

Нигматов Руфтулло Олимджонович

Ўзбекистон Республикаси ИИВ Академияси бошлиғининг илмий ишлар ва
инновациялар бўйича ўринбосари, фалсафа фанлари доктори, доцент

ВИРТУАЛ МАКОНДА ЖИНОЯТЛАРГА ҚАРШИ КУРАШИШ БЎЙИЧА ХАЛҚАРО ҲАМКОРЛИК

Нигматов Руфтулло Олимджонович

Доктор философских наук, доцент, заместитель начальника Академии
МВД Республики Узбекистан по научной работе и инновации.

МЕЖДУНАРОДНОЕ СОТРУДНИЧЕСТВО ПО ПРОТИВОДЕЙСТВИЮ ПРЕСТУПЛЕНИЯМ В ВИРТУАЛЬНОМ ПРОСТРАНСТВЕ

Nigmatov Ruftullo

Deputy Head of the Academy of the Ministry of Internal Affairs of the Republic of
Uzbekistan for scientific work and innovation, Doctor of Philosophy, Associate
Professor.

INTERNATIONAL COOPERATION TO FIGHTING AGAINST CRIMES IN VIRTUAL SPACE

Аннотация. Мақолада кибержиноятлар замонавий жамият хавфсизлигига янги таҳдид сифатида қаралиб, виртуал оламда жиноятлар даражасининг ошиб бориши сабаблари таҳлил қилинган, кибержиноятларга қарши курашиш жараёнида мавжуд муаммолар, хусусан, етарли даражада мутахассисларнинг йўқлиги, кибержиноятларга қарши курашиш учун қонунчилик базасининг етарлича эмаслиги, жабрланувчилар кибержиноят ҳолатлари аниқланганда у ҳақида хабар беришни истамаслиги оқибатида бу жиноятнинг латенлик даражаси юқорилиги ва шу каби муаммолар кўриб чиқилган. Кибержиноятчиликка қарши курашда фан ва техниканинг замонавий ютуқларидан фойдаланган ҳолда янгича ёндашувлар белгиланиши таъкидланган. Мақолада қайд этилишича, хусусий секторда ҳам, давлат секторида ҳам киберхужумлар ҳолатларининг ортиб бораётгани фойдаланувчиларнинг интернет маконида мавжуд хавфсизлик қоидаларини билмасликлари, шунингдек, хорижий мамлакатларда содир этилган кибержиноятларда жиноятчининг шахсини аниқлаш каби қийинчиликлар алоҳида ташвиш уйғотади. Шунини таъкидлаш керакки, кибержиноятчилик ўсишининг сабабларидан бири бу кибержиноятчиликка қарши кураш бўйича халқаро ҳамкорлик керакли даражада эмаслиги, кўплаб

davlatlar ushbu turdagi xavf-xatarни тўлиқ англаб етишдан узоқлигидадир ва бу турдаги жиноятлар нафақат жисмоний ёки юридик шахсларга, балки бутун давлатга зарар етказиши мумкинлигидадир. Бир томондан, ноқонуний хуфиёна бизнеснинг ривожланиши, солиқ тўлашдан бўйин товланиши, жиноятдан олинган даромадларнинг ноқонуний легаллаштирилиши, тадбиркорлар ва, умуман, хусусий секторнинг молиявий аҳволининг ёмонлашуви кўринишида мамлакатларнинг иқтисодиётига катта зарар етказилиши мумкин. Бошқа томондан, аҳолининг давлатга, технологияга ёки банк муассасаларига ишончи йўқолмоқда. Киберхужумни содир этган шахсларнинг шахсини аниқлаш ва зарурий далиллар базасини топишнинг имкони йўқлиги ёки қийинлиги, жазо муқаррарлигини таъминлашнинг иложи йўқлиги сабабли фош этилмаган кибержиноятлар сони ортиб бормоқда. Ҳуқуқни муҳофаза қилувчи идоралар ходимлари учун кибержиноятчиликка қарши курашиш устувор вазифалардан бири бўлиб белгиланган, чунки жиноят қурбонлари етказилган моддий зарарни қоплаш ва айбдор шахсларни жиноий жавобгарликка тортишни таъминлашни сўраб ҳуқуқни муҳофаза қилувчи органларга мурожаат қилишади. Мавжуд муаммоларни ҳал қилиш учун IT-соҳасида зарур кўникмаларни шакллантириш мақсадида мутахассисларнинг малакасини ошириб бориш, шунингдек, хакерларнинг жойлашган манзилини аниқлаш, уларни ушлаш ва олиб келиш имконини берувчи янги моддий-техник базани жорий этиш таклиф этилган. Ягона халқаро ҳужжат, шунингдек, давлатлар ўртасида имзоланган икки ва уч томонлама шартномаларнинг мавжуд эмаслиги сабабли давлатлар ҳуқуқни муҳофаза қилиш органларининг етарли даражада ўзаро ҳамкорлиги йўқлиги глобал муаммолардан бири ҳисобланади, бу муаммонинг ечими сифатида ягона халқаро ҳужжат – БМТ негизида “Кибержиноятчиликка қарши кураш тўғрисида”ги конвенцияни ишлаб чиқиш таклифи илгари сурилган.

