ПРОБЛЕМНЫЕ АСПЕКТЫ БОРЬБЫ С КИБЕРПРЕСТУПНОСТЬЮ В ГОСУДАРСТВАХ-УЧАСТНИКАХ СНГ

Надейкина Ольга Андреевна
Старший научный сотрудник 2 отдела
НИЦ № 3 ФГКУ «Всероссийского
научно-исследовательского
института Министерства внутренних дел России»,
подполковник полиции

Аннотация*. Введение.* В статье рассматриваются проблемные аспекты борьбы с киберпреступностью в странах-участниках СНГ.

Методы. Анализ информации, предоставленной из МВД стран-участниц СНГ. Анализ статистических данных Главного информационно- аналитического центра Министерства внутренних дел России.

Выводы и предложения. На основе проведенного статистического анализа стоит сделать вывод о своевременности и актуальности проведенного анализа в киберпреступности.

Ключевые слова: киберпреступность, страны-участники Союза независимых государств, информационно-компьютерные технологии.

Киберпреступность – это преступная деятельность, в рамках которой используются либо атакуются компьютер, компьютерная сеть или сетевое устройство. Большинство кибератак совершается киберпреступниками или хакерами с целью получения финансовой прибыли. Однако целью кибератак может быть и выведение компьютеров или сетей из строя – из личных или политических мотивов.

Киберпреступления совершают как физические лица, так и юридические – от начинающих хакеров до слаженных группировок, которые используют продвинутые методы и хорошо подкованы технически[1].

К типам киберпреступлений относятся такие виды преступлений как мошенничество с использованием электронной почты и интернета; кража

[1] http://www.kaspersky.ru/resource-center/threats/what-is-cybercrime (Дата обращения 14.03.2023 г.)

цифровой личности (хищение и использованием личных данных); кража платежных карт и другой финансовой информации; хищение и перепродажа корпоративных данных; кибершантаж (вымогательство денег под угрозой атаки); криптоджекинг (майниг криптовалют с использованием чужих ресурсов); кибершпионаж (получение несанкционированного доступа к государственным или корпоративным данным); нарушение работы систем с целью компрометации сети; нарушение авторских прав; незаконное проведение азартных игр; онлайн-торговля запрещенными товарами; домогательства, изготовление или хранение детской порнографии.

Специфика киберпреступлений заключается в том, что они совершаются дистанционно, зачастую с территории других стран, и ни одно государство в мире не способно в одиночку бороться с ними. Одновременно с этим стоит отметить, что напряженная ситуация в киберсфере связана с недостатками современной системы международного сотрудничества по соответствующим вопросам. Результаты кибератак могут быть разрушительными и даже приводить к катастрофам, в том числе в сфере нацбезопасности. Большинство ИТ-преступников ведут свою деятельность для извлечения финансовой выгоды или подрыва политических основ государства.

Стоит отметить, что киберпреступность угрожает национальной безопасности любого государства, так как на сегодняшний день проблема борьбы с ней глобально не изучена и нет единого правового и практического способа борьбы с ней. Преступное мастерство ИТ-преступников достигло совершенства - кибервзломщики не только блокируют компьютеры, но и похищают важную информацию, включая резервные копии, требуя затем выкуп, как за восстановление работы системы, так и за обещание не передавать перехваченные сведения широкой огласке.

В сложившихся реалиях цифровая безопасность (кибербезопасность) становится предметом пристального внимания со стороны государств - участников Содружества Независимых Государств, а ее обеспечение нуждается в комплексном правовом регулировании.

Несмотря на ряд принятых законодательных проектов по борьбе с киберпреступностью государствах-участниках СНГ все же существуют проблемы.

1. Одной из первых стоит выделить отсутствие единого правового обеспечения между странами – участниками СНГ. Злоумышленники дейст-

вуют на опережение и находятся на несколько шагов впереди тех, кто им противодействует: законодательство не успевает за новыми угрозами в сфере высоких технологий.

Решение законодательных вопросов стран СНГ приведет к положительным результатам борьбы с киберпреступностью.

