УДК 343.851

Айдарова Айнұр Айтуғанқызы
магистр юриспруденции, Казахский гуманитарно-юридический инновационный университет, г. Семей
E-mail: ainur_745@mail.ru
Қамбаров Азамат Қамбаруλы
магистр юридических наук, Казахский гуманитарно-юридический инновационный университет, г. Семей
E-mail: aza.kambarov@mail.ru

ПРОБЛЕМНЫЕ ВОПРОСЫ ПРЕДУПРЕЖДЕНИЯ КИБЕРПРЕСТУПНОСТИ

Осы мақалада дамыған елдерде киберқылмыстылықпен күресудің заманауи әдістері және оларды Қазақстан Республикеасының құқық қорғау органдары үшін қолдану мүмкіндіктері қарастырылған. Компьютерлік технологиялыардың экономикалық мүмкіндіктері қылмыскерлердің осы салаға ден қоюымен сипатталады. Киберқылмыстылық АТ және ғаламтор желілерінде кеңінен насихатталу үстінде. Компьютерлік технологияларды қолдану арқылы жасалған қылмыстық құқықбұзушылықтардан қорғаудың техникалық тәсілдері киберқылмыстылықты тергеуді тиімді жүргізуге, қылмыс компоненттерін дұрыс саралауға және әділ жаза қолдануға мүмкіндік беретін ұйымдастырушылық және қылмыстық-құқықтық тәсілдермен бірге зерттеледі.

Түйін сөздер: *киберқылмыстылық; қылмыстық құқық бұзушылық; ақпараттық технологиялар; қылмыстылықпен күресу; қылмыстылықпен күресу тәсілдері; киберқылмыстылықты алдын алу; қылмыстарды саралау.*

В представленной статье рассматриваются современные методы борьбы с киберпреступностью в развитых странах и возможности их использования для правоохранительных органов в Республике Казахстан. Экономические возможности компьютерных технологий делают их привлекательными для преступников. Киберпреступность пропагандируется ИТ в повседневной жизни и в Интернете. Технические методы защиты от уголовного преступления, совершенного с использованием компьютерных технологий, изучаются вместе с организационными и уголовно-правовыми методами, позволяющими проводить эффективное расследование киберпреступлений, правильно классифицировать компоненты преступлений и справедливое наказание. Обоснована возможность дальнейшей криминализации деяний, учитывающих порядок совершения преступлений и способ совершения преступлений в киберпреступности. Проведенные исследования позволили автору классифицировать современные современные методы борьбы с киберпреступностью и прийти к выводу об их комплексном использовании.

Ключевые слова: *киберпреступность; уголовные правонарушения; информационных технологии; борьба с преступностью; методы борьбы с преступностью; предупреждение киберпреступности; квалификация преступления.*

The article submitted covers advanced methods of cybercrime fighting in developed countries and opportunities of their use for law enforcement in Republic of Kazakhstan. Economic opportunities of computer technologies make them attractive for criminals. Cybercrime is promoted by IT in everyday life and Internet. Technical methods of protection from criminal offense committed with the use of computer technologies are studied together with organizational and criminal law methods enabling efficient investigation of cybercrimes, correct classification of crime components and fair punishment. Feasibility of further criminalization of acts accounting for lucri causa and crime commitment method in cybercrimes is substantiated. The conducted research enabled the author to classify the advanced contemporary methods in connection with fighting cybercrime and come to the conclusion on their comprehensive use.

Keywords: *Cybercrime; crimes; information technologies; prevention of crime; method of prevention crime; prevention against cybercrime; qualification of crime.*

В настоящее время происходит широкомасштабное формирование глобального информационного общества, когда вопрос информационной безопасности стоит в лидерах. Сегодня невозможно представить финансово-хозяйственную деятельность без использования информационно-коммуникационных технологий, сильно развившихся в XXI веке. В настоящее время такие технологии широко используются в бизнесе, в том числе в банковском деле (интернет-банкинг), электронных аукционах / торговле и т. Д. Между тем, их широкое внедрение создало такое негативное явление, как компьютерные преступления или киберпреступность, угрожая их безопасному использованию.

Между тем правоохранительные органы нуждаются в качественной и своевременной защите от уголовных преступлений в цифровой сфере. Киберпреступники угрожают экономическому развитию Казахстана и препятствуют созданию информационного общества. Как свидетельствует статистика, темпы роста преступности в сфере IT все еще высоки. В Казахстане количество угроз постоянно растет, и в прошлом году доля

уникальных пользователей, страдающих от интернет-атак, превысила 50% [1].

