ПРАВОВЫЕ АСПЕКТЫ ПРОТИВОДЕЙСТВИЯ КИБЕРПРЕСТУПНОСТИ НА ТЕРРИТОРИЯХ ГОСУДАРСТВ – УЧАСТНИКОВ СНГ

Дьяченко Наталья Николаевна
ФГКУ «ВНИИ МВД России»,
ведущий научный сотрудник НИЦ № 3,
подполковник полиции, к.ю.н.

Васильев Эдуард Анатольевич
ФГКУ «ВНИИ МВД России»,
главный научный сотрудник НИЦ № 3
д.ю.н., доцент

Аннотация: в статье на основе анализа двух- и многосторонних соглашений в сфере борьбы с киберпреступлениями между государствами – участниками СНГ, а также национального законодательства государств – участников СНГ рассматриваются правовые аспекты противодействия киберпреступности на территориях стран Содружества, рассматриваются проблемные вопросы в настоящей сфере и предлагаются пути их решения.

Ключевые слова: информационно-коммуникационные технологии, киберпреступность, преступления против информационной безопасности, государства – участники СНГ

Информационно-коммуникационные технологии[1] в настоящее время стали одной из наиболее распространенных, стержневых, глобальных форм человеческой деятельности, определяющих динамику развития мировой экономики и зависимых от нее ниш и сегментов. Глобальная тенденция цифровизации сокращает временные, материальные, административные и иные издержки в любых видах процессов и сделок. Однако помимо несомненной пользы обществу, глобальная цифровизация породила ряд проблем, одной из которых выступает использование ИКТ для совершения преступлений.

Сегодня киберпреступность активно выходит на лидирующие позиции наравне с торговлей оружием, проституцией и наркоторговлей, о чем все громче заявляют правоохранители различных стран мира. В настоящий момент мы наблюдаем, что в мировом сообществе пытаются навести порядок в данной

[1] Далее – ИКТ.

сфере и в той или иной мере взять Интернет под контроль.

На повышенную опасность киберпреступности указывает тот факт, что ущерб, причиняемый экономике данным видом преступности, колоссален по своим масштабам. Так, согласно данным экспертов «Лаборатории Касперского», в случае успешной атаки киберпреступников крупные компании теряют около 20 млн. рублей, а предприятия среднего и малого бизнеса в среднем 780 тыс. рублей за счет вынужденного простоя, упущенной прибыли и расходов на дополнительные услуги специалистов. На ликвидацию последствий инцидента и профилактику крупные компании дополнительно тратят около 2,1 млн. рублей, а небольшие - около 300 тыс. рублей [1, 87].

В настоящее время в рамках СНГ сформирована нормативная правовая база межгосударственного (многосторонние и двусторонние соглашения) и межведомственного уровня, а также национального уровня, регламентирующая вопросы борьбы с преступлениями, совершаемым с использованием ИКТ.

Преступления против информационной безопасности регламентированы соответствующим разделом 12 главы 30 Модельного Уголовного кодекса (Постановление Межпарламентской Ассамблеи государств участников СНГ от 17.02.1996, г. Санкт-Петербург). Кроме того, в иных разделах кодекса содержится ряд статей, предусматривающих ответственность за совершение преступлений, связанных с незаконным использованием компьютеров или компьютерной информации.

На многостороннем уровне взаимодействие органов внутренних дел государств – участников СНГ в сфере борьбы с киберпреступлениями определяется следующими документами:

Конвенцией о правовой помощи и правовых отношениях по гражданским, семейным и уголовным делам (СГГ СНГ от 22.01.1993, г. Минск);

Конвенцией о правовой помощи и правовых отношениях по гражданским, семейным и уголовным делам (СГГ СНГ от 07.10.2002, г. Кишинев);

Соглашение о сотрудничестве государств – участников СНГ в борьбе с преступностью (СГГ СНГ от 25.11.1998, г. Москва);