Функционирование единого экономического пространства в пределах СНГ невозможно без разработки и реализации действенных механизмов обеспечения защиты от противоправных посягательств. Предусматриваемые модельным законодательством механизмы должны учитывать особенности национального законодательства, признавая право каждого государства закреплять нормы, касающиеся противодействия преступности. В то же время законопроект должен включать нормы, применимые во всех национальных юрисдикциях, минимизируя предпочтения того или иного государства в пределах СНГ. Необходима гармонизация уголовно-правовых норм, предусматривающих ответственность за совершение киберпреступлений.

Для повышения эффективности противодействия киберпреступлениям необходимо сформировать многоуровневую институциональную систему кибербезопасности, которая будет включать в себя:

- прозрачные алгоритмы обсуждения вопросов обеспечения кибербезопасности как на национальном, так и на межгосударственном уровнях;

- гармонизацию уголовно-правовых и уголовно-процессуальных норм, предусмотренных законодательством государств, сотрудничающих в сфере борьбы с киберпреступностью, включая своевременное совершенствование законодательства с учетом возникновения новых технических угроз;

- сложившуюся практику заключения межгосударственных соглашений, предусматривающих конкретные мероприятия, направленные на противодействие киберпреступности;

- усиление взаимодействия национальных спецслужб и правоохранительных органов, координацию их действий, оперативное реагирование на поступающие запросы о взаимодействии;

- формирование современной материально-технической и кадровой базы для борьбы с киберпреступностью;

- повышение технической, цифровой и финансовой грамотности

населения[2];

- координацию деятельности всех участников противодействия киберпреступности, начиная с правоохранительных органов и заканчивая исследовательскими и академическими структурами[3].

В российской уголовной практике киберпреступления не выделяются в отдельную группу. Глава 28 «Преступления в сфере компьютерной информации» содержит четыре вида преступления, напрямую относящиеся к группе киберпреступлений, но, как показывает практика, киберпреступления крайне редко расследуются, а еще реже по ним удается установить преступников и привлечь к ответственности. Правоохранительные органы с трудом расследуют такие преступления из – за нехватки специальных методов и средств.

2. Немаловажным проблемным аспектом является трансграничность. Киберпреступления не являются сугубо «национальным бедствием».

На трансграничность и влияние на взаимозависимость национальных экономик преступных кибератак обратил особое внимание министр иностранных дел Российской Федерации С.В. Лавров, который отметил, что «преступная активность в онлайн-режиме, входящая, согласно рейтингу Всемирного экономического форума (ВЭФ), в пятерку глобальных рисков, угрожает существованию и успешному функционированию целых отраслей».[4]

Масштабы и динамика роста киберпреступлений не могут не вызывать беспокойства в пределах СНГ ввиду их трансграничного характера и угроз как национальной безопасности государств, так и межнациональной безопасности. Выступая 17 ноября 2021 г. на ежегодной, девятой встрече секретарей Советов Безопасности стран СНГ, заместитель секретаря Совбеза России О. Храмов подчеркнул, что «масштаб ущерба гражданам и бизнесу дает основания

---

[2] Цифровое право: глоссарий понятий / под общ. ред. **В.В. Блажеева, М.А. Егоровой**. М.: Проспект, 2020. 64с

[3]См: статья: «О концепции модельного закона стран - участниц СНГ "О борьбе с киберпреступностью"

Крайнова Н.А. «Право и цифровая экономика», 2022, № 2, С.8-10.

[4] **Лавров С.В**. Глобальные проблемы кибербезопасности и международные инициативы России по борьбе с киберпреступностью//Внешнеэкономические связи. 2020. URL: https://www.mid.ru/foreign_policy/international_safety/regprla/-/asset_publisher/ycxlfjnkud1w/content/id/4350978 (дата обращения: 19 ноября 2021 г.).

рассматривать эти преступления как угрозу национальной безопасности». При этом он отметил, что «наибольшее число киберпреступлений составляют дистанционные кражи и мошенничества, а также сбыт наркотиков»[5].

3. Отдельной проблемой стоит выделить отсутствие отдельной графы статистики ГИАЦ МВД России по числу случаев киберпреступлений и размеру ущерба в отношении юридических и физических лиц. Данная статистика даст возможность правоохранительным органам делать быстрый анализ и качественное прогнозирование, оперативно реагировать на изменение ситуации в сфере киберпреступлений.