Калит сўзлар: кибержиноят, виртуал макон, халқаро, ҳамкорлик, конвенция.

Аннотация. в статье киберпреступность рассматривается как новая угроза безопасности современного общества, анализируются причины роста уровня преступлений в виртуальном пространстве, а также изучены проблемы, возникающие в ходе противодействия киберпреступлениям, которые связаны с недостаточной подготовкой специалистов, неполноценности законодательной базы для борьбы с киберпреступлениями, увеличением уровня латентности киберпреступлений ввиду нежелания потерпевших сообщать о преступлениях. Определяются новые подходы с использованием современных достижений науки и техники в борьбе с киберпреступлениями. В статье отмечается, что особую обеспокоенность вызывают учащающиеся случаи кибератак как в частном, так и в

государственном секторе в связи с незнанием пользователями о существующих правилах безопасности в интернет-пространстве, а также трудности с обнаружением и установлением личности киберпреступников на территории зарубежных государств. Следует отметить, что одной из причин увеличения роста киберпреступлений является тот факт, что международное сотрудничество в борьбе с киберпреступностью находится не на должном уровне, многие государства далеко не осознают всю степень опасности данных видов преступлений, которые наносят ущерб не только физическим или юридическим лицам, но и государству в целом. С одной стороны, огромный ущерб, который наносится экономике стран в виде развития нелегального теневого бизнеса, сокрытия налогов, незаконной легализации доходов, добытых преступным путем, ухудшение финансового положения предпринимателей и частного сектора в целом. С другой стороны, утрачивается доверие общественности к государству, технологиям или банковским учреждениям. Наблюдается увеличение количества нераскрытых киберпреступлений ввиду невозможности или трудности установления личности злоумышленников, обнаружения необходимой доказательственной базы, невозможности обеспечения неотвратимости наказания. Для сотрудников правоохранительных органов борьба с киберпреступностью является одной из приоритетных задач, так как все больше жертв преступлений обращаются в правоохранительные органы с просьбой обеспечить возмещение материального ущерба или обеспечить привлечение лиц к уголовной ответственности. Для решения существующих проблем предложено повышать квалификацию специалистов для получения необходимых навыков и умений в IT сфере, а также внедрение новой материально-технической базы, позволяющей установить местоположение хакеров, а также задержать их и привлечь к установленной ответственности. В качестве решения одной из глобальных проблем, заключающейся в недостаточном взаимодействии между правоохранительными органами государств ввиду отсутствия единого международного документа, а также подписанных двусторонних и трехсторонних договоров между странами, предлагается создать единый международный документ – Конвенцию «О противодействии киберпреступности» на базе ООН.

Ключевые слова: киберпреступность, виртуальное пространство, международный, сотрудничество, конвенция.

Annotation. the article examines cybercrime as a new threat to the security of modern society, analyzes the reasons for the increase in the level of crimes in the virtual space, and also examines the problems arising in the course of countering cybercrime associated with insufficient training of specialists, insufficient legislative framework to combat cybercrime, an increase in the level of latency of cybercrime due to the unwillingness of victims to report crimes. New approaches using modern achievements of science and technology in the fight against cybercrime have been