Соглашение об обмене информацией в сфере борьбы с преступностью (СГГ СНГ от 22.05.2009, г. Астана);

Соглашение о сотрудничестве государств – участников Содружества Независимых Государств в борьбе с преступлениями в сфере компьютерной информации (СГГ СНГ от 01.06.2001);

Соглашение о сотрудничестве государств – участников СНГ в области обеспечения информационной безопасности (СГГ СНГ от 20.11.2013, г. Санкт-Петербург);

Соглашение о сотрудничестве государств – участников СНГ в борьбе с преступлениями в сфере информационных технологий (СГГ СНГ от 28.09.2018, г. Душанбе)[2]. Оно определяет такие основные понятия, как «преступление в сфере компьютерной информации», «компьютерная информация», «вредоносная программа» и «неправомерный доступ», приводит перечень уголовно наказуемых деяний. В соответствии с названным Соглашением стороны намерены в соответствии с национальным законодательством, указанным Соглашением и другими международными договорами, участниками которых они являются, сотрудничать в целях обеспечения предупреждения, выявления, пресечения, раскрытия и расследования преступлений в сфере компьютерной информации. Сотрудничество сторон в рамках Соглашения осуществляется непосредственно их компетентными органами.

Концепция сотрудничества государств – участников СНГ в борьбе с преступлениями, совершаемыми с использованием информационных технологий (СГГ СНГ от 25.20.2013, г. Минск).

Регламент согласованных действий органов внутренних дел (полиции) государств – участников СНГ по противодействию новым видам преступлений, совершаемых на территории стран СНГ в сфере современных информационных технологий (СМВД от 20.07.2018, г. Баку).

Межгосударственная программа совместных мер борьбы с преступностью на 2019–2023 годы (СГГ СНГ от 28.09.2018 г., г. Душанбе).

На межведомственном уровне действуют следующие нормативные правовые документы:

[2] Документ вступил в силу для следующих государств: Республика Беларусь (12.03.2020), Кыргызская Республика (12.03.2020), Республика Узбекистан (12.03.2020), Республика Казахстан (06.06.2020), Республика Армения (22.01.2022), Российская Федерация (17.07.2022). Данные СПС КосультантПлюс по состоянию на 14.02.2023. Далее также Соглашение.

Соглашение о взаимодействии министерств внутренних дел независимых государств в сфере борьбы с преступностью (СМВД от 24.04.1992 г., г. Алма-Ата);

Соглашение о взаимодействии министерств внутренних дел в сфере обмена информацией (СМВД от 03.08.1992, г. Чолпон-Ата).

Проведенный анализ позволяет также охарактеризовать состояние и особенности борьбы с рассматриваемым негативным явлением на территориях государств – участников Содружества Независимых Государств.

Азербайджанская Республика

Азербайджанская Республика присоединилась к Конвенции о преступности в сфере компьютерной информации (23.11.2001 г., Будапешт) [2][3]. Взаимодействие с правоохранительными органами других стран в целях предупреждения, выявления, пресечения, раскрытия и расследования преступлений, совершаемых с использованием ИКТ осуществляется на основе двусторонних соглашений по борьбе с преступностью. В Уголовном кодексе Азербайджанской Республики закреплен ряд статей, устанавливающих ответственность за деяния, где в качестве квалифицирующего признака предусмотрено использование ИКТ.

Вопросы противодействия преступлениям, совершаемым с использованием ИКТ в МВД Азербайджанской Республики входят в компетенцию Главного управления по борьбе с организованной преступностью.

Республика Армения

В 2022 году вступил в силу новый Уголовный Кодекс Республики Армения, 38 глава которого посвящена преступлениям, направленным против компьютерной системы и безопасности компьютерных данных. УК Армении также предусматриваются преступления, где компьютер является орудием или средством преступления.

Вопросы противодействия преступлениям, совершаемым с использованием ИКТ, входят в функциональные обязанности следующих структурных подразделений главного управления по противодействию киберпреступности[4] Полиции МВД Республики Армения.