Глобальная тенденция свидетельствует о том, что около 70% преступлений, совершаемых в сфере высоких технологий, - это те, в которых компьютеры и другие электронные устройства используются в качестве средства для кражи, а мошеннические намерения преступника направлены на арест имущества другого лица [2].

Государственная политика по борьбе с преступностью, в том числе в связи с транснациональными организационными формами (в том числе в киберпространстве), претерпела значительные изменения за последнее десятилетие. Результаты усилий по борьбе с киберпреступностью не устраивают создание информационного общества в Казахстане. Идет активный поиск оптимальных организационно-правовых форм борьбы с экономической и организованной, транснациональной преступностью. Министерство внутренних дел Казахстана своевременно реагирует на возникающие новые угрозы кибербезопасности, принимая активное участие в борьбе с киберпреступностью.

На сегодняшний день преступники чаще используют новые криминальные методы, такие как электронные методы и средства, например, мобильная связь, интернет-банкинг. На современном этапе важно и примечательно постоянно совершенствовать методы, обеспечивающие успешное предотвращение, пресечение и расследование киберпреступлений, обеспечивая неизбежность наказания. Следует отметить, что в последнее время появляется ряд научных школ по борьбе с киберпреступностью, в том числе российская научная школа, ориентированная главным образом на уголовно-правовые аспекты борьбы с киберпреступностью [3]. Эти исследования, как правило, являются основой традиционных методов борьбы с киберпреступностью, таких как криминализация и декриминализация киберпреступлений. Западные ученые уделяют наибольшее внимание криминологическим аспектам, классифицирующим киберпреступности или типы киберпреступников. Такое исследование направлено на установление широкой общественности методов борьбы с киберпреступностью и технической защиты. Не рассуждая о значении вышеупомянутых ученых, следует сказать, что сегодня целесообразно использовать передовые методы, применяемые в странах, борющихся с киберпреступностью, долго и успешно. В основном это страны Запада, ЕС, США, но в последнее время Россия также продемонстрировала успехи в борьбе с киберпреступностью. Изучение методов, позволяющих достичь определенных успехов в борьбе с киберпреступностью, является целью данной статьи. Использование методов, еще не используемых казахстанскими правоохранительными органами, позволит им всегда быть на шаг впереди, предотвращая акты киберпреступников всех видов.

В соответствии с Конвенцией о киберпреступности (Будапешт), вступившей в силу 1 июля 2004 года (далее именуемой Конвенцией), киберпреступления представляют собой акты против конфиденциальности, целостности и доступности компьютерных систем, сетей и компьютерных данных, а также злоупотребления такими системами, сетями и данными. Статья 12 предусматривает корпоративную ответственность, которая противоречит действующему российскому уголовному законодательству. Как обоснованно заявлено Арбузовым и Кубанцевым, действующие положения об уголовной корпоративной ответственности в России довольно поверхностны, игнорируют существующую уголовно-правовую доктрину и в случае их реализации способны дезорганизовать систему уголовного судопроизводства, становясь дополнительным источником правоприменения. коррупция в офисах и других государственных учреждениях [4].

В связи с острой необходимостью борьбы с киберпреступностью 1 июня 2001 года в Минске было заключено Соглашение стран СНГ о сотрудничестве в борьбе с киберпреступностью, статья 1 о том, что киберпреступление является уголовно наказуемым деянием, когда объектом насилия является компьютерная информация.

Учитывая, что вышеуказанные международные правила о киберпреступности довольно противоречивы, включая противоречия в определении киберпреступности, это может привести к уклонению от уголовной ответственности только потому, что государство, в котором совершено киберпреступление, и государство, в котором был задержан виновный, ориентированы на разные международные договоры о киберпреступности.

По оценке Европола, ежегодный ущерб от киберпреступности в мире оценивается в 290 миллиардов евро. Только в прошлом году

гражданам ЕС был нанесен прямой ущерб стоимостью 1,5 миллиарда евро. Это делает киберпреступность более выгодной, чем марихуана, героин и кокаин, которые все вместе продают [5].

Согласно докладу Европола «Оценка угрозы серьезной и организованной преступности ЕС» (SOCTA), только на территории ЕС было ликвидировано 3600 преступных группировок, совершивших преступления в Интернете с целью получения личной финансовой выгоды и нарушения экономической стабильности. Эксперты Европола должны заявить, что в настоящее время выявлено только 30% всех киберпреступлений, и поэтому прогнозируется рост преступных действий в этой сфере, что связывает рост киберпреступности с ростом значимости Интернета в личной жизни. Также упомянутые эксперты утверждают, что растущее значение мобильных устройств в качестве основного средства доступа в Интернет может стать причиной более широкого использования этих устройств преступниками [6].

Следует также отметить, что не все страны криминализировали киберпреступность. Киберпреступность не преследуется в уголовном порядке в некоторых странах, что создает безнаказанных профессиональных киберпреступников.

Для совершения киберпреступлений достаточно приобрести средства спутниковой связи. Время совершения такого рода преступлений может занимать менее минуты, и преступник не ограничен в выборе страны, на территории которой он / она будет его использовать. Правоохранителям, как правило, требуется много времени, чтобы найти и привлечь к ответственности такого человека, что позволит преступнику скрыть следы преступления, что сделает невозможным привлечение к ответственности киберпреступника. В этой ситуации только объединение усилий всех сотрудников правоохранительных органов всех стран делает возможным эффективное предотвращение этой категории транснациональных преступлений.

Из-за открытого доступа в Интернет большинство киберпреступлений совершаются через Интернет, так как найти человека, совершившего преступление, довольно сложно. Одним из факторов роста этих преступлений в Казахстане является отсутствие необходимого сотрудничества между правоохранительными органами в расследовании этих видов преступлений. В связи с этим особое значение приобретает необходимость повышения квалификации сотрудников правоохранительных органов при расследовании этих преступлений.

Как обоснованно отметил Костин, киберпреступления редко бывают самостоятельными, они, как правило, сопровождаются другими антиобщественными действиями и не являются обязательными [7]. Это обусловлено тем, что использование компьютерных технологий в качестве средства совершения другого преступления становится предметом антиобщественного деяния.

Правоохранители сталкиваются с большими проблемами в борьбе с компьютерным мошенничеством. На открытии IV Международной конференции Hightech по борьбе с мошенничеством против мошенничества в России начальник Управления по специальным техническим мерам Министерства внутренних дел Российской Федерации (далее именуемый БГТМ МВД РФ) генерал-майор полиции Мошков заявил, что с каждым годом сложность мошенничества в Интернете растет, предъявляя особые требования к квалификации сотрудников, занимающихся расследованием киберпреступлений.

Имеется некоторый отечественный и зарубежный опыт решения проблем информационно-аналитического обеспечения борьбы с киберпреступностью, особенно организованный. Некоторое время назад в Российской Федерации использовались различные системы принятия решений и системы управления базами данных (СУБД KRONOS, BINAR, LAGUNA, использующие информационную модель взаимосвязи сущностей) вместе со спецификой информационно-аналитической работы правоохранительных органов в борьбе с организованной преступностью [8].

Например, связь между любыми двумя людьми может быть обнаружена на пятом или шестом уровне. Недавно Московский институт МВД России, созданный для интересов правоохранителей в борьбе с организованной преступностью и готовящий для них компетентных специалистов, прошел специальный курс «Аналитическая разведка». Это касается всего, что связано с открытыми источниками информации, экономической, конкурентной или деловой разведкой и кибербезопасностью. Практические занятия включали в себя факультативный курс практики

в компьютерном классе и нахождение различных связей.

Некоторые аналитики пытаются синтезировать представление разбросанных данных (если некоторые данные отсутствуют, существуют некоторые статистические методы для работы с потерянными данными), ожидая оптимального решения. Когда мы принимаем определенного аналитика в процесс принятия решений, он/она должен хорошо владеть профессиональной областью. Но, к сожалению, это не преподается в юридических колледжах.

Когда упоминается информационная модель, под информационной моделью понимаются статистические данные о киберпреступности. На самом деле у нас что-то другое - информационная система. Ситуация также может быть представлена математической моделью. Поведение толпы в случае массового соперничества или нарушения общественного порядка описывается системой дифференциальных уравнений.

Вышеуказанные системы (СУБД) были хорошими для обнаружения цепочек связей, но не решали множество аналитических проблем и не могли дать вероятную структуру преступной группы (включая кибергруппу), в то время как структура является наиболее важной особенностью преступной организации [9].

Давайте посмотрим на некоторые примеры успешного использования других методов правоохранительными органами из других стран. Хорошо известен пример использования хакерских методов секретными службами.

ФБР США использует в течение нескольких лет по крайней мере один из самых сложных методов взлома, чтобы проникнуть в компьютеры пользователей, которые пытаются скрыть их интернет-серфинг, как сообщает Wired [10].

В частности, существует метод, называемый «загрузка с диска». Это позволяет установить на компьютер пользователя вредоносный код без необходимости устанавливать что-либо вручную. Для заражения достаточно зайти на веб-страницу с кодом, размещенным хакерами (в данном случае ФБР).

ФБР использовало хакерские методы для борьбы с преступниками с помощью сети Tor. Он не позволяет увидеть, какой компьютер использовался для доступа в Интернет, и помогает скрыть местоположение сервера веб-страницы.

Технология, на которой базируется Tor, была разработана научно-исследовательской лабораторией ВМС США в 1990-х годах для защиты правительственных каналов связи, а затем стала общедоступной в качестве средства защиты личной жизни. Однако эти сети стали популярными среди преступников, занимающихся распространением детской порнографии, продаже наркотиков, оружия и т.д.

В 2011 году ФБР и полиция Нидерландов начал операцию под названием Torpedo, чтобы поймать преступника занимается распространением порнографии ребенка через сеть Tor. Полицейские регулярно посещали сайт преступника и однажды обнаружили, что он оставил свой аккаунт администратора открытым для любого посетителя.

Взлом Tor также интересен для МВД России. В июле власти объявили закрытый конкурс с призовым фондом на сумму 3,9 миллиона. Эти средства обещаны человеку, который поможет взломать технологию Tor и найти способ раскрыть информацию о ее анонимных пользователях.

Добавим, что правительство США является основным источником финансовой поддержки и развития Tor Project. В 2013 году государственное финансирование выросло на 47%.

Оправдано ли использовать их методы противодействия? Многие думают, что для войны хороши любые средства. Однако цивилизованный мир не должен оставаться на одном шаге с преступниками. Даже в борьбе с абсолютным злом, таким как терроризм, мы должны различать средства. Самое эффективное оружие в борьбе с киберпреступниками - официальное [11].

Создание единой системы борьбы с вирусным программным обеспечением и межгосударственной правовой политики является одним из условий эффективного противодействия в связи с такого рода преступлениями.

Один только технический и технологический подход для обеспечения информационной безопасности в условиях информатизации, в том числе для предотвращения киберпреступлений, не имеет большого успеха [12].

Анализ киберпреступности предсказывает сложность борьбы с ней, поскольку методы киберпреступности становятся все более изощренными и их трудно обнаружить. Эта проблема должна быть решена комплексно.

Специалисты определяют следующие элементы правоприменения в глобальных информационных сетях: изучение и оценка ситуаций в сетях; оптимальное распределение ресурсов; сотрудничество; управление, планирование и контроль; координация деятельности правоохранительных органов.

Важным элементом борьбы с киберпреступностью является предотвращение или предосторожность. Большинство зарубежных специалистов утверждают, что предотвратить киберпреступность гораздо проще и проще, чем расследовать ее.

Обычно указываются три группы мер профилактики: правовая, организационная и техническая, криминалистическая, полностью составляющая совокупную систему борьбы с этим антиобщественным явлением [16].

Что может действовать в нормативных актах РК против указанных угроз? Только недавно была только одна статья 227 Уголовного кодекса РК, содержащая два простых компонента преступления и два обострения, и теперь есть целая глава (Глава 7 Особенной части Уголовного кодекса РК, 2014, содержащая 9 статей (205-213), каждая из которых содержит, помимо простых составляющих преступления, одно или два обострения, а также два обострения были включены в главу о преступлениях против собственности, предусматривающих ответственность за действия с использованием информационных систем и сетей (кража) ст. 188 УК РК, ч. 2, п. 4, путем незаконного доступа к информационной системе или изменения информации, передаваемой по информационной сети, и мошенничество, ст. 190 УК РК, ч. 2, п. 4, путем мошеннического поведения или злоупотребление доверием пользователя к пользователю информационной системы.) Видно, что в этом случае регулирующий орган сделал ответственность за киберпреступность более детальной, что вполне соответствует современным тенденциям уголовного законодательства. Преступники, использующие компьютерные технологии, достаточно сложны, и в будущем могут быть разработаны некоторые схемы краж, не включая доступ или изменение информационных систем или сетей. Поэтому мы полагаем, что законодатели РК должны заимствовать у своих российских коллег правовое понятие компьютерных технологий, применяемых при построении криминальных компонентов в соответствии со статьей 159.6 УК РФ, Мошенничество с использованием компьютерных технологий.

В настоящее время улучшены не только правила киберпреступности, но и программное обеспечение для автоматического обнаружения киберпреступлений. Правительство Нью-Джерси (США) спонсировало новый проект по борьбе с хакерами и профинансировало около 2,6 миллиона долларов США.

В борьбе с киберпреступностью невозможно использовать одни методы и отказываться от других или игнорировать их. Только комплексный подход в качестве общего метода обеспечит успешное решение задач борьбы с киберпреступностью и ее снижение. Конечно, в этой статье не рассматривается ряд современных и эффективных методов, что заставляет авторов углублять и расширять исследования методов борьбы с киберпреступностью в будущих работах.

Пайдаланылған әдебиеттер тізімі

1. Мамбетов С. (2015) Киберпреступников привлекают многие вещи в Казахстане.
2. Каиржанова С. (2015) Борьба с киберпреступностью: опыт Республики Казахстан и зарубежных стран.
3. Лебедева А. (2014) Мошенничество в сфере высоких технологий в соответствии с национальным и международным уголовным правом. Международное уголовное право и международное правосудие 5: 15-17.
4. Арбузов С., Кубанцев С. (2012) О перспективах института корпоративной уголовной ответственности в России. Российский юридический журнал.
5. Организация Объединенных Наций (2006) Европейский институт по предупреждению преступности и борьбе с ней.
6. (2013) Оценка угрозы серьезной и организованной преступности в ЕС (SOCTA).
7. Костин П. (2007) Исследование компьютерных носителей информации, используемых при совершении экономических преступлений. Конспект диссертации, Нижний Новгород.
8. Минин А., Овчинский А. (1996) Информационно-аналитическое обеспечение принятия решений в рискованных ситуациях. Информационно-аналитическое обеспечение управления коммерческими рисками.
9. Старостина Е. (2015) Компьютерный взлом - это инструмент хакера, а не защитника (Исследовательский центр киберпреступности).
10. Клаверов В. (2009) Проблемы борьбы с киберпреступностью.
11. Старостина Е., Фролов Д. (2005) Защита от киберпреступности и кибертерроризма.
12. Kroes N (2013) Выступление: Стратегия кибербезопасности ЕС.

Айдарова Айнұр Айтуғанқызы
Лауазымы: құқықтану магистрі, қылмыстық-құқықтық пәндер кафедрасы, Қазақ инновациялық гуманитарлық-заң университеті, Семей қ.
Пошталық мекен-жайы: 071400, ШҚО, Семей қ., К.Бозтаева к-сі 5-20
ұялы тел. 8 778 920 03 00
Қамбаров Азамат Қамбаруұлы
Лауазымы: заң ғылымдарының магистрі, қылмыстық-құқықтық пәндер кафедрасы, Қазақ инновациялық гуманитарлық-заң университеті, Семей қ.
Пошталық мекен-жайы: 071400, ШҚО, Семей қ., К.Бозтаева к-сі 5-20
ұялы тел. 8 778 920 03 00
Киберқылмыстылықты алдын алудың өзекті мәселелері

Айдарова Айнұр Айтуғанқызы
Должность: магистр юриспруденции, кафедра уголовно-правовых дисциплин, Казахский гуманитарно-юридический инновационный университет г. Семей
Почтовый адрес: ВКО, г. Семей, ул.К.Бозтаева 5, кв.20
Сот тел. 8 778 920 03 00
Қамбаров Азамат Қамбаруұлы
Должность: магистр юридических наук, кафедра уголовно-правовых дисциплин, Казахский гуманитарно-юридический инновационный университет г. Семей
Почтовый адрес: ВКО, г. Семей, ул.К.Бозтаева 5, кв.20
Сот тел. 8 778 920 03 00
Проблемные вопросы предупреждения киберпреступности

Aidarova Ainur Aitugankyzy
Position: Master of Laws, Department of Criminal Law Disciplines, Kazakh Humanitarian Juridical Innovative University, Semey city
Postal address: VKO, Semey, K. Boztaev St., 5, apt. 20
Sot tel. 8 778 920 03 00
Kambarov Azamat Kambaruly
Position: Master of Laws, Department of Criminal Law Disciplines, Kazakh Humanitarian Juridical Innovative University, Semey city
Postal address: VKO, Semey, K. Boztaev St., 5, apt. 20
Sot tel. 8 778 920 03 00
Problems of prevention of cibercrime