identified. The article notes that of particular concern are the frequent cases of cyber-attacks in both the private and public sectors due to the ignorance of users of the existing security rules in the Internet space, as well as difficulties in detecting and identifying cybercriminals on the territory of foreign states. It should be noted that one of the reasons for the increase in the growth of cybercrime is the fact that international cooperation in the fight against cybercrime is not at the proper level, many states are far from realizing the full extent of the danger of these types of crimes, which harm not only individuals or legal entities, but also the state as a whole. On the one hand, there is a huge damage caused to the economies of countries in the form of the development of illegal shadow business, tax concealment, illegal legalization of proceeds from crime, deterioration of the financial situation of entrepreneurs and the private sector. On the other hand, public confidence in the state, technology or banking institutions is being lost. There is an increase in the number of unsolved cybercrimes due to the impossibility or difficulty of identifying attackers, finding the necessary evidence base and the impossibility of ensuring the inevitability of punishment. For law enforcement officers, the fight against cybercrime is one of the priorities, since more and more victims of crimes are turning to law enforcement agencies with a request to provide compensation for material damage or to ensure that persons are brought to criminal responsibility. To solve the existing problems, it is proposed to improve the skills of specialists to obtain the necessary skills and abilities in the IT-sphere, as well as the introduction of a new material and technical base that allows you to locate hackers, as well as detain them and bring them to the established responsibility. As a solution to one of the global problems, which lies in the insufficient interaction of law enforcement agencies of states due to the lack of a unique international document, as well as signed bilateral and trilateral agreements between the countries, it is proposed to create a unique international document – the Convention “On Countering Cybercrime” at the UNO base.

Key words: *cybercrime, virtual space, international, cooperation, convention.*

1.1. Актуальность исследования. Проблемы касательно темы исследования

Совершенствование и бурное развитие информационных процессов в различных областях человеческой деятельности стало причиной стремительного формирования информационных технологий, по мере развития которых в условиях всеобщей компьютеризации возник вопрос защиты информации и компьютерной безопасности. Как отмечает, А.К. Расулев, одним из основных направлений повышения результативности борьбы с киберпреступностью является совершенствование соответствующих законодательных актов, то есть создание правовой основы для действенного прекращения и уголовного преследования преступлений в данной сфере. И изучение опыта борьбы и законодательства зарубежных стран в данной области может способствовать усовершенствованию национального законодательства.

Компьютеризация привела к качественному и количественному изменению всех сфер общества, следовательно к преобразованию и сферы деятельности преступников. На сегодняшний день одними из самых распространенных видов преступлений являются преступления в виртуальном пространстве или киберпреступления. Согласно статистическим данным, 4,66 миллиарда человек по состоянию на 2020 год пользуются возможностями Интернета, данный показатель был ниже более чем в 3 раза по сравнению с 2008 годом, причиной чему явилась доступность Интернета. 62,5% мирового населения используют интернет – число пользователей за 2021 год увеличилось на 192 млн (4%) и составляет 4,95 млрд человек. А в январе 2022 года в мире насчитывалось 4,62 миллиарда пользователей социальных сетей.

По статистике ежегодный глобальный ущерб от киберпреступности оценивается в 10,5 триллиона долларов к 2025 году. Согласно проведенным научным исследованиям в период с 2019 г. по 2023 г. ожидается нанесение частным компаниям ущерба в размере 5,2 триллионов долларов США.

Статистические данные подтверждают тот факт, что киберпреступления являются одними из самых разрушительных для экономики стран видов преступной деятельности, к тому же помимо имущественного ущерба, они подрывают доверие народа к технологиям и государству в целом, несут угрозу миру и безопасности человечества.

Но что означает само слово киберпреступность? Оксфордский толковый словарь определяет приставку «cyber-» как – «относящийся к информационным технологиям, сети Интернет, виртуальной реальности». Кембриджский словарь определяет приставку «cyber-» как – «включающий в себя использование компьютеров или относящийся к компьютерам, особенно к сети Интернет».

По мнению экспертов ООН, термин «киберпреступность» охватывает любое преступление, которое может совершаться с помощью компьютерной системы или сети, в рамках компьютерной системы или сети, или против компьютерной системы или сети.

Карпова Д.Н. определяет киберпреступление как «акт социальной девиации с целью нанесения экономического, политического, морального, идеологического, культурного и других видов ущерба индивиду, организации или государству посредством любого технического средства с доступом в Интернет».