[3] Конвенция вступила в силу 01.07.2004.

[4] Далее – ГУКП.

1. Имущественные преступления – отдел по борьбе с преступлениями, совершаемыми в сфере высоких технологий Управления оперативно-розыскной информации и по борьбе с компьютерными преступлениями ГУКП Полиции МВД Республики Армения.

2. Незаконный оборот наркотиков – отдел по борьбе с незаконным оборотом наркотиков по Интернет сети Управления по борьбе с незаконным оборотом наркотиков ГУКП Полиции МВД Республики Армения.

3. Терроризм и экстремизм – отдел по борьбе с терроризмом и экстремизмом Управления розыска, по борьбе с незаконной миграцией и терроризмом ГУКП Полиции МВД Республики Армения.

4. Экономические преступления – отдел по борьбе с преступлениями в финансово-кредитной сфере Управления по борьбе с преступлениями против человека и собственности ГУКП Полиции МВД Республики Армения.

Республика Беларусь

Международное сотрудничество по оперативному обмену информацией в рамках противодействия преступлениям в сфере информационных технологий осуществляется на основании Соглашения о сотрудничестве государств – участников Содружества Независимых Государств в борьбе с преступлениями в сфере компьютерной информации от 01.06.2001[5], соглашений о сотрудничестве между МВД Республики Беларусь и МВД рядом зарубежных государств, в том числе с МВД Российской Федерации[6] от 30.09.1997, а также посредством международной сети национальных контактных пунктов «24/7», функционирующей под эгидой Римско-Лионской подгруппы «Группы Восьми».

В Уголовном кодексе Республики Беларусь установлена уголовная ответственность за деяния, где в качестве квалифицирующего признака предусмотрено использование ИКТ, также использование ИКТ в некоторых случаях установлено в качестве квалифицирующего признака. Вместе с тем

[5] Утверждено Указом Президента Республики Беларусь № 475 от 07.09.2001 «Об утверждении Соглашения о сотрудничестве государств – участников Содружества Независимых Государств в борьбе с преступлениями в сфере компьютерной информации».

[6] Соглашение о сотрудничестве между Министерством внутренних дел Российской Федерации и Министерством внутренних дел Республики Беларусь (Заключено в г. Москве 30.09.1997).

практика показывает, что с использованием ИКТ совершаются и иные преступления (наиболее часто встречаются клевета и оскорбление, менее распространены доведение до самоубийства и склонение к самоубийству).

Вопросы противодействия преступлениям, совершаемым с использованием ИКТ, входят в функциональные обязанности представителей криминальной милиции МВД Республики Беларусь в Главном управлении по противодействию киберперступности, в Главном управлении по наркоконтролю и противодействию торговле людьми (в том числе по линии наркоконтроля и по линии противодействия торговле людьми).

Республика Казахстан

Для взаимодействия с правоохранительными органами зарубежных государств и обмена информацией в Центре по борьбе с киберпреступностью Департамента криминальной полиции МВД Республики Казахстан функционирует Национальный контактный пункт «24/7», который ранее образован под эгидой «Группы восьми» (G8) для обмена оперативной информацией в сфере борьбы с киберпреступлениями. Координатором сети является Отдел уголовных, компьютерных преступлений и интеллектуальной собственности Министерства юстиции США.

Взаимодействие с правоохранительными органами стран Содружества осуществляется в рамках Соглашения о сотрудничестве государств – участников Содружества Независимых Государств в борьбе с преступлениями в сфере информационных технологий[7].

По фактам совершения уголовных правонарушений в сфере ИКТ, ответственность за которые предусмотрена в статьях главы 7 Уголовного Кодекса Республики Казахстан[8], проводится достаточно эффективная работа по предупреждению и профилактике, результатами которых является высокий процент раскрываемости уголовных правонарушений и сокращение фактов их совершения.