За последние несколько лет во всех странах фиксируются изменения преступности в сторону увеличения доли киберпреступлений. Не являются исключением и страны, входящие в Содружество Независимых Государств.

Например, согласно статистке МВД России, подразделениями органов внутренних дел в 2021 году выявлено 81,8% от общего количества зарегистрированных преступлений экономической направленности и 74 % криминальных деяний коррупционной направленности.

В 2022 году выявлено более 64 тыс. преступлений экономической направленности. В крупном и особо крупном размере совершено более 22,5 тыс. преступлений. Размер материального ущерба составил 183 млрд. рублей. При этом наложен арест на имущество, добровольно погашено, либо изъято имущества, денег и ценностей на сумму свыше 230 млрд. руб.[6].

Однако данный расчет можно сделать только исходя из общего количества зарегистрированных преступлений экономической направленности, отдельно выделить киберпреступления не представляется возможным.

4. Немаловажным фактором представляется недостаточная подготовка сотрудников правоохранительных органов в области знаний компьютерных технологий. В настоящее время знание основ компьютера для сотрудника правоохранительных органов является нормой, однако, для выявления и раскрытия киберпреступлений необходимы специальные знания в данной

[5] Совбез РФ: Масштаб киберпреступлений угрожает национальной безопасности // URL: https://rg.ru/2021/11/17/sovbez-rf-masshtab-kiberprestuplenij-ugrozhaet-nacionalnoj-bezopasnosti.html (дата обращения: 18 ноября 2021 г.).

[6] http://www.tadviser.ru/index (Дата обращения 14.03.2023 г.)

области. В связи с чем, является необходимостью получения дополнительного образования сотруднику правоохранительных органов.

5. Еще одним проблемным аспектом является отсутствие упрощенных способов взаимодействия между сотрудниками правоохранительных органов стран-участниц СНГ. Взаимодействие государств – участников СНГ в сфере борьбы с преступностью посредством бумажного документооборота приводит к затягиванию оформления требуемых документов, сроков процессуальных действий, а также утрате подлинных экземпляров документов при их отправлении.

Страны – участники СНГ выделяют следующие проблемные аспекты:

МВД Республики Азербайджан:

- сложности в приобретении из базы данных зарубежных компаний информации для идентификации личности лиц, которые при совершении преступлений воспользовались приложениями для обмена мгновенными сообщениями, либо социальными сетями;

- определение иностранных IP – адресов, которыми воспользовались преступники;

- идентификация личности преступников, которые воспользовались услугой VPN;

- нахождение серверов использованных электронных почт за границей;

- сложности в получении информации из зарубежных стран.

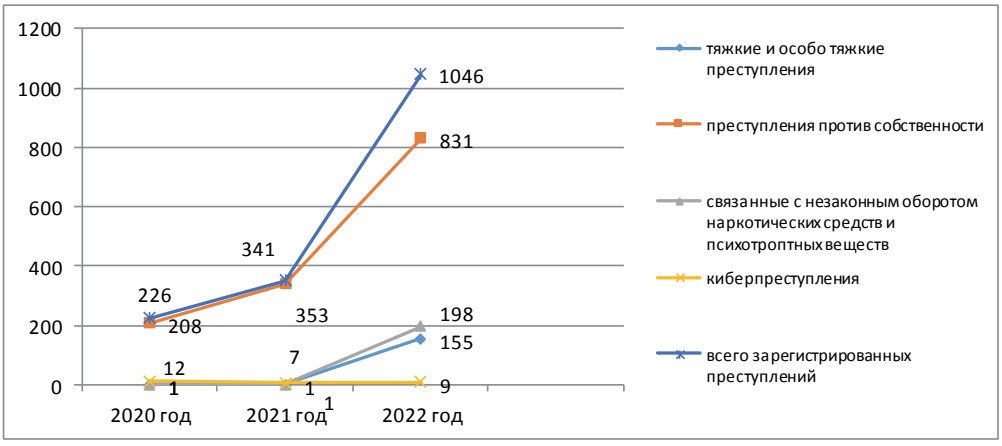

Рисунок 1. Количество зарегистрированных преступлений, совершенных с использованием ИКТ за 2020-2022 гг. в Республике Азербайджан

МВД Республики Армения указывает на проблему имеющихся различий в законодательствах стран – участников СНГ.