По мнению Зигмунта О.А., Петровского А.В. «под кибер- и интернет-преступностью мы понимаем совокупность совершенных на определенной территории за определенный промежуток времени преступных деяний, предметом которых выступают компьютерные сети, компьютерное программное обеспечение, носители компьютерной информации, сетевая информация, а средством совершения являются компьютерная техника либо компьютерные, электронно-информационные технологии».

По нашему мнению, под киберпреступностью необходимо понимать любые противоправные, виновные деяния, совершенные с использованием информационно-коммуникационных технологий, устройств, сети или программ обеспечения.

1.2. Пути решения проблемы

Несмотря на то, что киберпреступления появились к концу 20 века, они становится большой проблемой во всем мире, поэтому многие страны приступают к принятию законов и других регламентирующих механизмов в попытке свести к минимуму число случаев киберпреступности. Каждая страна борется с данным социально опасным явлением по-разному, исходя из норм национального законодательства, менталитета и уровня угрозы национальной безопасности. Речь идет о национальных законодательных актах по борьбе с киберпреступностью, нормативно-правовых документах по защите личных данных, а также государственных секретов.

Акцентируем внимание на сравнительно-правовом анализе уголовных законодательств некоторых зарубежных государств в сфере противодействия киберпреступлениям. К примеру, в Дании в 2018 году был принят Датский Закон о защите данных; в Фиджи в «Декрет о преступлениях» от 2009 года включен раздел «Компьютерные преступления», в Объединенных Арабских Эмиратах имеется Федеральный Закон «Об электронной торговле и транзакциях», а в Великобритании еще в 1990 году был принят Закон «О неправомерном использовании компьютеров», а в 2018 году Закон «О защите данных». Каждая страна совершенствует национальное законодательство для эффективной борьбы с киберпреступностью для искоренения данных видов преступлений.

Помимо этого, вышеуказанных мер, многие страны создают специальные управления по вопросам кибербезопасности и борьбе с киберпреступлениями. Перечислим некоторые из них, к примеру, Совет по кибербезопасности в Исландии, Федеральное управление по информационной безопасности в ФРГ, Управление Кибербезопасности и обеспечения информации в Великобритании, Министерство науки, информационно-коммуникационных технологий и планирования будущего в Республике Корея, а также Министерство информационных технологий и связи в Колумбии, в функциональные обязанности которых включены вопросы обеспечения как кибербезопасности, так и вопросы оказания противодействия кибератакам.

Стоит отметить, что в Узбекистане также существует Государственное унитарное предприятие «Центр кибербезопасности», одной из задач которого является «обеспечение защиты от потенциальных кибератак и бесперебойного функционирования объектов информатизации Республики Узбекистан, централизованное внедрение инструментов для обнаружения, предупреждения уязвимостей и угроз информационной и кибербезопасности, участие в обнаружении,

предупреждения и ликвидации последствий компьютерных атак, осуществление методического обеспечения по вопросам защиты от компьютерных атак и реагирования на компьютерные инциденты» и т.д.

Учитывая, что эффективные меры по борьбе с киберпреступностью касаются также и повышения уровня осведомленности, образования и обучения в области кибербезопасности, некоторые страны проводят компании по повышению осведомленности общественности, а также финансируют научные исследования в сфере кибербезопасности. Так, власти Австралии проводят профилактические и разъяснительные работы с населением и проводят компании типа Stay Smart Online, предоставляя необходимую информацию в доступной форме по существующим видам киберпреступлений, защите себя и своих данных от киберпреступников. Также пользователи могут в электронной форме оперативно сообщить об инцидентах киберпреступлений в онлайн форме.

На 74-й сессии ООН, страны-члены ООН в своих докладах акцентировали внимание на имеющихся в их странах, проблемах противодействия киберпреступности в виде отсутствия четкой структуры международно-правовой базы борьбы с киберпреступностью, что не позволяет скоординировать и объединить совместные усилия государств. Причиной кроется в отсутствии единого международного документа по противодействию киберпреступности. Первым международным документом по борьбе с киберпреступностью «Конвенция о компьютерных преступлениях» от 2001 года, которую подписали и ратифицировали помимо стран-членов ЕС, также США, Япония, Австралия и Израиль. Хотя говорить об эффективности сотрудничества по борьбе с киберпреступностью исходя из того, что данный документ подписали только 53 стран, нельзя. Учитывая, что большая часть кибератак происходит из стран, которые данную конвенцию не подписали, такие как Китай, РФ, страны Латинской Америки, Африки. Иначе говоря, без всестороннего сотрудничества нельзя рассчитывать на эффективность приложенных усилий.