Кыргызская Республика

Кыргызская Республика осуществляет собственное движение к цифровой трансформации национальной экономики и обеспечению доступа граждан к

[7] Ратифицировано Законом Республики Казахстан от 09.12.2019 № 277-VI ЗРК.
[8] Далее – УК РК.

современным цифровым сервисам. Построение цифровой экономики рассматривается как необходимое условие и национальный приоритет развития Кыргызской Республики на краткосрочную и среднесрочную перспективы. Контуры стратегии цифровой трансформации кыргызской экономики формируются в рамках Концепции цифровой трансформации «Цифровой Кыргызстан 2019-2023», одобренной решением Совета безопасности Кыргызской Республики от 14.12.2018 № 2.

Республикой заключены соглашения, направленные на организацию взаимодействия с правоохранительными органами других стран в целях предупреждения, выявления, пресечения, раскрытия и расследования преступлений, совершаемых с использованием ИКТ:

Соглашение о сотрудничестве между Министерством внутренних дел Кыргызской Республики и МВД Российской Федерации (16.06.2007, г. Санкт-Петербург);

Соглашение о сотрудничестве между Министерством внутренних дел Кыргызской Республики и Министерством внутренних дел Республики Казахстан (04.09.2014, г. Чолпон-Ата);

Соглашение о сотрудничестве между Министерством внутренних дел Республики Кыргызстан и Министерством внутренних дел Республики Узбекистан (13.05.1992, г. Ош);

Соглашение о сотрудничестве между Министерством внутренних дел Кыргызской Республики и Министерством внутренних дел Республики Таджикистан (04.09.2014, г. Чолпон-Ата).

К законодательству Кыргызской Республики в сфере кибербезопасности могут быть отнесены:

1. Стратегия кибербезопасности Кыргызской Республики на 2019-2023 годы (утверждена постановлением Правительства Кыргызской Республики от 24.07.2019 года № 369 «Об утверждении Стратегии кибербезопасности Кыргызской Республики на 2019-2023 годы»).

2. Национальная стратегия развития Кыргызской Республики на 2018-2040 годы (утверждена указом Президента Кыргызской Республики от 31.10.2018 УП № 221 «О Национальной стратегии развития Кыргызской Республики на 2018-2040 годы»).

3. Концепция информационной безопасности Кыргызской Республики на 2019-2023 годы (утверждена Постановление Правительства Кыргызской Республики от 03.05.2019 года № 209 «О Концепции информационной безопасности Кыргызской Республики на 2019-2023 годы»).

4. Концепция цифровой трансформации «Цифровой Кыргызстан 2019-2023» (утверждена Решением Совета безопасности Кыргызской Республики от 14.12.2018 № 2 у).

5. Концепция национальной безопасности Кыргызской Республики (утверждена Указом Президента Кыргызской Республики от 20.12.2021 № 570 «О Концепции национальной безопасности Кыргызской Республики»).

6. Законы Кыргызской Республики от 19.07.2017 № 127 «Об электронном управлении», от 14.04.2008 № 58 «Об информации персонального характера», от 15.12.2017 № 210 (15) «О защите государственных секретов Кыргызской Республики».

Постановлением Правительства Кыргызской Республики от 21.05.2020 № 266 «О некоторых вопросах в сфере обеспечения кибербезопасности Кыргызской Республики» было утверждено «Положение о Координационном центре по обеспечению кибербезопасности Государственного комитета национальной безопасности Кыргызской Республики», также утвержден главный уполномоченный орган в сфере обеспечения кибербезопасности, реагирования на компьютерные инциденты, а также по выявлению, предупреждению и пресечению причин и условий, способствующих подготовке и реализации компьютерных атак – Государственный комитет национальной безопасности.

Уголовным Кодексом Кыргызской Республики с квалифицирующим признаком использования ИКТ предусмотрен ряд статей в сфере имущественных преступлений, в экономической сфере, а также иные составы преступлений, где в качестве квалифицирующего признака предусмотрено использование ИКТ.

