КРИМИНОЛОГИЧЕСКИЕ АСПЕКТЫ ИНФОРМАЦИОННОЙ ПРЕСТУПНОСТИ

Кабжанов А.Т., Ахметбеков Д.
гор. Караганда, РК

Аннотация: рассматриваются криминологические проблемы информационной преступности,

Ключевые слова: информационная преступность, терроризм, экстремизм, наркотизм, коррупция, киберпреступления, кибербезопасность.

Профилактика информационных преступлений в настоящее время выходит в один ряд с такими опасными проявлениями беззакония как терроризм, экстремизм, наркотизм и коррупция. В науке информационные преступления или уголовные правонарушения в сфере информатизации и сети называют – киберпреступлениями.

В Послании Президента Республики Казахстан Н. Назарбаева народу Казахстана. 10 января 2018 г. «Новые возможности развития в условиях четвертой промышленной революции» сказано о том, что «Внедряя новые технологии, государству и компаниям следует обеспечивать надежную защиту своих информационных систем и устройств.

Сегодня понятие кибербезопасности включает в себя защиту не просто информации, но и доступа к управлению производственными и инфраструктурными объектами. Эти и иные меры должны найти отражение в Стратегии национальной безопасности Казахстана» [1].

Рассмотрим современные взгляды на некоторые аспекты киберпреступлений. В соответствии с рекомендациями экспертов ООН термин «киберпреступность» подразумевает любое преступление, которое может совершаться с помощью компьютерной системы или сети, в рамках, а также против компьютерной системы или сети. 15 Конвенция Совета Европы выделяет четыре вида компьютерных преступлений, связанных с нарушением конфиденциальности, целостности и доступности компьютерных данных и сети. Остальные преступления, в которых компьютер является орудием или средством совершения преступлений, должны рассматриваться как традиционные преступления, но правовые механизмы их расследования должны быть адекватными средствам совершения этих преступлений [2].

Казахстанским же законодательством была отмечена особая актуальность вопросов защищенности технических средств приема, передачи и накопления информации от несанкционированного доступа, в частности Законом РК «О национальной безопасности» от 26 июня 1998 года введением понятия «информационная безопасность», а также Указом Президента РК «О Концепции информационной безопасности РК». С закреплением в Уголовном кодексе РК главы 7 (Уголовные правонарушения в сфере информатизации и сети), предусматривающей ответственность за такого рода деяния, правоохранительные органы получили реальную возможность борьбы с лицами, использующих компьютерную технику в преступных целях. В целом, статистические данные о количестве зарегистрированных преступлений, предусмотренных статьей 205 УК РК за неправомерный доступ к компьютерной информации, создание, использование и распространение вредоносных программ для ЭВМ свидетельствует о том, что количество таких преступлений стремительно растет. Так, если в 2000 году зарегистрированных преступлений такого рода по стране было только 12, то в 2008 году их было в 5 раз больше. При этом следственным органам

становится известно о совершении компьютерных преступлений не более 10 процентов деяний такого характера. А показатель раскрываемости таких преступлений имеет еще меньшее число. По отношению к общему числу совершенных преступлений, деяний подобного рода с масштабным ущербом совершается не так уж много. Гораздо больший урон наносят мелкие компьютерные жулики-изготовители фиктивных документов. Изготовление
подложных документов, хищение денежных средств в крупных размерах с использованием компьютерной техники стали делом обычным [3].

Сегодня обычный рядовой пользователь компьютерной техники и сети может запросто произвести распечатку на принтере документов разного рода, бланков, свидетельств, штампов, сертификатов и т.д. Так за последние несколько лет преступлений, предусмотренных статьей 325 УК РК «подделка, изготовление или сбыт поддельных документов, штампов, печатей, бланков, государственных наград» было зарегистрировано около 20 тысяч. Начиная с 2004 года по 2008 года количество фактов подделок, изготовления или сбыта поддельных документов, штампов, печатей, бланков и государственных наград увеличилось на 22,6 % с 1645 до 2017. Однако, компьютерная техника и средства коммуникаций на территории РК используются в большей степени не как объекты посягательства (для сравнения, неправомерный доступ к компьютерной информации, хищение машинного времени, а также денежных средств посредством электронной транзакции - это далеко не полный перечень преступлений, с которыми вынуждены бороться правоохранительные органы США, Канады, стран Европы и т.д.), а в большей степени как средства преступной деятельности[4].

Киберпреступность угрожает не только отдельным лицам или организациям, но потенциально - национальной безопасности любой страны, достигшей значительного уровня компьютеризации жизненно важных отраслей экономики.