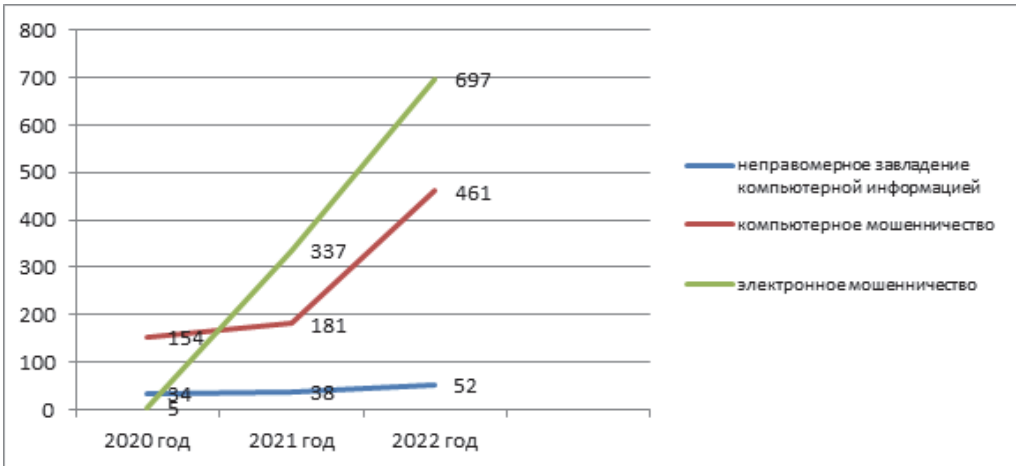

Рисунок 2. Количество зарегистрированных преступлений, совершенных с использованием ИКТ за 2020 - 2022 год в Республике Армения

МВД Республики Беларусь одной из важнейших проблем считает отсутствие взаимодействия между правоохранительными органами стран – участник СНГ. Анализ киберпреступлений показал, что такие преступления обладают рядом характерных признаков, существенно затрудняющих их раскрытие «по горячим следам»: а именно трансграничный характер совершения, использование динамичных IP – адресов, принадлежащих преимущественно зарубежным сегментам сети Интернет.

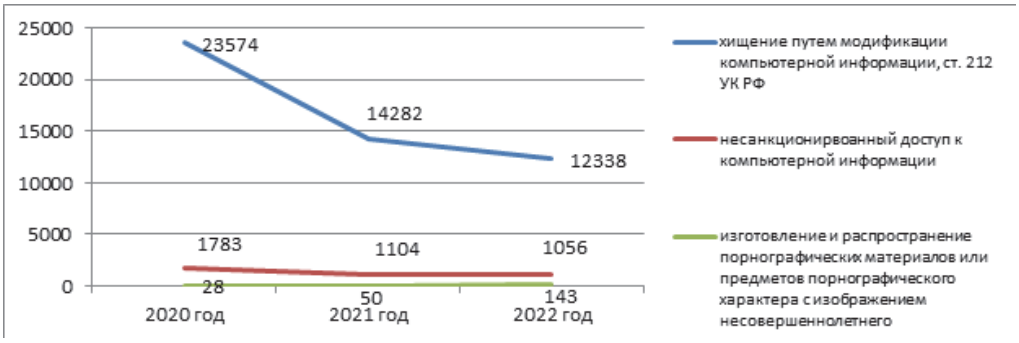

Рисунок 3. График преступлений, совершенных с использованием ИКТ за 2020-2022 гг. в Республике Беларусь

МВД Республики Казахстан основной проблемой считает отсутствие оперативного обмена информации, касательно социальных сетей и почтовых сервисов, не зарегистрированных на территории Казахстан; использование прокси-серверов, использование VPN, использование криптокошельков, отсутствие представителей зарубежных технических площадок.