Республика Молдова

Двусторонние соглашения, направленные на организацию взаимодействия правоохранительных органов других стран в целях предупреждения выявления, пресечения, раскрытия и расследования преступлений, совершаемых с использованием ИКТ в Республике отсутствуют.

Ответственность за деяния, где в качестве квалифицирующего признака предусмотрено использование ИКТ установлена Уголовным кодексом Республики Молдова за имущественные преступления, преступления в сфере с незаконного оборота наркотических средств и психотропных веществ, преступления в экономической сфере, преступления экстремисткой направленности, преступления, совершаемые против несовершеннолетних. Также внесены предложения в Уголовный кодекс РМ по регулированию «Незаконных операций с безналичными средствами платежа».

Российская Федерация

Существующая оценка криминологической ситуации, связанной со сферой IT-преступности, подтверждается созданием специализированных подразделений по борьбе с преступлениями в сфере высоких технологий.

Так, в состав МВД России входит подразделение – Бюро специальных технических мероприятий (БСТМ), одним из направлений деятельности которого является борьба с преступлениями в сфере компьютерных технологий, региональные подразделения БСТМ действуют во всех субъектах России. В структуру БСТМ МВД России также входит Управление «К», раскрывающее преступления в сфере информационных технологий. Дополнительно в декабре 2020 года принято решение о создании в МВД России киберполиции, в Следственном департаменте МВД России и территориальных органах предварительного следствия созданы специализированные подразделения по расследованию преступлений, совершенных с использованием ИКТ. Также в МВД России в 2022 году создано Управление по организации борьбы с противоправным использованием ИКТ [3].

С 2013 года в Российской Федерации образована и действует Государственная система обнаружения, предупреждения и ликвидации последствий компьютерных атак, которой обеспечение информационной безопасности по сервисной модели осуществляется в соответствии с требованиями и методическими рекомендациями ФСБ России и ФСТЭК России.

Российский Уголовный кодекс в главе 28 «Преступления в сфере компьютерной информации» содержит четыре вида преступления, однако круг совершаемых с использованием информационных технологий деяний куда как более широк.

Республика Таджикистан

Заключаемые Республикой двусторонние соглашения, направленные на организацию взаимодействия с правоохранительными органами других стран в целях предупреждения, выявления, пресечения, раскрытия и расследования преступлений, совершаемых с использованием ИКТ, опираются на «Конвенцию о правовой помощи и правовых отношениях по гражданским, семейным и уголовным делам» (22.01.1993, г. Минск).

В настоящее время на основе протокола, подписанного в рамках переговоров между Департаментом общественной безопасности города Нанкина КНР и Управлением МВД по городу Душанбе, осуществляется совместная реализация договоренностей и сотрудничество, направленное на поощрение и внедрение устойчивых передовых методов предупреждения и пресечения преступлений, фактов присоединения граждан республики к международным террористическим группировкам, незаконного оборота наркотиков, оружия и региональной безопасности. Периодически изучается передовой опыт Департамента общественной безопасности г. Нанкина по обеспечению общественного порядка, борьбе с преступностью и другим приоритетным направлениям, которые непосредственно используются в практической оперативно-служебной деятельности УМВД.

В Уголовном кодексе Республики Таджикистан определена отдельная глава 28 (Преступления против информационной безопасности), где квалифицирующим признаком являются деяния, связанные с информацией, хранящейся в компьютерной системе, сети или на машинных носителях. В 15 статьях УК РТ в качестве квалифицирующего признака предусмотрена ответственность за использование ИКТ. Также установлены иные составы преступлений, совершаемые с использованием ИКТ.

Республика Узбекистан

В Республике планируется создать систему предотвращения киберпреступности и разработать Стратегию кибербезопасности Республики Узбекистан на 2023-2026 годы. Определен комплекс задач и основные направления по кибербезопасности интернет-пространства в доменной зоне «UZ», а также по защите электронного правительства, энергетики, цифровой экономики и других сфер, связанных с важной информационной инфраструктурой. Одно-

временно планируется пересмотреть уголовную ответственность за киберпреступность.

