Ученые записки Крымского федерального университета имени В. И. Вернадского
Юридические науки. – 2023. – Т. 9 (75). № 3. – С. 448–456.

УДК 343.851.3

К ВОПРОСУ О ПРОТИВОДЕЙСТВИИ КИБЕРПРЕСТУПНОСТИ В УСЛОВИЯХ НОВОЙ ГЕОПОЛИТИЧЕСКОЙ РЕАЛЬНОСТИ

Запорожец С. А., Крайнова Н. А.

Севастопольский государственный университет

Одним из наиболее опасных видов международной преступности является киберпреступность. Предупреждение, выявление и расследование киберпреступлений крайне затруднено из-за удаленности преступника от места преступления и общественно опасных последствий, отсутствия единого подхода к расследованию данного вида преступлений и разработки процедуры взаимодействия на международном уровне на территориях разных стран. Национальное законодательство Российской Федерации в настоящее время находится в поиске эффективных форм и методов противодействия киберпреступности в целях защиты неприкосновенности частной жизни и конфиденциальной информации. В условиях новой геополитической реальности выявление, расследования и пресечение киберпреступлений становится еще более затруднено в связи с тем, что между некоторыми странами и Российской Федерацией отсутствует взаимопонимание в силу чрезмерной политизированности и ангажированности государственных структур. В настоящей работе на основе исследования действующей нормативно-правовой базы, правоприменительной практики предлагаются пути и способы совершенствования национального законодательства, международно-правовых норм, оптимизации международного сотрудничества в области противодействия киберпреступлениям

Ключевые слова: кибербезопасность, противодействие киберпреступности, защита информации, персональные данные, информация, защита информации.

Проблема противодействия киберпреступности за последнее время приобрела особую актуальность в виду экспоненциально увеличивающегося числа регистрируемых преступлений, совершаемых в информационно-коммуникационной среде, а также с использованием компьютерного оборудования. Быстрое развитие информационных технологий, использование различных электронных устройств, доступ в Интернет сделали уязвимыми не только собственность, но и личные данные.

Несмотря на то, что в 2022 г. темпы прироста киберпреступлений значительно снизились по сравнению с фиксируемыми в последнее пятилетие, тем не менее, эта динамика все еще положительна. Кроме того, отмечается ухудшение структуры киберпреступности. Если годом ранее основную массу совершенных с использованием информационно-коммуникационных сетей преступлений составляли дистанционные кражи и мошенничества, то в 2022 г. официальная статистика свидетельствует об увеличении числа заведомо ложных сообщений об акте терроризма и сбыта наркотиков. Согласно статистическим данным МВД РФ за 2022 г. правоохранительными органами зарегистрировано больше на 20,9% фактов сбыта наркотиков, 92,2 % заведомо ложных сообщений об акте терроризма, количество которых также увеличилось, были совершены дистанционно [1].

Выступая на заседании расширенной коллегии МВД РФ, Президент РФ, Владимир Путин, отметил, что борьба с преступностью с использованием информационных технологий является одним из приоритетов работы правоохранителей. Президент указал, что необходимо не только активно противодействовать уже совершенным преступлениям, но и действовать на опережение, предупреждать новые риски, чтобы преступники не паразитировали на технологическом прогрессе [2]. Важно

подчеркнуть, что необходимость профилактики киберпреступлений обусловлена не только тем колоссальным экономическим ущербом, который зачастую является результатом таких преступлений, но и значимым имиджевым уроном для всех участников информационного обмена, огромным риском для личной безопасности каждого человека, интересов национальной безопасности общества и государства в целом. Как справедливо отмечают Е.М. Якимова, С.В. Нарутто, «киберпреступность может нарушать интересы, как государства, так и отдельного человека» [3, с. 371].

Следует отметить, что в настоящее время, несмотря на достаточную сложность анализируемой проблемы, ее связанность с техническими знаниями, специалистами предпринимается немало усилий, направленных на ее изучение и поиск оптимальных способов противодействия киберпреступности. Предупреждение преступлений, совершаемых в информационно-коммуникационной среде, становилось предметом внимания таких ученых как Е.А. Антонян, И.Б. Горелик, Е.Н. Клещина, В.Б. Клишков, Е.В. Стебенева, М.А. Яковлева и других. В 2005 г. в Дальневосточном государственном университете на кафедре уголовного права была успешно защищена диссертация Т.Л. Тропиной на тему «Киберпреступность: понятие, состояние, уголовно-правовые меры борьбы» [4]. Однако, несмотря на проработанность проблемы в силу динамично меняющихся условий внешней среды в настоящий момент исследования проблем противодействия киберпреступности представляются все также актуальными.

За последнее время в Российской Федерации было организовано и проведено множество мероприятий, посвященных обсуждению проблем противодействия киберпреступлениям, поиску оптимальных решений. Наиболее значимыми площадками для диалога стали Международные конгрессы по кибербезопасности. На страницах научной печати отмечается значимость дискуссий в подобном формате и определены ключевые выводы Международных конгрессов по кибербезопасности. К их числу отнесены «необходимость организации эффективного международного и межотраслевого сотрудничества государственных органов, правоохранительных структур и частного бизнеса, наращивание кадрового потенциала в области кибербезопасности высококлассными специалистами, необходимость обмена информацией об угрозах, модернизация системы и внедрение новых методов защиты» [5, с. 15]. Следует отметить, что это, в целом, достаточно традиционные положения, которые могут быть применимы при формировании стратегий противодействия любому виду преступности. Однако противодействие киберпреступности имеет свои особенности, что отмечалось в ходе обсуждения на различных дискуссионных площадках конгрессов по кибербезопасности.

Способы противодействия киберпреступности зависят от вида предотвращаемого преступления: хакерство, «скручивание», фрикинг, диффамация, рассылка спама, «фишинг», киберхулиганство, кибер-терроризм и другие. Безопасность в Интернете может быть достигнута только с помощью профилактических мер, применяемых на различных уровнях (социальном, специальном и индивидуальном). В силу специфики методов борьбы с киберпреступностью важную роль в этом процессе играет сотрудничество правоохранительных органов, как на национальном, так и на международном уровнях. Именно особая важность международного сотрудничества в противодействии киберпреступлениям выходит на первый план, однако, именно

этот аспект противопреступной деятельности в сфере кибербезопасности в настоящее время максимально осложнен.

Следует отметить, что международный аспект сотрудничества в области противодействия киберпреступлениям всегда был связан со значительными затруднениями. Принятая в 2001 г. Конвенция о преступности в сфере компьютерной информации ETS № 185 (Будапешт, 23 ноября 2001 г.) [6] так и не стала документом, упростившим сотрудничество в данной сфере. Следует отметить, что РФ не стала участником данного международного документа в виду очевидных его недостатков. К концу 2005 г. Конвенцию подписали 38 европейских стран, США, Канада, Япония и ЮАР. Камнем преткновения для участия в соглашении Российской Федерации стал п. b ст. 32, согласно которому «сторона может без согласия другой стороны получать через компьютерную систему на своей территории доступ к хранящимся на территории другой стороны компьютерным данным или получить их, если эта сторона имеет законное и добровольное согласие лица, которое имеет законные полномочия раскрывать эти данные этой стороне через такую компьютерную систему».

Взамен Конвенции о преступности в сфере компьютерной информации 2001 г. Россия в 2021 г. внесла в ООН проект Конвенции о борьбе с киберпреступностью. В проекте документа Российская Федерация предложила свой вариант взаимодействия в вопросах об оказании правовой помощи по делам о киберпреступлениях, о выдаче преступников. Проектом предлагается классификация киберпреступлений, которая охватывает 23 вида наиболее распространенных деяний [7]. Однако данный документ не был одобрен для подписания Организацией Объединенных Наций. Вопросы международного сотрудничества в настоящее время регламентируются по большей части международными документами двустороннего характера.

Нормы, касающиеся противодействия киберпреступлениям, определены в Дополнительном протоколе к Конвенции о преступлениях в сфере компьютерной информации относительно введения уголовной ответственности за правонарушения, связанные с проявлением расизма и ксенофобии, совершенные посредством компьютерных систем (ETS № 189) от 28.01.2003 [8], Директивой Европейского Парламента и Совета Европейского Союза 2002/58/ЕС в отношении обработки персональных данных и защите конфиденциальности в секторе электронных средств связи, принятые с поправками от 25.11.2009 [9], Директивой Европейского Парламента и Совета Европейского Союза 2013/40/ЕС об атаках на информационные системы и замене Рамочного Решения 2005/222/PVD Совета ЕС от 12.08.2013 [10]; Рамочным решением Совета Европы от 28.05.2001 о борьбе с мошенничеством и подделкой безналичных платежных средств и других, Регламент Европейского парламента и ЕС 2016/679 «Защита персональных данных» [11].

Условия новой геополитической реальности диктуют необходимость расширения международного сотрудничества в сторону Азиатско-Тихоокеанского региона (АТР). Следует отметить, что Россия имеет давние устойчивые дружественные связи с государствами на пространстве АТР, предпринимает усилия, направленные на достижение баланса, установления справедливых отношений, основанных на равенстве, взаимном уважении экономических, политических и духовных интересов. Достигнутые договоренности в формате СНГ, претворяются в жизнь в форме модельного законотворчества. Что касается противодействия киберпреступлениям, защите информации и персональных данных, гарантии безопасности последних закреплены

в Модельном законе «О персональных данных», который был принят на 48-м пленарном заседании Межпарламентской Ассамблеи государств – участников СНГ [12], а также в Соглашении о сотрудничестве государств – участников СНГ по борьбе с преступлениями в сфере компьютерной информации (Минск, 01.06.2001) [13]. Приняты и другие документы.

Несмотря на достаточно объемную нормативно-правовую базу, тем или иным образом регламентирующую вопросы противодействия киберпреступлениям, на пространстве СНГ до сих пор не принят основополагающий модельный закон «О борьбе с киберпреступлениями», проект которого был разработан в рамках проведенного конкурса и предложен для принятия МПА СНГ. На страницах научной литературы высказывается обоснованная критика в отношении термина «борьба с преступностью» и выдвигается предложение использовать в криминологическом законодательстве более емкого выражения «противодействие преступности». Следовательно, логичным было бы принятие модельного закона «О противодействии киберпреступности» [14, с. 53], а также в ближайшем будущем следует гармонизировать национальное законодательство стран СНГ, предусматривающее правовые нормы о защите персональных данных, ответственности за совершение киберпреступлений.

Важным вопросом профилактики киберпреступлений является проблема защиты информации, прежде всего, защиты персональных данных. В Российской Федерации защита конфиденциальности данных о физических и юридических лицах, а также безопасность операций с денежными средствами гарантированы на законодательном уровне ФЗ «О персональных данных» от 27.07.2006 № 152-ФЗ [15], «О банках и банковской деятельности» от 02.12.1990 г. № 351-1 [16], «О Центральном банке Российской Федерации (Банке России)» от 10.07.2002 № 86-ФЗ [17], «О Национальной платежной системе» от 27.06.2011 г. № 161-ФЗ [18], «Об информации, информационных технологиях и защите информации» от 27.07.2006 № 149-ФЗ [19], «О коммерческой тайне» от 29.07.2004 № 98-ФЗ [20], «Об электронной подписи» от 006.04.2011 г. № 63-ФЗ [21], «О безопасности критической информационной инфраструктуры Российской Федерации» от 26.07.2017 № 187-ФЗ [22]. КоАП РФ от 30.12.2001, УК РФ от 13.06.1996 г. и предусмотрена ответственность за правонарушения в сфере защиты информации. Данные нормативно-правовые акты регламентируют различные вопросы защиты информации, безопасности способов передачи информации, ответственности за совершение киберпреступлений. Однако в России отсутствует специальный нормативно-правовой акт на уровне федерального закона, который бы регламентировал вопросы предупреждения киберпреступлений или, что видится предпочтительным, противодействия киберпреступности.

Способы противодействия киберпреступности весьма специфичны и определяются в зависимости от способа действия. Это может быть уничтожение, блокирование, копирование, модификация и использование информации посредством непосредственного или опосредованного доступа к информации и компьютерным системам. Предупредительные меры могут различаться в зависимости от способов использования и получения информации, полученной с помощью компьютерных систем, а также мотивов преступления (корыстный импульс), распространения вредоносного программного обеспечения, получения и использования бесплатного

программного обеспечения, способов кражи денег, мести, коммерческого шпионажа, содействия террористической деятельности и других.

Сложность предупреждения, выявления и расследования киберпреступлений определяется следующим: 1) место преступления и место наступления общественно опасных последствий находятся далеко друг от друга и могут находиться на территории разных стран; 2) высокая скорость обмена криминологической информацией, значимой для уголовного дела, когда правоохранительный орган находится далеко. Сложность противодействия зависит от личности преступника, совершившего киберпреступление, виктимологических особенностей личности, активных розыскных мероприятий, проводимых с целью раскрытия преступления, а также возможной легализации результатов этих мероприятий.

Согласно информационному письму Банка России от 14.08.2018 № ИН014-12/54 «О национальной оценке рисков отмывания доходов и финансирования терроризма», «длительное рассмотрение запросов о правовой помощи и сложности получения этой помощи, а также информация о конечных бенефициарах от властей определенных стран» является серьезной уязвимостью для противодействия отмыванию доходов, полученных преступным путем. легализация незаконных доходов и финансовых рисков [23].

В правовом аспекте необходимо выработать единую концепцию сотрудничества по выявлению, судебному преследованию и разрешению киберпреступлений, определению единой формы запроса и возможному предоставлению информации, имеющей значение для уголовного дела; разработке безопасных средств защиты личных данных и проведению совместных научных исследований положительных результатов опыта борьбы с киберпреступностью. В настоящее время в условиях общемировой нестабильности более вероятным представляется достижение соглашений, касающихся единой концепции сотрудничества в сфере выявления, судебного преследования и противодействия преступности в целом в формате двусторонних соглашений, а также правовой работы в рамках сложившихся союзов стран.

С точки зрения организации крайне важно проводить разъяснительную беседу с людьми, приобретающими цифровые и микропроцессорные устройства, повысить правовую культуру населения, разработать стандарты набора, проверки и инструктажа персонала, имеющего доступ к ресурсам, содержащим личные данные, проводить плановые и внеплановые проверки соблюдения процедур информационной безопасности лицами, работающими с компьютерными системами. Проверка соблюдения законодательства, касающегося защиты, передачи и сбора личных данных также представляется обязательной.

К числу существенных нарушений, позволяющих совершать киберпреступления, как представляется, можно отнести: 1) неконтролируемый доступ сотрудников к компьютерной информации; 2) использование сотрудниками собственных флэш-накопителей; 3) отсутствие контроля над компьютерами, содержащими личные данные; 4) риск представляют организации, использующие компьютеры без защиты и подходящего антивирусного программного обеспечения; 5) несовершенство системы паролей защиты от несанкционированного доступа к рабочей станции и ее программному обеспечению, не обеспечивающему идентификацию пользователя; 6) использование баз сохраненных паролей на работе; 7) отсутствие обязательной проверки порядка секретности; 8) отсутствие договоров или расписок о неразглашении

информации, которую работники обнаружили при работе с компьютером или личными данными, коммерческой тайной или другой конфиденциальной информацией; 9) все сотрудники, имеющие доступ к личным данным, информации, содержащей деловую тайну или коммерческую конфиденциальность, или другой конфиденциальной информации, должны пройти инструктаж, в ходе которого будет разъяснена их ответственность за несоблюдение порядка работы с такого рода информацией.

Криминалистическими мерами противодействия киберпреступности являются следующие: 1) использование в расследовании новейших достижений науки; 2) совершенствование теории доказательств, позволяющей признавать достоверными не только вещественные доказательства и документированную информацию, но и виртуальную и электронную информацию; 3) разработка унифицированных баз данных, позволяющих идентифицировать лиц, совершающих киберпреступления. Основная претензия к виртуальной и электронной информации состоит в невозможности обеспечить ее достоверность. В этой связи некоторыми специалистами предлагается обратиться к опыту Китая, где, например, «регистрация в социальных сетях проводится только с подтверждением личности регистрируемого лица другими пользователями. В случае удаления страницы администрация сети всегда может связаться с человеком, который подтвердил регистрацию, и через него установить личность преступника» [24].