Среди стран СНГ также было подписано в 2001 году Соглашение Содружества Независимых Государств «О сотрудничестве в борьбе с преступлениями, связанными с компьютерной информацией», однако учитывая, что сотрудничество осуществляется только на основании возбужденного уголовного дела и для направления одного запроса уходит около месяца говорить об оперативности и эффективности данного сотрудничества не приходится.

1.3. Научно обоснованные предложения и рекомендации

Исходя из вышеизложенного, можно прийти к выводу, что, несмотря на предпринимаемые каждым государством мерами по борьбе с киберпреступностью, однако без принятия международных конвенций, разработки единого эффективного механизма по оперативному

разрешению вопросов, связанных с установлением инцидентов кибератак и лиц, совершивших преступление, а также с регламентацией основ и стратегических направлений реальных действий по совершенствованию законодательства по обеспечению кибербезопасности, нельзя миновать увеличения количества киберпреступлений. В связи с этим, предлагается внести предложения о разработке единой международной Конвенции «О противодействии киберпреступлениям» на базе ООН.

Кроме того, для эффективного противодействия киберпреступности необходимо, чтобы все принятые в данной сфере международные нормативно-правовые документы (Конвенции, декларации) носили не исключительно рекомендательный характер, а использовались при разработке законодательных актов и имплементировались в практическую деятельность органов, обеспечивающих борьбу с киберпреступностью. Для эффективной борьбы с киберпреступностью необходимо международное сотрудничество и совершенствование международного законодательства всеми странами мира, а также проведение профилактических работ, чтобы отдельные пользователи и компании понимали, в чем состоит опасность, и имели достаточные знания и инструментарий, чтобы свести к минимуму риск стать жертвой киберпреступников.

БИБЛИОГРАФИЧЕСКИЕ ССЫЛКИ:

1. А.К. Расулев. Уголовно-правовой анализ норм национального и зарубежного законодательства, обеспечивающих информационную безопасность в сети Интернет. Ҳуқуқий тадқиқотлар журнали / Журнал Правовых исследований / Journal of Law Research. 2018, № 5. – С. 33–41.

2. <https://vc.ru/u/937816-raddy/361755-obzor-otcheta-global-digital-2022-internet-socseti-chto-bylo-i-chto-budet-po-prognozam>

3. www.websiterating.com

4. Lewis, James Andrew, “Economic Impact of Cybercrime”, Center for Strategic & International Studies (CSIS), 21 February 2018, <https://www.csis.org/analysis/economic-impact-cybercrime>

5. <https://www.oxfordlearnersdictionaries.com/definition/english/cyber>.

6. <https://dictionary.cambridge.org/dictionary/learner-english/cyber>.

7. Доклад X Конгресса ООН по предупреждению преступности и обращению с правонарушителями // Десятый Конгресс ООН по предупреждению преступности и обращению с правонарушителями. [Электронный ресурс] – URL: http://www.un.org/ru/documents/decl_conv/declarations/crime91.shtml.

8. Карпова Д.Н. Киберпреступность: глобальная проблема и её решение. Власть. 2014. – №8. – С. 47.

9. Зигмунт О.А., Петровский А.В. Кибер- и интернет-преступность в Германии и России: возможности сравнительного исследования. Юридическая наука и правоохранительная практика №4 (34). 2015. – С. 181.

10. Черкасов Д.Ю., Иванов В.В., Лубова Е.С. Киберпреступность в современном мире. – Москва, 2016. – С. 87. <https://cyberleninka.ru/article/n/kiberprestupnost-v-sovremennom-mire>.

11. <http://infocom.uz/2020/12/11/kiberbezopasnost-kak-trebovanie-vremeni/>.

12. Конвенция о компьютерных преступлениях. Будапешт, 23 ноября 2001 года.

13. Расулев, Абдулазиз, and Сурайё Рахмонова. «Преступления в сфере информационных технологий и безопасности: детерминанты и предупреждение». Общество и инновации 1.1 (2020): 200–209.

14. Расулев А.К. «Повышение качества и результативности юридического образования и науки». Фан ва таълим замонавий босқичда: ислохотлар ва стратегик йўналишлар: 16-23.