Система мониторинга кибератак и угроз в информационном пространстве будет и дальше совершенствоваться. Это включает в себя расширение технической инфраструктуры Единой сети кибербезопасности, дальнейшее ускорение деятельности «IT-парка инноваций в кибернетике», а также проведение на базе центров обучения цифровым технологиям в регионах обучения по кибербезопасности для молодежи, ежегодное проведение республиканских конкурсов среди учащихся и студентов по выявлению кибератак.

Статья 3 Закона Республики Узбекистан от 15.04 2022 № ЗРУ-764 «О киберпреступности» гласит, что киберпреступность - совокупность преступлений, осуществляемых в киберпространстве с использованием программного обеспечения и технических средств с целью завладения информацией, ее изменения, уничтожения или взлома информационных систем и ресурсов.

В национальном понимании под преступлениями в сфере информационных технологий понимаются такие уголовно запрещенные под угрозой наказания общественно опасные деяния, которые непосредственно совершены с использованием информационных технологий и информационно-телекоммуникационных сетей, в виртуальном мире. В Узбекистане термин «киберпреступность» употребляется в тесной связи с преступлениями, совершенными с использованием информационных технологий. Но учитывая, что преступления с использованием информационных технологий является более широким понятием, нежели киберпреступность, употребления термина «киберпреступность» для обозначения широкого спектра правонарушений, включая традиционные компьютерные и сетевые преступления, не является критической ошибкой в толковании.

На данный момент двусторонних соглашений, направленных на организацию взаимодействия с правоохранительными органами других стран в целях предупреждения, выявления, пресечения, раскрытия и расследования преступлений, совершаемых с использованием ИКТ, в Республике Узбекистан не имеется.

Глава XXI Уголовного кодекса Республики Узбекистан очерчивает спектр преступлений в сфере информационных технологий. Также в уголовном законодательстве имеются преступления, где в качестве квалифицирующего

признака или диспозиции предусмотрено использования информационных технологий. В связи с ростом экономических преступлений в 2022 году было ужесточено наказание краж и мошенничеств, так как данные виды преступлений начали совершаться с использованием высоких технологий. В настоящее время ведется работа по внесению дополнений и изменений в Уголовный кодекс Республики Узбекистан касательно оборота наркотических средств с использованием информационных технологий и сети Интернет, а также прорабатывается нормы упорядочивающие взаимоотношения, где объектом выступают цифровые финансовые активы, криптовалюты, а также токены.

Как можно видеть из проведенного анализа на территориях государств – участников СНГ в ответ на усиление и активизацию киберпреступности происходит реагирование со стороны государств: заключаются двух- и многосторонние соглашения в сфере борьбы с киберпреступлениями между государствами – участниками СНГ, а также зарубежными странами, принимаются новые законы. С учетом национальных особенностей киберпреступности в уголовных кодексах криминализируются деяния, связанные с неправомерным использованием ИКТ, а уже имеющиеся составы преступлений дополняются квалифицирующим признаком - использованием ИКТ, делаются попытки нормативно определить понятия «преступлений в сфере информационных технологий», «киберпреступность».

Несмотря на ряд принятых законодательных проектов по борьбе с киберпреступностью, в странах Содружества все же продолжают оставаться проблемы, препятствующие эффективному осуществлению данной борьбы.

Одной из первых стоит выделить длительность законодательного ответа на появление новых видов киберпреступности.

Механизмы борьбы с киберпреступностью разрабатываются и действуют исходя из общепризнанных норм международного права и необходимости соблюдения обязательств по международным договорам, правовых режимов, установленных модельным законодательством, с учетом норм национального законодательства. Чтобы согласовать и учесть все это требуются значительные временные затраты, в том время как преступники, необремененные необходимостью соблюдения закона, действуют на опережение и находятся на несколько шагов впереди тех, кто им противодействует. Для того, чтобы успевать за быстро меняющейся преступностью, существующие законода-

тельные процедуры нуждаются в максимальном упрощении.