Российская судебная практика идет по пути признания виртуальной и электронной информации в качестве источника доказательств. Так, в апреле 2019 г. Верховный Суд РФ указал, что «при решении вопроса о наличии нарушения суд вправе принять любые средства доказывания, предусмотренные процессуальным законодательством, в том числе полученные в интернете. Допустимыми доказательствами являются, в том числе сделанные и заверенные лицами, участвующими в деле, распечатки материалов, размещенных в информационно-телекоммуникационной сети (скриншот), с указанием адреса интернет-страницы, с которой сделана распечатка, а также точного времени ее получения. Такие распечатки подлежат оценке судом при рассмотрении дела наравне с прочими доказательствами» [25].

Единая практика расследования и использования достижений науки в процессе пресечения, раскрытия и расследования преступлений позволит установить личность лица, совершившего преступление, и осудить его за совершение уголовного правонарушения, что в свою очередь, позволит соблюсти реализацию принципа неотвратимости наказания. Неотвратимость наказания обеспечит как снижение числа преступлений, так и защиту одной из высших ценностей государств, которой являются права и законные интересы личности. На основе вышеизложенного можно выделить 3 основных направления противодействия киберпреступлениям: криминологическое (предупреждение киберпреступлений), криминалистическое (своевременное выявление и расследование преступлений), уголовно-правовое (неотвратимость ответственности и наказания виновных).

Установленная многочисленными научными изысканиями неэффективность противодействия киберпреступлениям в отсутствии международного сотрудничества, представляется очевидной. Однако в условиях реальной действительности следует обратить внимание на внутреннее законодательство и правоприменительную деятельность, начинать выстраивать многоуровневую институциональную систему кибербезопасности внутри государства.

Система кибербезопасности должна включать в себя различные компоненты, включая повышение уровня цифровой грамотности населения, помощь в продвижении индивидуальных способов защиты личной информации, а также механизмы противодействия и предотвращения киберугроз. Как представляется, единая система противодействия киберпреступлениям должна быть основана на следующих подходах: разработка стратегии кибербезопасности не только на национальном, но и на международном уровне; гармонизация соответствующих положений законодательства государств, сотрудничающих в борьбе с киберпреступностью; заключение межгосударственных соглашений, предусматривающих меры по борьбе с киберпреступностью; активизация международного сотрудничества, усиление взаимодействия национальных разведывательных служб и координации их действий; своевременное совершенствование российского законодательства с учетом новых технических угроз; формирование современной материально-технической и кадровой базы для борьбы с киберпреступностью; повышение технической и финансовой грамотности населения; координация деятельности всех участников борьбы с киберпреступностью, начиная от правоохранительных органов и заканчивая исследовательскими и академическими институтами.

Таким образом, проведенное исследование позволяет сделать вывод о том, что противодействие киберпреступлениям представляется собой актуальную проблему международного характера. Несмотря на наличие достаточного количества нормативно-правовых актов, регламентирующих вопросы противодействия киберпреступлениям, в настоящее время нельзя говорить об эффективности правоприменительной деятельности. Основной проблемой следует назвать обострившиеся на фоне геополитических конфликтов и противостояний отношения с рядом стран. Выходом из данной ситуации видится межгосударственное взаимодействие на уровне двусторонних соглашений, а также в формате устоявшихся союзом, которым является, например, Содружество независимых государств. Представляется необходимым обратить внимание на национальное законодательство РФ и принять на федеральном уровне закон «О противодействии киберпреступлениям». Кроме того, следует акцентировать внимание на формирование современной материально-технической и кадровой базы для борьбы с киберпреступлениями, вести грамотную информационную политику, работать над правовым просвещением населения, обеспечить неотвратимость ответственности и наказания киберпреступников.

Список литературы:

1. Краткая характеристика состояния преступности в Российской Федерации за январь-декабрь 2022 года. – Текст электронный // МВД РФ : [сайт] – URL: https://мвд.рф/reports/item/35396677/. (дата обращения 01.04.2023 г.).
2. Путин назвал одним из приоритетов МВД борьбу с киберперступностью. Текст электронный // Взгляд. Деловая газета : [сайт] – URL: https://vz.ru/news/2023/3/20/1203922.html.
3. Якимова Е.М., Нарутто С.В. Международное сотрудничество в борьбе с киберпрступностью // Криминологический журнал Байкальского государственного университета экономики и права. – 2016. – Т. 10. - № 2. - С. 369-378.
4. Тропина Т.Л. Киберпреступность: понятие, состояние, уголовно-правовые меры борьбы: специальность 12.00.08 «Уголовное право, уголовно-исполнительное право и криминология» : дис. на соиск. … канд. юрид. наук / Тропина Татьяна Львовна ; Дальневост. гос. ун-т. - Владивосток, 2005. 234 с.
5. Антонян Е.А., Клещина Е.Н. Киберпреступность на современном этапе: тенденции и направления противодействия // Вестник экономической безопасности. - 2022. - № 5. - С. 11-15.
6. Конвенция о преступности в сфере компьютерной информации ETS № 185 (Будапешт, 23 ноября 2001 г. / Гарант: [сайт]. – URL https://base.garant.ru/4089723/. (дата обращения 01.04.2023 г.).

7. Россия внесла в ООН проект конвенции о борьбе с киберпреступностью. Текст электронный // РИА Новости: [сайт] – URL: https://ria.ru/20210727/konventsiya-1743130628.html.
8. Дополнительный протокол к Конвенции о преступлениях в сфере компьютерной информации относительно введения уголовной ответственности за правонарушения, связанные с проявлением расизма и ксенофобии, совершенные посредством компьютерных систем (ETS № 189) от 28.01.2003 ФЗ / Гарант : [сайт]. – URL: https://base.garant.ru/4084840//(дата обращения 01.04.2023 г.).
9. Директива Европейского Парламента и Совета Европейского Союза 2002/58/ЕС в отношении обработки персональных данных и защите конфиденциальности в секторе электронных средств связи, принятые с поправками от 25.11.2009 года / Гарант : [сайт]. – URL: https://base.garant.ru/2570354/.
10. Директива Европейского Парламента и Совета Европейского Союза 2013/40/ЕС об атаках на информационные системы и замене Рамочного Решения 2005/222/PVD Совета ЕС от 12.08.2013 года / Гарант : [сайт]. – URL: https://base.garant.ru/70557982/ (дата обращения 01.04.2023 г.).
11. Право Европейского Союза / Консультант Плюс : [сайт]. – URL: https://www.consultant.ru/cons/cgi/online.cgi?req=doc&base=ARB&n=568366&dst=100276#7ZFdCaTuq4QQQwA81 (дата обращения 01.04.2023 г.).
12. Постановление МПА СНГ от 29.11.2018 г. № 48-9 «О новой редакции модельного закона «О персональных данных». / Контур Норматив: [сайт]. – URL: https://www.consultant.ru/document/cons_doc_LAW_61801/(дата обращения 01.04.2023 г.).
13. Соглашение о сотрудничестве государств - участников СНГ по борьбе с преступлениями в сфере компьютерной информации / Гарант: [сайт]. – URL: https://base.garant.ru/5283054/.
14. Крайнова Н.А. О концепции модельного закона стран-участниц СНГ «О борьбе с киберпреступностью» // Право и цифровая экономика. - 2022. - № 2 (16). - С. 48-56.
15. Федеральный закон «О персональных данных» от 27.07.2006 г. № 152-ФЗ / Консультант Плюс: [сайт]. – URL: https://www.consultant.ru/document/cons_doc_LAW_61801/(дата обращения 01.04.2023 г.).
16. Федеральный закон «О банках и банковской деятельности» от 02.12.1990 г. № 351-1/ Консультант Плюс: [сайт]. – URL: https://www.consultant.ru/document/cons_doc_LAW_5842//.
17. Федеральный закон «О Центральном банке Российской Федерации (Банке России)» от 10.07.2002 г. № 86-ФЗ **/** Консультант Плюс: [сайт]. – URL: https://www.consultant.ru/document/cons_doc_LAW_37570/
18. Федеральный закон «О Национальной платежной системе» от 27.06.2011 г. № 161-ФЗ / Консультант Плюс: [сайт]. – URL: https://www.consultant.ru/document/cons_doc_LAW_115625/ /.
19. Федеральный закон «Об информации, информационных технологиях и защите информации» от 27.07.2006 г. № 149-ФЗ/ Консультант Плюс: [сайт]. – URL: https://www.consultant.ru/document/cons_doc_LAW_61798/ /(дата обращения 01.04.2023 г.).
20. Федеральный закон «О коммерческой тайне» от 29.07.2004 г. № 98-ФЗ / Консультант Плюс: [сайт]. – URL: https://www.consultant.ru/document/cons_doc_LAW_48699/ /(дата обращения 01.04.2023 г.).
21. Федеральный закон «Об электронной подписи» от 006.04.2011 г. № 63-ФЗ / Консультант Плюс: [сайт]. – URL: https://www.consultant.ru/document/cons_doc_LAW_112701/ / /
22. Федеральный закон «О безопасности критической информационной инфраструктуры Российской Федерации» от 26.07.2017 г. № 187-ФЗ / Консультант Плюс: [сайт]. – URL: https://www.consultant.ru/document/cons_doc_LAW_220885/ / /(дата обращения 01.04.2023 г.).
23. Информационное письмо Банка России от 14.08.2018 г. № ИН014-12/54 «О национальной оценке рисков отмывания доходов и финансирования терроризма» ФЗ / Консультант Плюс: [сайт]. – URL: https://www.consultant.ru/document/cons_doc_LAW_304897// (дата обращения 01.04.2023 г.).
24. Вершицкая Г.В. Возможности использования виртуальных следов в ходе расследования киберпреступлений // Вестник поволжского института управления. - 2022. – Том 22. - № 2. - С. 17-23.

Zaporozhets S. A. Krainova N. A. On the issue of countering cybercrime in the conditions of a new geopolitical reality // Scientific notes of V. I. Vernadsky crimean federal university. Juridical science. – 2023. – T. 9 (75). № 3. – P. 448–456.

One of the most dangerous types of international crime is cybercrime. The prevention, detection and investigation of cybercrimes is extremely difficult due to the distance of the criminal from the crime scene and the socially dangerous consequences, the lack of a unified approach to the investigation of this type of crime and the development of procedures for interaction at the international level in the territories of different countries. The national legislation of the Russian Federation is currently in search of effective forms and methods of countering cybercrime in order to protect privacy and confidential information. In the context of the new geopolitical reality, the detection, investigation and suppression of cybercrimes becomes even more difficult due to the fact that there is no mutual understanding between some countries and the Russian Federation due to excessive politicization and engagement of state structures. In this paper, based on the study of the current regulatory framework, law enforcement practice, ways and means of improving national legislation, international legal norms, optimization of international cooperation in the field of countering cybercrime are proposed.

Keywords: cybersecurity, countering cybercrime, information protection, personal data, information, information protection.

Spisok literatury:

1. Brief description of the state of crime in the Russian Federation for January-December 2022. – Electronic text // Ministry of Internal Affairs of the Russian Federation : [website] – URL: https://мвд.рф/reports/item/35396677 /. (date of appeal 01.04.2023).
2. Putin called the fight against cybercrime one of the priorities of the Ministry of Internal Affairs. Electronic text // Sight. Business newspaper : [website] – URL: https://vz.ru/news/2023/3/20/1203922.html .
3.Yakimova E.M., Narutto S.V. International cooperation in combating cybercrime // Criminological Journal of the Baikal State University of Economics and Law. - 2016. – Vol. 10. - No. 2. - pp. 369-378.
4.Tropina T.L. Cybercrime: concept, state, criminal law measures of struggle: specialty 12.00.08 "Criminal law, criminal enforcement law and criminology" : dis. on the job. ... cand. jurid. Sciences / Tropina Tatiana Lvovna ; Far Eastern State University - Vladivostok, 2005. 234 p. – Direct text.
5. Antonyan E.A., Kleschina E.N. Cybercrime at the present stage: trends and directions of counteraction // Bulletin of Economic Security. - 2022. - No. 5. - pp. 11-15.
6. Convention on Computer Information Crime ETS No. 185 (Budapest, November 23, 2001 / Guarantor: [website]. – URL https://base.garant.ru/4089723 /. (accessed 01.04.2023).
7. Russia has submitted to the UN a draft convention on combating cybercrime. Electronic text // RIA Novosti: [website] – URL: https://ria.ru/20210727/konventsiya-1743130628.html . (accessed 01.04.2023).
8. Additional Protocol to the Convention on Crimes in the Field of Computer Information concerning the Introduction of Criminal Liability for Offenses Related to the Manifestation of racism and xenophobia committed through computer systems (ETS No. 189) of 28.01.2003 FZ / Garant : [website]. – URL: https://base.garant.ru/4084840 //(accessed 01.04.2023).
9. Directive of the European Parliament and of the Council of the European Union 2002/58/EC on the processing of personal data and the protection of privacy in the electronic communications sector, adopted as amended on 25.11.2009 / Garant : [website]. – URL: https://base.garant.ru/2570354 / (accessed 01.04.2023).
10. Directive of the European Parliament and of the Council of the European Union 2013/40/EC on attacks on information systems and the replacement of the Framework Decision 2005/222/PVD of the Council of the EU of 12.08.2013 / Guarantor : [website]. – URL: https://base.garant.ru/70557982 / (accessed 01.04.2023).
11. European Union Law / Consultant Plus : [website]. – URL: https://www.consultant.ru/cons/cgi/online.cgi?req=doc&base=ARB&n=568366&dst=100276#7ZFdCaTuq4QQQwA81 (accessed 01.04.2023).
12. Resolution of the IPA CIS dated 29.11.2018 No. 48-9 "On the new edition of the Model Law "On Personal Data". / Contour Standard: [website]. – URL: https://www.consultant.ru/document/cons_doc_LAW_61801
13. Agreement on cooperation of the CIS member states on combating crimes in the field of computer information / Garant: [website]. – URL: https://base.garant.ru/5283054 / (accessed 01.04.2023).
14. Krainova N.A. On the concept of the model law of the CIS member states "On combating cybercrime" // Law and Digital Economy. - 2022. - № 2 (16). - Pp. 48-56.
15. Federal Law "On Personal Data" dated 27.07.2006 No. 152-FZ / Consultant Plus: [website]. – URL: https://www.consultant.ru/document/cons_doc_LAW_61801 /(accessed 01.04.2023).
16. Federal Law "On Banks and Banking Activities" dated 02.12.1990 No. 351-1/ Consultant Plus: [website]. – URL: https://www.consultant.ru/document/cons_doc_LAW_5842 //(accessed 01.04.2023).
17. Federal Law "On the Central Bank of the Russian Federation (Bank of Russia)" dated 10.07.2002 No. 86-FZ / Consultant Plus: [website]. – URL: https://www.consultant.ru/document/cons_doc_LAW_37570 /
18. Federal Law "On the National Payment System" dated 27.06.2011 No. 161-FZ / Consultant Plus: [website]. – URL: https://www.consultant.ru/document/cons_doc_LAW_115625 / /(accessed 01.04.2023).
19. Federal Law "On Information, Information Technologies and Information Protection" dated 27.07.2006 No. 149-FZ/ Consultant Plus: [website]. – URL: https://www.consultant.ru/document/cons_doc_LAW_61798
20. Federal Law "On Trade Secrets" dated 29.07.2004 No. 98-FZ / Consultant Plus: [website]. – URL: https://www.consultant.ru/document/cons_doc_LAW_48699 / /(accessed 01.04.2023).
21. Federal Law No. 63-FZ "On Electronic Signature" dated 06/06/2011 / Consultant Plus: [website]. – URL: https://www.consultant.ru/document/cons_doc_LAW_112701 / / /(accessed 01.04.2023).
22. Federal Law "On the Security of Critical Information Infrastructure of the Russian Federation" dated 26.07.2017 No. 187-FZ / Consultant Plus: [website]. – URL: https://www.consultant.ru/document/cons_doc_LAW_220885 / / /(accessed 01.04.2023).
23. Information Letter of the Bank of Russia dated 14.08.2018 No. IN014-12/54 "On the national assessment of the risks of money laundering and terrorist financing" FZ / Consultant Plus: [website]. – URL: https://www.consultant.ru/document/cons_doc_LAW_304897 // (accessed 01.04.2023).
24. Vershitskaya G.V. Possibilities of using virtual traces during the investigation of cybercrimes // Bulletin of the Volga Institute of Management. - 2022. – Volume 22. - No. 2. - pp. 17-23.

.