С возрастанием роли Интернета в информационном пространстве возникает необходимость защиты прав и свобод человека и общества от информации, пропагандирующей насилие и жестокость, навязывания им ложной и недостоверной информации, от целенаправленного формирования негативного мировоззрения молодого поколения. При этом, источники внешних угроз могут находиться вне юрисдикции законодательства РК, что существенно затрудняет применение системы правовых мер.

Одной из актуальных проблем является отсутствие отечественных информационных технологий, что вынуждает массового потребителя приобретать импортную технику, не имеющую подтверждения соответствия требованиям информационной безопасности. Это представляет угрозу информационной безопасности баз и банков данных, а также возможной зависимости страны от иностранных производителей компьютерной и телекоммуникационной техники и информационной продукции. Жертвами преступников становятся учреждения, предприятия и организации, использующие автоматизированные информационные системы для обработки бухгалтерских документов, проведения платежей и других операций. Чаще всего мишенями киберпреступников становятся банки или счета физических лиц в тех же банках и финансовых организациях [5].

Но, пожалуй, наиболее уязвимыми для потока информационного мусора из Всемирной сети являются дети. А иногда, жертвы компьютерной преступности (большинство из них, частные предприниматели) проявляют нежелание контактировать с правоохранительными органами, опасаясь распространения мнения о собственной халатности и ненадежной работе своей фирмы или организации, что тоже создает немалую проблематику в

противодействиях преступности. Основной целью киберпреступника является компьютерная система, которая управляет разнообразными процессами, и та информация, что циркулирует в них. В отличие от обычного преступника, что действует в реальном мире, киберпреступник не использует традиционное оружие, например, нож или огнестрельное оружие.

В послании Президента страны народу Казахстана «Казахстан - 2030. Процветание, безопасность и улучшение благосостояния всех казахстанцев» в качестве долгосрочного приоритета определена национальная безопасность, одной из составляющих которой является информационная безопасность [6]. Современное состояние информационной безопасности в Казахстане показывает, что ее уровень в настоящее время не соответствует

потребностям человека, общества и государства. Нынешние условия политического и социально-экономического развития страны вызывают обострение противоречий между потребностями общества в расширении свободного обмена информацией и необходимостью сохранения отдельных ограничений на ее распространение. Особых методов для борьбы с компьютерными преступлениями не выделяют ни криминалисты, ни ученые-юристы, ни практики, ни IT-специалисты, используются те же методы и средства, что во всем мире. В мировой практике применяются в совокупности технические, организационные и правовые методы. К техническим методам можно отнести все те приемы, где для выявления незаконного проникновения в компьютерную сеть используется специальное оборудование. К организационным - мероприятия, которые направлены на повышение эффективности раскрытия киберпреступлений, в том числе совместные оперативно-профилактические мероприятия, направленные на выявление продукции и информации, запрещенной в свободном обороте, пропагандирующие экстремизм, терроризм, культ жестокости и насилия и детскую порнография. К правовым методам относятся разработка и совершенствования норм, устанавливающих ответственность за компьютерные преступления, защиту авторских прав программистов,принятие международных договоров в данной сфере. Все проблемы связанные с раскрытием компьютерных преступлений уже давно пересекли границы государств и получили международное значение. В настоящее время осуществляется постоянный обмен информацией и опытом со странами бывшего СНГ и дальнего зарубежья [7]. Для системной борьбы с преступлениями подобного рода в 2006 году был создан Национальный контактный пункт по борьбе с преступлениями в сфере информационных технологий, были внесены необходимые изменения в законодательство РК по вопросам совершенствования уголовной ответственности за преступления связанные с новыми технологиями. Конвенция Совета Европы о преступности в сфере компьютерной информации (ETSN 185) была подписана 23 ноября 2001 года в Будапеште. Она открыта для подписания как государствами - членами Совета Европы, так и не являющимися его членами государствами, которые участвовали в ее разработке. В частности, ее подписали Россия, США и Япония.Конвенция Совета Европы о киберпреступности подразделяет преступления в данной сфере на следующие группы. Преступления, направленные против конфиденциальности, целостности и доступности компьютерных данных и систем: незаконный доступ (статья 2), незаконный перехват (статья 3), воздействие на компьютерные данные (противоправное преднамеренное повреждение, удаление, ухудшение качества, изменение или блокирование компьютерных данных) или системы (статья 4, статья 5). Также в эту группу

преступлений входит противозаконное использование специальных технических устройств (компьютерных программ, разработанных или адаптированных для совершения преступлений, компьютерных паролей, кодов доступа, их аналогов, посредством которых может быть получен доступ к компьютерной системе в целом или любой ее части) (статья 6).

Преступления, связанные с использованием компьютерных средств. К ним относятся подлог и мошенничество с использованием компьютерных технологий (статьи 6, 7 и 8). Подлог с использованием компьютерных технологий включает в себя злонамеренные противоправные ввод, изменение, удаление или блокирование компьютерных данных, влекущие за собой нарушение аутентичности данных, с намерением, чтобы они рассматривались или использовались в юридических целях в качестве аутентичных. Производство, предложение или предоставление в пользование, распространение и приобретение детской порнографии, а также владение детской порнографией, находящейся в памяти компьютера (статья 9). Преступления, связанные с нарушением авторского права и смежных прав [2]. Согласно Конвенции каждое государство-участник обязан создать необходимые правовые условия для предоставления следующих прав обязанностей компетентным органам по борьбе с киберпреступностью: выемка компьютерной системы, ее части или носителей; изготовление и конфискация копий компьютерных данных; обеспечение целостности и сохранности хранимых компьютерных данных, относящихся к делу;
уничтожение или блокирование компьютерных данных, находящихся в компьютерной системе. Конвенция также требует создать необходимые правовые условия обязать Интернет-провайдеров проводить сбор и фиксацию или перехват необходимой информации с помощью имеющихся технических средств, а также способствовать в этом правоохранительным органам. При этом рекомендуется обязать провайдеров сохранять полную конфиденциальность о фактах подобного сотрудничества.

В начале 2002 года был принят Протокол №1 к Конвенции о киберпреступности, добавляющий в перечень преступлений распространение информации расистского и другого характера, подстрекающего к насильственным действиям, ненависти или дискриминации отдельного лица или группы лиц, основывающегося на расовой, национальной, религиозной или этнической принадлежности. Во многих странах мира в целях пресечения факта информационного преступления в последние годы специалисты по компьютерной безопасности начали сотрудничество с психологами, которые составляют профиль так называемого хакера, то есть преступника в сфере компьютерной информации и техники, который позволяет выявить уровень его квалификации и технической подготовки. Но следует отметить, что хотя компьютерные специалисты и могут многое сказать о хакере и о методах его работы, но они никогда не смогут понять психологию его криминального мышления. Подобными вопросами занимаются клинические психологи, судебные эксперты и другие специалисты совместно с органами внутренних дел. Подобная практика активно используется в США, Европе и других странах, где киберпреступления широко развиваются. Некоторые ученые считают, что налаживание подобной практики и в нашей стране, где преступления в сфере
информационных технологий пока неразвиты, позволит еще в зачаточной форме уничтожить основы киберпреступности. Для этого необходимо активизировать потребность международного сотрудничества.

Для обеспечения государственных органов полной, достоверной и своевременной информацией требуются принятие обоснованных решений, в том числе для защиты

государственных информационных ресурсов, а также разработка отечественных средств защиты информации и системы подтверждения соответствия импортируемых технических средств установленным требованиям, а также дальнейшая проработка вопросов противодействия техническим разведкам, защиты от информационного оружия и совершенствования нормативной правовой базы в данной сфере. Необходима комплексная координация мер по защите информации в общегосударственном масштабе и на ведомственном уровне для обеспечения целостности и конфиденциальности информации [4].

Новые информационные технологии должны быть не только орудием, средством совершения преступлений нарушителями закона, но и должны стать эффективным наступательным инструментом в борьбе с различными угрозами и в том числе преступностью во всех ее проявлениях, в связи с чем нужно привлекать в государственные структуры высококвалифицированных специалистов по борьбе с компьютерной преступностью.

Список литературы:

1. Послание Президента Республики Казахстан Н. Назарбаева народу Казахстана. 10 января 2018 г. «Новые возможности развития в условиях четвертой промышленной революции». http://gb.akmzdrav.kz/poslanie-prezidenta

2. «Европейская Конвенция по преступлениям в киберпространстве» // Будапешт, 23 ноября 2001 года (перевод: Институт проблем информационного права).

3. Крылов В.В. «Расследование преступлений в сфере информации» Глава 1, § 3 «Информация как элемент преступной деятельности».

4. Современные взгляды на некоторые аспекты киберпреступлений. https://articlekz.com/article/9662

5. Ахметов Е. «Киберпреступность в Казахстане» // Журнал «Законность и правовая статистика» 2009, № 2 (11).

6. Указ Президента Республики Казахстан «О Концепции информационной безопасности РК» от 10 октября 2006 года №199.

7. crime-research.ru Голубев В. «Стратегия и тактика борьбы с киберпреступностью в странах СНГ» 20 июня 2005 года.