Различия в национальных законодательствах стран Содружества, затрудняющие международное сотрудничество в борьбе с преступлениями, совершаемыми с использованием ИКТ (сети Интернет), также препятствуют эффективной борьбе с рассматриваемыми деяниями.

Так, например, несмотря на наличие перечня деяний, относимых к категории совершенных в сфере информационных технологий, отсутствует терминологическая определенность в характеристике киберпреступлений; отдельные деяния, такие, как наркопреступность с использованием информационно-телекоммуникационных сетей в качестве элемента состава либо в качестве квалифицирующего признака находит свое отражение в УК не всех стран – участников.

Для решения отмеченных проблем, а также повышения эффективности борьбы с киберпреступностью на территориях государств – участников СНГ целесообразно предпринять ряд мер, направленных на достижение согласованности и оперативности действий по ряду вопросов.

Видится необходимой гармонизация уголовно-правовых и уголовно-процессуальных норм, предусматривающих ответственность за совершение киберпреступлений, содержащихся в законодательстве государств, сотрудничающих в сфере борьбы с киберпреступностью, включая своевременное совершенствование модельного и на его основе - национального законодательства с учетом возникновения новых технических угроз. Необходима разработка единого перечня преступлений, совершаемых с использованием ИКТ, с учетом современных их видов. Это можно сделать путем актуализации раздела 12 главы 30 Модельного Уголовного кодекса «Преступления против информационной безопасности» и внесения соответствующих корректив в иные его разделы, где содержатся статьи, предусматривающие ответственность за совершение преступлений, связанных с незаконным использованием ИКТ.

Учитывая то, что развитие кибертехнологий и вовлечение их в совершение преступлений идет максимально быстро, требуется адекватное реагирование со стороны законодательной базы. Повышению эффективности противодействия киберпреступлениям будут способствовать актуализация Соглашение о сотрудничестве государств - участников Содружества Независимых Государств в борьбе с преступлениями в сфере информационных технологий от 28.09.2018.

В целях урегулирования проблемы отсутствия единого понимания терминов, используемых при организации взаимодействия правоохранительных органов стран Содружества, имеется необходимость в разработке Глоссария терминов, связанных с противодействием преступлениям, совершаемым с использованием ИКТ.

Список литературы

1. Евдокимов К.Н. Структура и состояние компьютерной преступности в Российской Федерации // Юридическая наука и правоохранительная практика. № 1 (25) 2016. С. 87-94.
2. Конвенция о преступности в сфере компьютерной информации ETS № 185 (Будапешт, 23.11.2001).
3. Мвд.рф/news/item/32844180/. Дата обращения 19.04.2023.

LEGAL ASPECTS OF COUNTERING CYBERCRIME IN CIS MEMBER STATES

Natalia Dyachenko
Federal State Budgetary Institution "All-Russian Scientific Research Institute of the Ministry of Internal Affairs of the Russian Federation " Leading Researcher at Research Center No. 3, Police Lieutenant Colonel, Ph.D. of Juridical Sciences

Eduard Vasiliev
Federal State Budgetary Institution "All-Russian Scientific Research Institute of the Ministry of Internal Affairs of the Russian Federation " Chief Researcher, Research Center No. 3 Ph.D. of Juridical Sciences, Associate Professor

Abstract: The article, based on an analysis of bilateral and multilateral agreements in the field of combating cybercrime between the CIS member states, as well as the national legislation of the CIS member states, examines the legal aspects of combating cybercrime in the territories of the Commonwealth countries; considers problematic issues in this area and suggests ways to solve them.

Key words: information and communication technologies, cybercrime, crimes against information security, CIS member states

Հոդվածը գրախոսվել է՝ 16.05.2023թ.:
Ներկայացվել է տպագրության՝ 17.05.2023թ.: