МРНТИ:10.81.71 *DOI 10.51889/4749.2022.28.19.012*
УДК: 343.3/.7

Сералиева А.М.[1]
[1]Казахский национальный педагогический университет имени Абая

КИБЕРПРЕСТУПНОСТЬ: ПОНЯТИЕ, ПРИЧИНЫ И ПРЕДУПРЕЖДЕНИЕ

Аннотация

В настоящее время в различных сферах жизни общества внедрены коммуникационные и информационные технологии. Они быстрыми темпами совершенствуются.

Активное и повсеместное внедрение информационных технологий привело к изменению перечня экономических преступлений. К таким противозаконным действиям относятся компьютерные преступления, причиняющие вред экономике государства, ее отдельным секторам, предпринимательской деятельности и экономическим интересам отдельных групп граждан.

На сегодняшний день жертвами преступников, орудующих в виртуальном пространстве, могут стать не только отдельные люди, но и целые государства. Безопасность тысяч пользователей может оказаться в руках нескольких преступников. Количество преступлений, совершаемых в киберпространстве, растёт пропорционально числу пользователей компьютерных сетей, и темпы роста преступности в глобальной сети Интернет являются самыми быстрыми на планете.

В статье раскрываются понятие, причины и предупреждение киберпреступности в Республике Казахстан. Приведены различные взгляды на происхождение кибер-преступности.

Ключевые слова: глобализация, киберпреступность, информационные преступления, интернет, кибератаки, компьютерные преступления, киберпространство кибертерроризм.

А.М. Сералиева[1]
[1]Абай атындағы Қазақ ұлттық педагогикалық университеті

КИБЕРҚЫЛМЫС: ТҮСІНІГІ, СЕБЕПТЕРІ ЖӘНЕ АЛДЫН-АЛУ ЖОЛДАРЫ

Аңдатпа

Қазіргі уақытта қоғамдық өмірдің түрлі салаларында коммуникациялық және ақпараттық технологиялар енгізілді. Олар жылдам қарқынмен дамуда.

Ақпараттық технологияларды белсенді және кеңінен енгізу экономикалық қылмыстардың тізімінің өзгеруіне әкелді. Мұндай заңсыз әрекеттерге компьютерлік қылмыстар жатады және де мемлекет экономикасына, оның жекелеген секторларына, кәсіпкерлік қызметке және азаматтардың жекелеген топтарының экономикалық мүдделеріне зиян келтіреді .

Бүгінгі таңда виртуалды кеңістіктегі қылмыскерлердің құрбандары тек жеке адамдар ғана емес, мемлекеттер де бола алады. Мыңдаған пайдаланушылардың қауіпсіздігі бірнеше қылмыскерлердің қолында болуы мүмкін. Киберкеңістікте жасалатын қылмыстардың саны компьютерлік желілерді пайдаланушылар санына пропорционалды түрде өсуде және ғаламдық Интернет желісіндегі қылмыстың өсу қарқыны планетадағы ең жылдам болып табылады.

Мақалада Қазақстан Республикасындағы киберқылмыстың түсінігі, себептері және алдын алу ашылады. Киберқылмыстың пайда болуы туралы әртүрлі көзқарастар келтірілген.

Түйін сөздер: жаһандану, киберқылмыс, ақпараттық қылмыстар, интернет, кибершабуылдар, компьютерлік қылмыстар, киберкеңістік кибертерроризм.

Seraliyeva Aliya[1]
[1]Abai Kazakh National Pedagogical University

CYBERCRIME: CONCEPT, CAUSES AND WARNING

Abstract

At the present time, communication and information technologies have been introduced in various spheres of society. They are improving rapidly.

The active and widespread introduction of information technology has caused a change in the list of economic crimes. Such unlawful actions include computer crimes that cause harm the economy of the state, its individual sectors, business activities, and the economic interests of certain groups of citizens.

Today, not just individuals but also entire states can become victims of criminals operating in the virtual space. The security of thousands of users could end up in the hands of a few criminals. The number of crimes committed in cyberspace is growing in proportion to the number of users of computer networks, and the growth rate of crime on the global Internet is the fastest on the planet.

The article reveals the concept, causes, and prevention of cybercrime in the Republic of Kazakhstan. Various views on the origin of cybercrime are provided.

Keywords: globalization, cybercrime, information crimes, Internet, cyber-attacks, computer crimes, cyberspace cyberterrorism.

Введение

Процессы глобализации, в том числе глобализация информационных технологий, открывают неограниченные возможности воздействия на личность и общество. Одним из негативных последствий развития информационных технологий является появление и развитие новой формы преступности – высокотехнологичной преступности, когда объектом преступного посягательства, а также средством или способом совершения преступления выступают компьютеры или информационные сети. Проблема киберпреступности актуализировалась в эпоху информационного общества, когда компьютеры и телекоммуникационные системы охватили все сферы жизни человека и государства, а глобальный Интернет является одним из самых быстрых для развития телекоммуникацион-ных технологий.

Возрастающий профессионализм киберпреступников и постоянное совершенство-вание информационных технологий, а, следовательно, и постоянная эволюция возможностей для совершения преступлений, создают новые угрозы для пользователей глобальных информационных сетей [1, с.45].

Проблема использования достижений науки и техники в преступных целях связана с одним из важнейших направлений интеграционных процессов: созданием, по своей сути, международной и глобальной по форме сети Интернет, объединившей миллионы компью-теров, расположенных в разных уголках земли. Всемирная паутина, открывшая широчайшие возможности для получения информации и обмена ею, развивается очень быстрыми темпами.

Научная статья актуальна, определяется несовершенством законодательства, в рассматриваемой сфере уголовных и международных отношений, а также необходимостью исследования института киберпреступности в Республики Казахстан.

Материалы и методы

Теоретическую и нормативную основу исследования составили труды отечественных и зарубежных авторов по уголовному праву и криминологии, информатики, психологии,

международное и национальное законодательство, относящиеся к рассматриваемой проблеме киберпреступности. В процессе исследования применялись такие научные методы, как: историко-правовой, сравнительный, статистический и метод системного анализа.

Результаты и обсуждение

Большинство преступлений, совершаемых в глобальных компьютерных сетях, характеризуются следующими характеристиками:

1) Повышенная скрытность совершения преступления, обусловленная спецификой информационного пространства сети (развитые механизмы анонимности, сложность инфраструктуры и т. п.).

2) Трансграничный характер сетевых преступлений, при которых преступник, объект преступной узурпации, потерпевший могут находиться на территориях разных государств.

3) Специальная подготовка преступников, интеллектуальный характер преступной деятельности.

4) Нестандартность, сложность, разнообразие и частое обновление способов совершения преступлений и используемых специальных средств.

5) Возможность совершения преступления в автоматизированном режиме в нескольких местах одновременно. Возможность объединить относительно слабые ресурсы множества отдельных компьютеров в мощный инструмент для совершения преступления.

6) Многоэпизодность преступных деяний с множественностью потерпевших.

7) Неосведомленность потерпевших о том, что они подверглись преступному влиянию.

8) Дистанционный характер преступных действий при отсутствии физического контакта между виновным и потерпевшим.

9) Невозможность предупреждения и пресечения преступлений данного вида традиционными средствами [2].

В отечественных и зарубежных научных кругах преступления, совершаемые в компьютерных и телекоммуникационных системах, именуются по-разному: компьютерные преступления [3; 4], высокотехнологичные преступления [5], киберпреступления [6], преступления в области компьютерной безопасности [7; 8], компьютерные преступления в сфере информации [9] и т. д.

Существующий разброс мнений в определении рассматриваемого понятия, по-видимому, связан с отсутствием единого подхода в научных исследованиях, посвященных изучению киберпреступности и теоретических аспектов правонарушений данной категории.

Многообразие существующих подходов к пониманию рассматриваемого явления проанализировано В.А. Дуленко, Р. Р. Мамлеевым и В. А. Пестриковым, которые считают, что киберпреступностью в широком смысле является любое противоправное деяние, совершаемое с помощью вычислительных устройств или в связи с ними, в том числе такие преступления, как незаконное хранение, предложение или распространение информации с использованием компьютерных технологий [10]. В целом киберпреступность, по сообщениям преступников, связывается с правонарушениями, совершенными в различных информационных сетях.

В позиции И. М. Рассолова к киберпреступлениям относятся общественно-опасные деяния, совершаемые с использованием средств вычислительной техники в отношении информации, обрабатываемой и используемой в сети Интернет [11]. Нельзя не заметить, что суждения, выносимые по существу дела, имеют очень узкую направленность.

Международное право также выступает против проведения различия между концептуальными единицами «киберпреступность» и «компьютерная преступность» и предпочтения отдается первой. Впервые «Конвенция о киберпреступлениях», принятая Советом Европы 23 ноября 2001 года, классифицировала киберпреступность, и определила термин «киберпреступность», а не «компьютерная преступность». Конвенция о

киберпреступности представляет собой комплексный документ, содержащий нормы, призванные оказать существенное влияние на различные отрасли права: уголовное, уголовно-процессуальное, авторское, гражданское, информационное. Она базируется на основных принципах международного права: уважения прав человека, сотрудничества и добросовестного выполнения обязательств [12, с.17].

Термин «киберпреступность» в настоящее время часто используется в сочетании с термином «компьютерная преступность», и часто эти термины используются как синонимы. В литературе наибольшее предпочтение отдается термину «компьютерная преступность». Возможно, это потому, что большинство исследований проводится на криминалистическом или процессуальном уровне. Кроме того, глава 7 УК РК «Уголовные правонарушения в сфере информационной связи», предусматривает ответственность за правонарушения, объектом которых является информация и информационные системы [13].

На самом деле эти термины очень близки друг к другу, но еще не являются синонимами. На наш взгляд, понятие «киберпреступность» (в англоязычном варианте – cybercrime) шире, чем «компьютерная преступность» (computercrime) и более точно отражает сущность такого явления, как преступность в информационном пространстве. Так, Оксфордский словарь определяет приставку «cyber-» как составную часть сложного слова. Его значение «относится к информационным технологиям, Интернету, виртуальной реальности» [2].

Почти такое же определение дает Кембриджский словарь: префикс «cyber-» означает «связанный с использованием компьютеров или относящийся к компьютерам, особенно к сети-Интернет». При этом в качестве примера Кембриджский словарь приводит слово «cybercrime» - киберпреступность (киберпреступление) [14].

Таким образом, «киберпреступность» – это преступление, связанное как с использованием компьютеров, так и с использованием информационных технологий и глобальных сетей. При этом термин «компьютерное преступление» относится только к преступлениям, совершенным против компьютеров или компьютерных данных. Глобальное информационное пространство, мегаинформационная среда нематериальны и принципиально несводимы к физической среде, в которой они воплощены.

Компьютерное преступление – это преступление, посягающее на безопасное функционирование компьютеров и компьютерных сетей, а также данных, которые они обрабатывают. Таким образом, компьютерная преступность является разновидностью киберпреступности [15].

Необходимо выделить следующие факторы, влияющие на рост числа киберпреступлений.

1. Глобальная компьютеризация всех сфер общества не повышает, а снижает степень его защищенности.

2. Ускорение научно-технического прогресса увеличивает вероятность использования преступниками сугубо мирных технологий в качестве средств поражения, а возможность их «двойного» применения зачастую не только непреднамеренна, но и не осознана создателями техники.

3. Терроризм все больше становится особым видом информационных технологий, поскольку, во-первых, террористы все больше используют возможности современных информационно-телекоммуникационных систем в целях связи и разведки; во-вторых, сегодня реальностью становится так называемый «кибертерроризм»; в-третьих, определяющая часть террористических актов направлена на причинение материального ущерба и создание угрозы жизни и здоровью людей, а также на информационно-психологическое потрясение, воздействие которых на большие массы людей создает благоприятную среду для достижения террористических целей [1].

Состояние киберпреступности в стране помогает нам выделить ряд текущих тенденций. Решающая доля случаев неправомерного доступа к компьютерной информации, которые на сегодняшний день составляют 19% от общего числа зафиксированных компьютерных

преступлений, или изготовление вредоносного программного обеспечения (8%), касается кражи денежных средств, незначительно преступлений, совершенных из хулиганских побуждений [3].

Еще одной проблемой является низкий уровень компьютерной грамотности населения, юридических лиц. Хакеры обманным путем, используя отсутствие знаний по обеспечению элементарной информационной безопасности, получают доступ к личной, коммерческой информации физических и юридических лиц, что становится инструментом вымогательства денежных средств. Государственными органами на недостаточном уровне проводится профилактическая работа по предупреждению преступлений в сфере информатизации и связи, не освещаются наиболее распространенные способы взлома средств безопасности компьютеров, смарт-телефонов и т. д., не пропагандируются элементарные способы обеспечения информационной безопасности.

В зависимости от объекта атаки выделяют следующие группы киберпреступлений: компьютерные преступления в сфере предпринимательства, компьютерные преступления против прав личности и неприкосновенности частной жизни, компьютерные преступления против общественных и государственных интересов [16].

Исходя из характера использования компьютеров или компьютерных систем, можно выделить три классификации киберпреступлений:

- деяния, при которых компьютеры являются объектом преступления (кража информации, несанкционированный доступ, уничтожение или повреждение файлов и устройств и т. д.);
- действия с использованием компьютеров в качестве орудий преступления (кража электронных средств и т. д.);
- преступления, в которых компьютеры играют роль интеллектуальных средств (например, размещение порносайтов в Интернете) [17, с.11].

По предмету криминального вмешательства преступления, совершаемые с использованием электронных средств и платежных систем, подразделяются на:

- На преступления против собственности (мошенничество, кража, вымогательство): Мошенничество, совершенное с использованием электронных платежных инструментов и систем; Воровство с помощью электронных средств и платежных систем.
- Преступления в сфере экономической деятельности (легализация незаконных доходов, незаконное предпринимательство): легализация доходов, полученных незаконным путем от электронных платежных средств и систем; незаконная торговля.
- Компьютерные информационные преступления: неправомерный доступ к компьютерной информации, являющейся информационным объектом электронных платежных систем.
- Создание, использование и распространение вредоносных программ, предназначенных для осуществления неправомерных действий в электронных платежных системах или с электронными платежными инструментами.
- Преступления против государственной власти, интересов государственной службы и службы в муниципалитетах (дача взятки с использованием электронных средств и платежных систем; получение взятки с использованием электронных средств и платежных систем) [18].

В 2007-2008 гг. экспертами Международного союза электросвязи с учётом новых деяний, появившихся в последние годы, также подготовлено несколько видов классификаций киберпреступлений, например, «Модельный закон» [19] ITU содержит, помимо традиционно известной классификации, предложенной Конвенцией Совета Европы, также такой вид преступления, как кибертерроризм – однако он отнесен к подвидам других правонарушений, например, «несанкционированный доступ» (неуполномоченный доступ для совершения террористических актов).

Кибератакам в мире подвергаются 12 тыс. человек ежесекундно, а ущерб от киберпреступлений составляет более 100 млрд долларов в год. [20].

Особое внимание, подтверждающее актуальность исследования данного вопроса, уделено в постановлении Правительства РК № 407 от 30 июня 2017 года об утверждеии Концепция кибербезопасности («Киберщит Казахстана») [20].

Правительством РК отмечено, что эффективная реализация мероприятий по цифровизации экономики будет обеспечена только при обеспечении единства, устойчивости и безопасности информационно-коммуникационной инфраструктуры, сохранности данных и доверии граждан к процессам, в основе которых лежат решения, основанные на использовании информационно-коммуникационных технологий Одним из этапов цифровизации, направленной на обеспечение надежной правовой среды и неукоснительной защиты прав и свобод граждан, интересов юридических лиц и государства является внедрение «электронного дела», состоящее из 5 связанных компонентов: электронные обращения граждан, единый реестр субъектов и объектов проверок, единый реестр административных производств, электронное уголовное дело, аналитический центр, а также судопроизводство в судебных стадиях процессам противодействие преступлениям, совершенным с применением информационных технологий [21].

Однако, согласно статистическим данным совершенных в сфере информатизации и связи (глава 7, ст.205-213 УК РК), из которых 50% (53) составляют преступления по ст.205 УК РК (неправомерный доступ к информации, в информационную систему или информационно-коммуникационную сеть), 20% – ст.206 (неправомерные уничтожение или модификация информации), 11 % – ст.210 (создание, использование или распространение вредоносных компьютерных программ и программных продуктов). В целом за последние три года наблюдается снижение количества зарегистрированных преступлений.

По мнению М. В. Старичкова, латентность неправомерного доступа к компьютерной информации (ст.272 УК РФ) и создание, использование и распространение вредоносных компьютерных программ (ст.273 УК РФ) составляет примерно 99,7 -99,8 % [22, с.109–112]. Аналогичного мнения придерживаются и отечественные ученые, оценивая их регистрацию на уровне 10 -15% от количества совершенных [23, с.19]. Основными причинами высокой латентности являются отсутствие должной реакции со стороны жертв преступлений, а также скрытый характер с использованием компьютерных технологий [24, с.67].

Отсюда, в Республике Казахстан законодательство в области киберпространства находится лишь на стадии становления. Данное положение обусловлено тем, что широкое применение информационных технологий в Казахстане и соответственно увеличение количества с ними связанных правонарушений возникли сравнительно недавно.

В октябре 2017 года был утвержден План мероприятий по реализации Концепции кибербезопасности, в рамках которого усовершенствованы и законодательно закреплены нормы сферы информационной безопасности.

Кроме того, в отраслевой закон внесено понятие «киберстрахование», которое позволяет возмещать имущественный вред организации, причиненный в результате компьютерных инцидентов, а также моральный вред физлицу, причиненный в результате утечки данных.

В стране также был определен уполномоченный орган в сфере защиты персональных данных – Комитет по информационной безопасности МЦРИАП РК.

В 2020 г. утверждены правила сбора и обработки персональных данных, которыми определен порядок и требования к обращению с персональными данными от стадии сбора до стадии их уничтожения.

В 2020 г. начата правоприменительная практика по привлечению к ответственности за нарушение требований по защите персональных данных на ЭИР (проверка в отношении оператора связи, субъектов частного предпринимательства) и законодательства об электронном документе и ЭЦП.

Начиная с 2018 года для апробации механизмов реагирования на киберугрозы в рамках Национального антикризисного плана реагирования на инциденты информационной безопасности, проводятся командно-штабные учения с участием представителей заинтересованных государственных органов.

В 2018 г. Комитетом национальной безопасности Республики Казахстан был создан и начал работу Национальный координационный центр информационной безопасности (НКЦИБ), обеспечивающий защиту информационных ресурсов государственных органов и критически важной информационной инфраструктуры от кибератак и киберинцидентов [25].

Все это подтверждает актуальность усиления борьбы с киберпреступлениями и необходимость международного сотрудничества в данной сфере с целью обеспечения безопасности и правопорядка. Международному сотрудничеству в сфере уголовного судопроизводства посвящен раздел 12 (ст. 557 -611) в УПК РК. Также источниками международного сотрудничества, помимо УПК РК, являются международные договоры Казахстана с другими государствами и принцип взаимности.

Заключение

Таким образом, считаю, что противодействие киберпреступности должно быть возведено в ранг первоочередных задач правоохранительных органов, эффективности которой будут способствовать следующие факторы:

– в Республике Казахстан процесс формирования законодательства в сфере противодействия киберпреступлениям должен основываться на следующих основных принципах: международное сотрудничество; приоритет профилактики киберпреступлений; использование международного опыта для прогнозирования появления новых преступлений; взаимодействие законодателя со специалистами в области информационной безопасности для формирования актуальной правовой базы. Указанные принципы должны быть выделены не только в теории права, но и закреплены законодательно, что создаст фундамент для принятия актуальных нормативных правовых актов;

– необходимо организовать подразделения по борьбе с киберпреступностью, включающие в себя следственные и оперативные группы, функционирующие круглосуточно - 24/7, согласно рекомендациям Европейской конвенции о киберпреступности от 23.11.2001 г. Введение в следственные подразделения органов уголовного преследования групп, специализирующихся на противодействии киберпреступлениям, обеспечит квалифицированное расследование преступлений данной категории. На перспективу – объединение оперативных и следственных служб с определением четкой вертикальной подчиненности и специализации, в т.ч. по противодействию киберпреступности (существующая система сбора материалов подразделениями МВД РК, последующее процессуальное их закрепление следователями, находящимися в иной организационной структуре, не обладающими специальными познаниями в сфере информационных технологий, не отвечает современным требованиям борьбы с данными видами преступлений);

– полагаю возможным использовать положительный опыт зарубежных стран, привлекающих на должности оперативных работников и специалистов - лиц, имеющих, как правило, техническое образование, с прохождением курсов юридической подготовки;

– исходя из официальных данных, мы видим, что несмотря на усилия, которые предпринимаются государством в области борьбы с преступлениями, совершаемые посредством информационно-телекоммуникационных технологий, результаты таких мер являются не столь действенными. В связи с этим, считаю, что, основными мерами по предупреждению указанных видов преступлений должны стать средства массовой информации, а также сами граждане страны. Например, в ряды познавательных передач еженедельно можно включать программы, которые на примере обманутых граждан покажут способы и лазейки мошеннических комбинаций, которыми пользуются злоумышленники.

Также указанный способ предупреждения относится и к рекламе на ТВ-каналах, распространяется на бумажные баннеры, расположенные на транспортных остановках. Имеет место упоминание о наиболее частых способах мошеннических действий в колонках газет, такой факт обусловлен тем, что среди жертв от мошеннических действий немало граждан пенсионного возраста, которые отдают предпочтение именно бумажным источникам информации. Кроме того, следует проводить работу с сотрудниками банков, призывать их обращать внимание на странные действия и операции, совершаемые гражданами, а также интересоваться у лиц, вызвавших подозрение, целью операции. Сами граждане также могут оказывать содействие в предупреждении преступлений в информационно-телекоммуникационной сфере. Например, в кругу семьи и знакомых следует обсуждать случаи, связанные с хищением денежных средств, которые произошли с рассказчиком;

– также одной из мер предупреждения может являться введение дополнительных способов засекречивания персональных данных граждан, а также многослойные способы аутентификации. Например, перед тем как перевести значительную сумму денег, целесообразно задавать вопросы, которые могут заставить гражданина усомниться в правильности выполняемых им действий. Кроме того, если гражданин часто пользуется банковскими картами, производит по ним операции, то ему следует знать и помнить о простых правилах их использования. Не всем известно, что снять деньги с банковской карты куда проще, чем с банковского счета, поскольку для списания денежных средств требуется очное участие в процедуре списания или перевода владельца данного счета;

– еще одной профилактической мерой по сохранению безопасности денежных средств от нежелательных потерь является система компьютерной безопасности – антивирусы, среди наиболее популярных и качественных, разработчики в сфере IT-технологий выделяют Kaspersky Total Security, Bitdefender Antivirus Free Edition;

– если говорить о способах защиты от последствий кибермошенничества, то существует несколько методов защиты компьютеров от информационных преступлений и атак, соблюдение которых не допускает возникновения и проникновения заразных вирусов в компьютерные сети:

а) Постоянное обновление программного обеспечения и операционной системы, которое гарантирует, что для защиты компьютера используются новейшие исправления безопасности;

б) Использование антивируса или комплексного решения для обеспечения интернет-безопасности;

в) Использование сильных паролей, которые трудно подобрать. Также рекомендуется нигде их не записывать. Можно воспользоваться услугой надежного менеджера паролей, который облегчит задачу, предложив сгенерированный им сильный пароль;

г) классический способ заражения компьютеров с помощью вредоносных атак и других типов киберпреступлений – это вложения в электронных спам-сообщениях. Не следует открывать вложение от неизвестного отправител;

д) вредоносные ссылки в спамовых электронных письмах, а также на незнакомых веб-сайтах. Не следует переходить по этим ссылкам, чтобы не стать жертвой интернет-мошенников;

е) не передавать личные данные по телефону или по электронной почте, если нет уверенности, что телефонное соединение или электронная почта защищены.

– Предлагаем ввести «*кибертеракт*» в УК РК, как квалифицированный состав в п.2 ст. 255. Это необходимое направление оптимизации уголовного закона по противодействию террористическим атакам. Предлагаемая редакция указанной нормы:

«П.2 ст. 255 УК РК

2. Те же деяния, совершенные:

12) с применением оружия либо предметов, используемых в качестве оружия, взрывчатых веществ или взрывных устройств, «*кибератак»,* которые могут создать реальную угрозу для жизни и здоровья граждан».

– Необходимо для профилактики киберпреступности обучать сотрудников правоохранительных органов информационным технологиям, и также внедрить в программы обучения и переподготовки кадров такие предметы, как: «Профилактика киберпреступности» и «Правовые основы информационной безопасности».

Исходя из вышеизложенного, можно сделать вывод о том, что киберпреступность представляет собой реальную угрозу безопасности и мира современного общества и человечества, отнимает доверие не только к людям, но и к компетенциям государственной власти и международных организаций. Поэтому, помимо указанных наверху подходов и решений, для борьбы с киберпреступностью необходимы свежие подходы, основанные на широком использовании успехов науки и техники, а также подготовка сотрудников нового поколения, в совершенстве владеющих навыками компьютерных технологий и компьютерного программирования**.**

Список использованной литературы:

1. Номоконов В.А., Тропина Т.Л. Киберпреступность как новая криминальная угроза //Криминология интернет-пространства. – 1 (24)2012. – С.45-55.

2. Oxford English Dictionary. URL: http:/ /www. askoxford.com. Document (дата обращения: 22.11.2022.)

3. Волеводз А.Г. Противодействие компьютерным преступлениям: правовые основы международного сотрудничества. М.: Юрлитинформ, 2002. – 496 с.

4. Суслопаров А. В. Компьютерные преступления как разновидность преступлений информационного характера: Дис. … канд. юрид. наук. Красноярск, 2010 //https://www.dissercat.com/content/kompyuternye-prestupleniya-kak-raznovidnost-prestuplenii-informatsionnogo-kharaktera. Document (дата обращения: 23.11.2022.)

5. Нарижный А.В. Использование специальных познаний при выявлении и расследовании преступлений в сфере компьютерной информации и высоких технологий: Дис. … канд. юрид. наук. Краснодар, 2009 // https://www.dissercat.com/content/ispolzovanie-spetsialnykh-poznanii-pri- vyyavlenii-i-rassledovanii-prestuplenii-v-sfere-kompy. Document (дата обращения: 24.11.2022.)

6. Суслопаров А. В. Информационные преступления: Дис. … канд. юрид. наук. Красноярск, 2008 //https://www.dissercat.com/content/informatsionnye-prestupleniya. Document (дата обращения: 24.11.2022.)

7. Тропина Т.Л. Киберпреступность: понятие, состояние, уголовно-правовые меры борьбы: Дис… канд. юрид. наук. Владивосток, 2005 // https://www.dissercat.com/content /kiberprestupnost-ponyatie-sostoyanie- golovno-pravovye-mery-borby. Document (дата обращения: 02.12.2022.)

8. Чекунов И.Г. Криминологическое и уголовно-правовое обеспечение предупреждения киберпреступности: Дис. … канд. юрид. наук. – М., 2013 // https://www.dissercat.com/ content/ kriminologicheskoe-i-ugolovno-pravovoe-obespechenie-preduprezhdeniya-kiberprestupnosti. Document (дата обращения: 02.12.2022.)

9. Степанов-Егиянц В.Г. Преступления в сфере безопасности обращения компьютерной информации: Сравнительный анализ: Дис. … канд. юрид. наук. – М., 2005 //https://www. dissercat.com/content/prestupleniya-v-sfere-bezopasnosti-obrashcheniya-kompyuternoi-informatsii-sravnitelnyi-anali. Document (дата обращения: 02.12.2022.)

10. Дуленко В.А., Мамлеев Р.Р., Пестриков В.А. Использование высоких технологий криминальной средой. Борьба с преступлениями в сфере компьютерной информации: учеб. пособие. Уфа: УЮИ МВД России, 2007. –187 с.

11. Рассолов И.М. Киберпространство и позитивное право //Политика и общество. 2009. № 2. – С.33-37.

12. Волеводз А.Г. Конвенция о киберпреступности: новации правового регулирования // Правовые вопросы связи. – 2007. – № 2. – С. 17 -25.

13. Уголовный кодекс Республики Казахстан от 3.07.2014 № 226-v (с изм. и доп. по сост. на 02.03.2022) //https://online.zakon.kz/Document. Document (дата обращения: 04.12.2022.)

14. Cambridge Advanced Learner's Dictionary URL: http: //dictionary. cambridge. Org. Document (дата обращения: 04.12.2022.)

15. Тропина Т.Л. Киберпреступность. – Владивосток, 2009. – С.45-55.

16. Бекряшев А.К., Белозеров И. П. Теневая экономика и экономическая преступность /Электронный учебник. Омск: Омский государственный университет. Омск: Омский государственный университет. 2000. – 459 с.

17. Батурин Ю. М., Жодзишский А.М. Компьютерная преступность и компьютерная безопасность. – М., 1991. – 160 с.

18. Яковлев А. Н., Олиндер Н.В. Особенности расследования преступлений, совершенных с использованием электронных платёжных средств и систем: научно-методич. пособие. – М., 2012. – 249 с.

19. Модельный закон о киберпреступности Международного Союза Электросвязи (2009) //См.: URL: http://www.itu.int/ITU- D/cyb/cybersecurity /docs/itu-toolkit-cybercrime-legislation.pdf. ITU, 2009. Document (дата обращения: 04.12.2022.)

20. Постановление Правительства Республики Казахстан от 30.06.2017 № 407 «Об утверждении Концепции кибербезопасности («Киберщит Казахстана»)» //http://adilet.zan.kz/rus/docs/P1700000407. Document (дата обращения: 05.12.2022.)

21. Постановление Правительства Республики Казахстан от 12 декабря 2017 № 827 «Об утверждении Государственной программы «Цифровой Казахстан» // http://adilet. zan.kz/rus/docs/P1700000827. Document (дата обращения: 05.12.2022.)

22. Старичков М.В. Умышленные преступления в сфере компьютерной информации: уголовно-правовая и криминологическая характеристики: дис. ... канд. юрид. наук. – Иркутск, 2006. – 237 с.

23. Сеитов Т. Б. Правовые аспекты компьютерной преступности в зарубежных странах и в Казахстане. Учебное пособие. – Алматы: Издательство «Данекер», 2000. – 134 с.

24. Бимолданов Е.М. и др. Уголовные правонарушения в сфере информатизации и связи: Учебное пособие. – Алматы: ООНИиРИР Алматинской академии МВД Республики Казахстан, 2015. – 194 с.

25. Фишинговые сайты, spear-phishing, whaling – «киберщит Казахстана» совершенствует систему безопасности. Официальный информационный ресурс Премьер-министра РК//https://primeminister.kz/ru/news/reviews/fishingovye-sayty-spear-phishing-whalingkibershchit-kazahstana-sovershenstvuet-sistemu-bezopasnosti-2675856. 26 август 2021, 13:00. Document (дата обращения: 05.12.2022.)