улучшения понимания киберпреступности и имеющихся технических средств и технологий для борьбы с ней;
- соответствие требованиям времени для создания условий для прокуроров, судей и центральных национальных властей для надлежащего судебного преследования и вынесения судебных решений по делам, связанным с такими преступлениями.

Таким образом, следует обратить внимание на отсутствие правового механизма регулирования кибербезопасности, записи и использования цифровых доказательств и нормативной базы для международного сотрудничества, поскольку некоторые страны могут не признавать действия киберпреступлениями и запрещать расследования на своей территории.

Эта ситуация значительно увеличивает потребность Европейского союза в укреплении сотрудничества с международными партнерами.

Международное сотрудничество, кибердиалоги в большей степени сосредоточены на обмене информацией об институциональной структуре и полномочиях органов власти в киберпространстве, о последних достижениях в разработке соответствующей политики и законодательных инициатив, включая обновление Директивы ЕС о сетях и информационных системах (ISD), и партнерами в разработке политики и законодательства в области кибербезопасности в соответствии с правовой и институциональной базой ЕС. Особое внимание уделяется координации и сотрудничеству в рамках международных организаций для усиления киберустойчивости и обеспечения ответственного поведения государств в киберпространстве.

Правовую основу кибербезопасности составляют Конституция Российской Федерации, выше названная Доктрина информационной безопасности, международные нормативные правовые документы, федеральные конституционные законы, федеральные законы, нормативные правовые акты Президента и Правительства Российской Федерации, федеральных министерств и ведомств, государственных органов местного самоуправления.

Однако в силу особенностей, законодательство в нашей стране с осторожностью относится к вводу в явные категории угроз цифрового пространства. Поэтому мы можем обратиться к опыту других стран.

ЕС сосредоточил свои усилия на вышеуказанных видах киберпреступности, а Конвенция Совета Европы о киберпреступности привела к появлению следующих актов:

Директива о борьбе с сексуальной эксплуатацией детей в Интернете и детской порнографией – 2011;

Директива об атаках на информационные системы – 2013;

нормативные предложения и директивы, способствующие трансграничному доступу к электронным доказательствам для уголовных расследований – 2018;

Директива о безналичном мошенничестве – 2019;

Предложение о временном регулировании обработки личных и других данных в целях борьбы с сексуальным насилием в отношении детей – 2020;

Европол также создал и действует в качестве ключевого органа в борьбе с киберпреступностью в ЕС - Европейского центра по борьбе с киберпреступностью. Его цель - объединить европейский опыт борьбы с киберпреступностью для поддержки расследований киберпреступлений в государствах-членах.

Первая Стратегия кибербезопасности ЕС, принятая в 2013 году, определила стратегические цели и конкретные действия по достижению киберустойчивости, сокращению киберпреступности, развитию возможностей киберзащиты, развитию технологических ресурсов и установлению согласованной международной политики в области киберпространства для ЕС.

Одной из основ нормативной базы ЕС была Директива 2016/1148 о безопасности сетей и информационных систем, принятая в 2016 году.

В том же году была представлена Глобальная стратегия ЕС по внешней политике и политике безопасности. В разделе "Кибербезопасность" говорится, что стратегической целью ЕС остается укрепление институционального потенциала институтов ЕС и государств-членов для борьбы с киберугрозами, сохраняя при этом открытое, свободное и безопасное киберпространство.

Европейская комиссия также приняла Пакет мер по кибербезопасности, который направлен на достижение следующих целей: принять меры по обеспечению киберустойчивости, разработать механизмы киберудержания и киберзащиты. Подчеркивается важность установления эффективной уголовной ответственности за киберпреступность, для чего следует развивать международное сотрудничество.

В 2018 году Европейский парламент принял резолюцию "Борьба с киберпреступностью", в которой говорится, что Россия и Китай через правительственные и неправительственные учреждения планируют и

осуществляют кибератаки на критическую инфраструктуру государств-членов ЕС.

В мае 2019 года Совет ЕС принял решение ввести ограничительные меры против отдельных лиц и организаций, которые осуществляют кибератаки. Так родился новый режим санкций, который впервые заработал в 2020 году.

В июле прошлого года Совет ЕС принял решение ввести санкции за кибератаки и другую вредоносную активность в Интернете. Российские граждане были признаны причастными к кибератакам на ресурсы ОЗХО (Гаага, Нидерланды) в апреле 2018 года. Им был запрещен въезд в ЕС, а их активы заморожены.

Главный центр специальных технологий Главного управления Генерального штаба Министерства обороны Российской Федерации признан причастным к осуществлению кибератак NotPetya и EternalPetya.

Ряд стран разработали специальные законы, направленные на борьбу с киберпреступностью. Например, Германия, Япония и Китай внесли поправки в соответствующие положения своих уголовных кодексов для описания киберпреступности и борьбы с ней.

Некоторые страны, вместо того чтобы разделять киберпреступность на отдельные преступные деяния, просто добавили специальные положения в свое национальное законодательство и кодексы, криминализирующие незаконное использование цифровых технологий для совершения любого преступления. Такой подход привел к тому, что преступнику предъявили обвинения в двух преступлениях одновременно.

Этапы криминологического расследования.

В целом, эти процедуры включают следующие три этапа:

Сбор данных. Информация, хранящаяся в электронном виде, должна собираться таким образом, чтобы поддерживать ее целостность. Это часто включает в себя физическую изоляцию тестируемого устройства, чтобы гарантировать, что оно не может быть случайно загрязнено или подделано.

Эксперты создают цифровую копию носителя информации, также называемую криминалистической, и хранят оригинальное устройство в безопасном месте для сохранения его первоначального состояния. Расследование проводится по цифровой копии. В других случаях общедоступная информация может быть использована в криминалистических целях, например, для публикации в Facebook или публичного обвинения Venmo в приобретении незаконных продуктов или услуг, представленных на веб-сайте Vicemo.

Анализ. Следователи анализируют цифровые копии носителей информации в стерильных условиях для сбора информации по делу. Для облегчения этого процесса используются различные инструменты, включая вскрытие жесткого диска с помощью Basis Technology и анализатор сетевых протоколов Wireshark. Покачивание мыши полезно при сканировании вашего компьютера, чтобы он не переходил в спящий режим или не терял данные энергозависимой памяти, которые теряются при переходе компьютера в спящий режим или отключении питания.

Презентация. Судебные следователи представляют свои выводы в ходе судебных разбирательств, где судья или присяжные используют их для определения исхода судебного процесса. В ситуации восстановления данных судебные следователи представляют то, что они смогли восстановить из поврежденной системы.

Компьютерные средства часто используются в компьютерных криминалистических расследованиях для проверки полученных результатов. Следователи используют различные методы и свои собственные криминалистические программы для изучения копии, которую они сделали со сломанного устройства. Они ищут в скрытых папках и нераспределенном дисковом пространстве копии удаленных, зашифрованных или поврежденных файлов. Любые доказательства, обнаруженные на цифровой копии, должны быть тщательно задокументированы в отчете о результатах и проверены оригинальным устройством при подготовке к судебному разбирательству,

которое включает обнаружение, хранение или фактическое судебное разбирательство.

В компьютерных судебных расследованиях используется комбинация методов и экспертных знаний. Некоторые распространенные методы включают следующее:

Обратная стеганография.

Стохастическая криминология.

Перекрестный анализ.

Оперативный анализ.

Восстановление удаленных файлов.

Компьютерная криминалистика стала независимой областью научного опыта. Согласно Salary.com средняя годовая зарплата компьютерного криминалиста-аналитика составляет около 65 000 долларов. Некоторые примеры карьерных путей кибер-криминалистов включают следующее:

Инженер-криминалист. Эти специалисты участвуют на этапе составления компьютерного судебного процесса, сбора данных и подготовки их к анализу. Они помогают определить причину сбоя устройства.

Судебный бухгалтер. Этот пост посвящен преступлениям, связанным с отмыванием денег и другими транзакциями, осуществляемыми для сокрытия незаконной деятельности.

Аналитик по кибербезопасности. Этот пункт относится к анализу данных после их сбора и анализа, которые затем могут быть использованы для улучшения стратегии организации в области кибербезопасности.

В данном исследовании рассматриваются основные аспекты внедрения инструментов для криминалистического исследования компьютерных средств и систем в борьбе с киберпреступностью. Доказано, что расследование уголовных дел по большинству уголовных преступлений имеет цифровую составляющую. Анализ показывает, что в настоящее время способность организаций противостоять киберугрозам низка практически во всех областях.

Существенным препятствием является низкий уровень межведомственного сотрудничества, а внедрению усиленных мер кибербезопасности в большинстве случаев препятствует недостаточная осведомленность сотрудников по этим вопросам.

Предлагается более широко использовать методы компьютерных криминалистических исследований, чтобы не отставать от растущих показателей киберпреступности. Различают следующие виды компьютерных криминалистических экспертиз: криминалистика базы данных; электронная криминалистика; криминалистика вредоносных программ; криминалистика памяти; мобильная криминалистика; сетевая криминалистика. В процессе компьютерных криминалистических расследований используется сочетание специальных методов и знаний.

Следовательно, существует необходимость укрепления международного сотрудничества и в разработке соответствующей политики и законодательных инициатив в области безопасности сетей и информационных систем, совершенствования законодательства в области противодействия киберпреступности.

Литература

1. Adu, K.K. & Adjei, E. (2018). The phenomenon of data loss and cyber security issues in Ghana, Foresight, 20(2), 150-161, https://doi.org/10.1108/FS-08-2017-0043

2. Apau, R. & Koranteng, F.N. (2019). Impact of cybercrime and trust on the use of Ecommerce Technologies : an application of the theory of planned behavior, J. Cyber Criminol. 13, 228-254, https://doi.org/10.5281/zenodo.3697886.

3. Association of Chief Police Officers (ACPO), Good practice guide for computer based electronic evidence (2012). https://www.digital-detective.net/digital-forensicsdocuments/ACPO_Good_Practice_Guide_for_Digital_Evidence_v5.pdf, (Accessed 25.07.2021).

4. Barrett, D. (2020). Cloud based evidence acquisitions in digital forensic education. Inf. Syst. Electron. J., 18 (6), 46-56.

5. Baylon, C. & Antwi-Boasiako A. (2016). Increasing internet connectivity while combatting cybercrime: Ghana as a case study. https://www.cigionline.org/publications/increasing-internet-connectivity-while-combatting-cybercrime-ghana-case-study. (Accessed 6.06.2021).

6. Becker, W.S., Dale, W.M. & Pavur, E.J. Jr. (2010). Forensic science in transition: critical leadership challenges. Forensic Sci. Pol. Manag., 1, 214-223.

7. Berghel, H. (2012). Breaking the Fourth Wall of Electronic Crime: Blame It on the Thespians. Computer, 45(5), 86-88, doi: 10.1109/MC.2012.161.

8. Gaggero, M., Paola D. Di, Petitti, A. & Caviglione, L. (2019). When Time Matters: Predictive Mission Planning in Cyber-Physical Scenarios, IEEE Access, 7, 11246-11257.

9. Gradon, K. (2013). Crime Science and the Internet Battlefield: Securing the Analog World from Digital Crime. IEEE Security & Privacy, 11(5), 93-95, doi: 10.1109/MSP.2013.112.

10. James, J. (2017). How Businesses Can Speed Up International Cybercrime Investigation. IEEE Security & Privacy, 15(2), 102-106, doi: 10.1109/MSP.2017.40.

11. Oppliger, R., Pernul, G. & Katsikas, S. (2017). New Frontiers: Assessing and Managing Security Risks. Computer, 50(4), 48-51, doi: 10.1109/MC.2017.93.

12. Parker, D. (2007). The Dark Side of Computing: SRI International and the Study of Computer Crime. IEEE Annals of the History of Computing, 29(1), 3-15, doi: 10.1109/MAHC.2007.15.