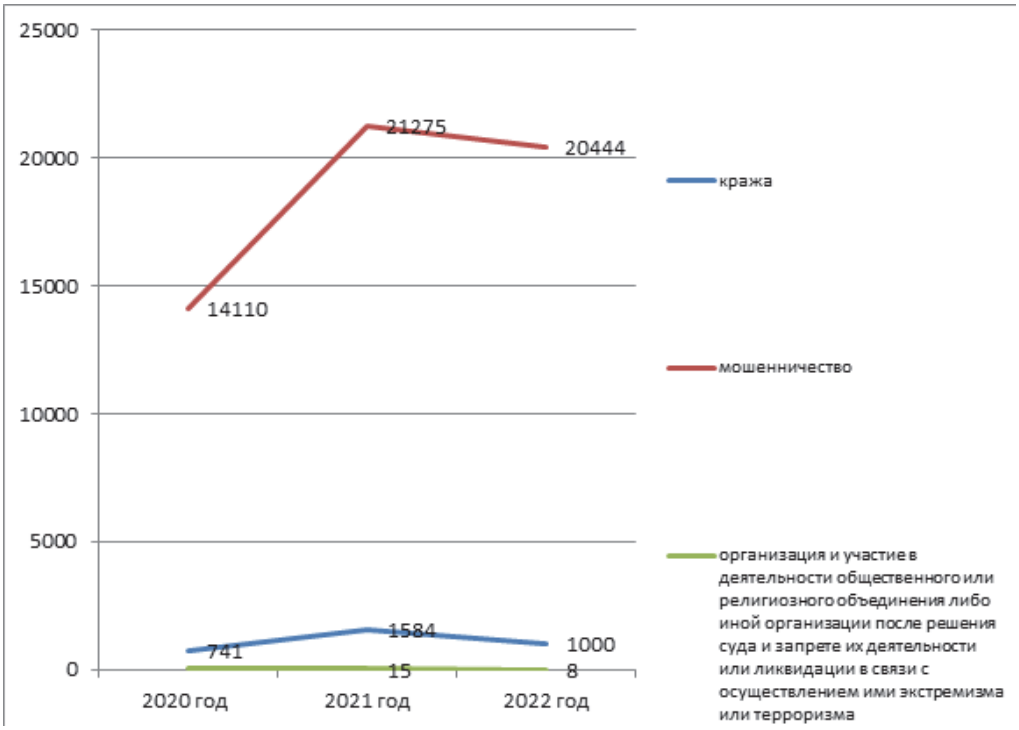

Рисунок 4. Количество зарегистрированных преступлений, совершенных с использованием ИКТ за 2020-2022 гг. в Республике Казахстан

МВД Кыргызской Республики указывает на отсутствие специализированных компьютерных программных обеспечений, позволяющих отследить выводы криптовалют (bitcoin, ethereum, litecoin и т.д.), и их дороговизна. Отсутствие оперативности при получении ответов на запросы при межгосударственном сотрудничестве. Необходимость повышения квалификации сотрудников правоохранительных органов.

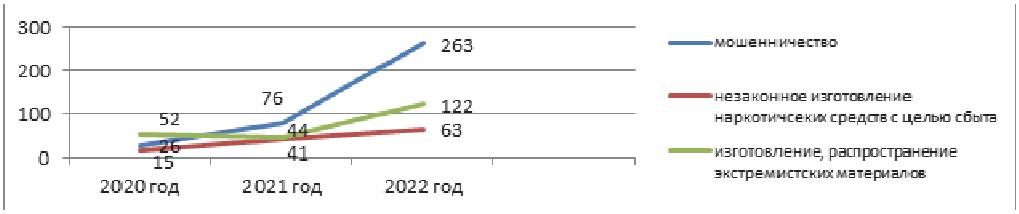

Рисунок 5. Количество, зарегистрированных преступлений, совершенных с использованием ИКТ за 2020-2022 гг. в Кыргызской Республики

МВД Республики Молдовы указывает на проблему долгосрочности ответов на запросы.

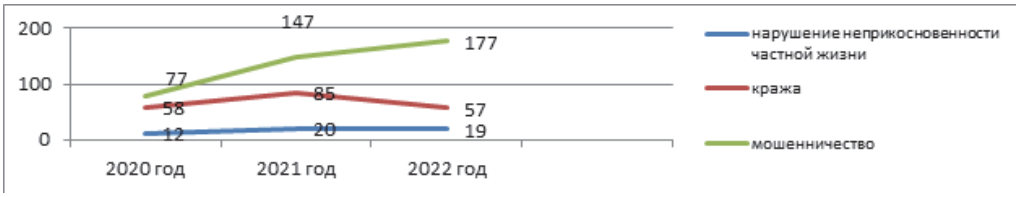

Рисунок 6. Количество зарегистрированных преступлений, совершенных с использованием ИКТ за 2020-2022 гг. в Республики Молдова

МВД Республики Таджикистан указывает на следующие проблемные аспекты:

- недостаточное количество сотрудников с специализированными знаниями в области информационно-коммуникационных технологий;

- отсутствие передового опыта и обмена информацией, в том числе методической литературы в данной сфере, соответствующих служб и подразделений по совместному, комплексному применению оперативных мер по борьбе с преступлениями, совершаемых с использованием ИКТ;

- не в полной мере соответствует реалиям обеспеченность органами милиции оборудованиями ИКТ, современными технологиями в данной борьбе; эффективность и уровень международного взаимодействия по данному направлению деятельности;

- необходимость внесения изменений и дополнений в статьи УК Республики Таджикистан, а именно за имущественные преступления (кражи, мошенничества, вымогательства и другие преступления в сфере незаконного оборота наркотиков, также преступления в экономической сфере, предусматривающие уголовную ответственность за деяния, где в качестве квалифици-

рующего признака предусмотрено использование информационно-коммуникационных технологий).

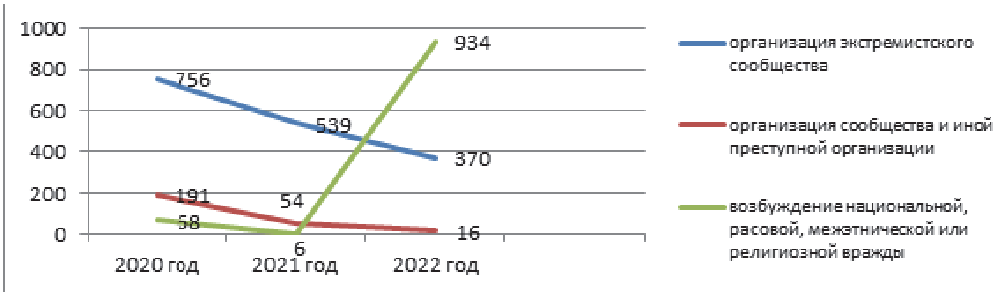

Рисунок 7. Количество зарегистрированных преступлений, совершенных с использованием ИКТ за 2020- 2022 гг. в Республике Таджикистан

МВД Республики Узбекистан также считает проблемой сложность в получении информации касательно транзакции похищенных у граждан денежных средств.

Таким образом, следует сделать вывод, что борьба с киберпреступлениями на сегодняшний день находится на стадии становления, продолжает развиваться правовая база в области противодействия данным преступлениям на национальном, региональном и международном уровнях. Однако в глобальном плане пока нет единого международного правового механизма противодействия преступлениям в сфере цифровых технологий, не выработана единая терминология, и это осложняет взаимодействие государств в данной области.

PROBLEMATIC ASPECTS OF COMBATING CYBERCRIME IN THE CIS MEMBER STATES

Olga Nadeikina

Senior Researcher, Department 2,
Research Center No. 3 of the Federal
State Budgetary Institution "All-Russian Scientific
Research Institute of the Ministry of Internal
Affairs of the Russian Federation "

Annotation. Introduction. The article discusses the problematic aspects of the fight against cybercrime in the CIS member countries.

Methods. Analysis of information provided by the Ministry of internal Affairs of the CIS member states. Analysis of statistical data of the Main Information and Analytical Centre of the Ministry of Internal Affairs of Russia.

Conclusions and offers. Based on the statistical analysis carried out, it is worth making a conclusion about the timeliness and relevance of the analysis in the field of gas production and transportation.

Key words: cybercrime, member countries of the Union of Independent States and computer technologies.

Հոդվածը գրախոսվել է՝ 16. 05.2023թ.:
Ներկայացվել է տպագրության՝ 17.05.2023թ: