КИБЕРПРЕСТУПНОСТЬ В РЕСПУБЛИКЕ КАЗАХСТАН: ПРОБЛЕМЫ И ПУТИ РЕШЕНИЯ

КАНАТ АЛЬСЕИТОВ,
доцент Института профессионального обучения Академии,
младший советник юстиции

Темпы цифровизации, развитие информационно-коммуникационных технологий и всеобщей интеграции информационных систем повлекли за собой возникновение новой формы преступности – киберпреступности, превратившейся в глобальную международную проблему.

Практически каждое государство столкнулось с проблемами защиты и сохранности данных, касающихся как коммерческой и личной информации, так и защиты государственных данных. Количество киберпреступлений по всему миру ежегодно растет.

Как один из лидеров цифровизации среди стран СНГ Казахстан также подвержен киберугрозам.

Руководство страны периодически отмечает актуальность борьбы с киберпреступностью[1].

К примеру, социологическое исследование, проведенное Министерством цифрового развития, инноваций и аэрокосмической промышленности РК, показало, что процент осведомленности населения об угрозах информационной безопасности в 2018 году составил ***62,9%***, 2019г. – ***73,5%***, 2020г. – ***78%*** и 2021г. – ***75%.***

Тем самым, отмечается снижение уровня осведомленности граждан на ***3%*** в 2021 году, чему поспособствовали такие факторы, как пандемия, использование онлайн приложений, удаленная работа и обучение.

Анализ отечественной правовой информации за последние 5 лет выявил некоторые проблемы в организации противодействия киберпреступности.

Так, согласно статистическим данным КПСиСУ, в период с 2017 по 2021 годы в стране было зарегистрировано ***20 145*** уголовных правонарушений, совершенных с использованием Интернета, обмана или злоупотребления доверием пользователя информационной системы и незаконного доступа в информационную систему, либо изменения информации, передаваемой по сетям телекоммуникаций, которые составили лишь ***1,7%*** в общей структуре преступности.[2]

На первый взгляд, данное количество кажется незначительным и не вызывает беспокойства.

Однако, если с 2017 по 2021 годы общая преступность в Казахстане снизилась на ***50,1%*** или с ***361,5 тысячи*** до ***157,9 тысяч*** *(т.е. на 158,5 тыс. уголовных правонарушений)*, то количество киберпреступлений возросло в ***31*** раз – со ***345*** до ***10 724*** в год.

И это лишь те факты, по которым правоохранительными органами начато досудебное расследование, поскольку учет преступности ведется только по зарегистрированным в ЕРДР уголовным правонарушениям.

По сведениям Службы реагирования на компьютерные инциденты «KZ-CERT» за последние 5 лет в Казахстане зарегистрировано ***115 900*** инцидентов *(кибератак)*, в том числе: ботнеты – ***74 897***, вредоносное программное обеспечение – ***15 505***, отсутствие доступа к интернет ресурсу – ***7 833***, фишинг – ***3 238***, незаконный доступ и модификация содержания ИР – ***2 820***, отказ в обслуживании – ***840*** и другие – ***10 767*** инцидентов[3].

Как видно, способы совершения киберпреступлений различны, они постоянно развиваются и становятся более профессиональными.

Статданные свидетельствуют, что низкая регистрация связана вовсе не с тем, что преступления данной категории не совершаются, а с их низкой

[1] https://www.akorda.kz/ru/addresses/addresses_of_president/poslanie-prezidenta-respubliki-kazahstan-nnazarbaeva-narodu-kazahstana-31-yanvarya-2017-g.

[2] Отчет № 1-М «О зарегистрированных уголовных правонарушениях» за 2016 – 2020 годы.

[3] https://www.cert.gov.kz/.

выявляемостью и отсутствием специальных познаний в области новых компьютерных технологий у сотрудников правоохранительных органов, что указывает на необходимость проведения комплекса исследовательских и организационных мер. При этом, немаловажным является организация надлежащего взаимодействия и координация деятельности профильных подразделений правоохранительных органов.

В этой связи, эффективность деятельности правоохранительных органов в области выявления и раскрытия киберпреступлений снижается.

Если говорить на языке цифр, по результатам досудебного расследования раскрыто всего ***6955*** или ***34,5%*** уголовных дел, прекращено по реабилитирующим основаниям ***2030*** или ***10,1%***, прерваны сроки по ***12 546 или 62,3%*** уголовному делу.

Изучение уголовных дел, прекращенных по реабилитирующим основаниям, показало, что признание и допрос потерпевшего произведен только по 5 делам, а запрос по установленным IP-адресам всего лишь по одному делу. По остальным делам следственные действия не проводились, объем таких дел в среднем составил 12 страниц.

Имеются факты вынесения судом оправдательного приговора в отношении лица, совершившего уголовные правонарушения в сфере информатизации и связи.

Так, согласно материалам дела, в период с 11 по 26 июня 2018 года гражданин Л., используя возможности сети Интернет взломал пароль и без согласия собственника неоднократно осуществлял неправомерный доступ к электронной почте гражданки С., которую использовал в личных целях.

Причастность гражданина Л. подтверждена добытыми в ходе расследования доказательствами, однако, приговором районного суда №2 Бостандыкского района г.Алматы гражданин Л. признан невиновным, поскольку протокол об уголовном проступке составлен в нарушение требований ст.526 ч.1 УПК РК по истечению 18 дней с момента установления подозреваемого.

Количество преступлений, совершаемых в киберпространстве, растет пропорционально числу пользователей компьютерных сетей, и, по оценкам Интерпола, темпы роста преступности в глобальной сети Интернет являются самыми быстрыми на планете.

Государства применяют самые разнообразные методы борьбы с киберпреступлениями, одним из которых является привлечение хакеров.

Так, в Японии для борьбы с киберпреступностью полицией созданы условия для привлечения «этичных» хакеров и взаимодействие с учебными заведениями и компаниями, занимающимися IT-технологиями для привлечения к сотрудничеству экспертов по киберпреступности.

В Великобритании с 2001 года действует национальный отдел борьбы с высокотехнологичными преступлениями, включающий в себя следователей, судебно-медицинских экспертов и консультантов по компьютерам.

В США национальный центр защиты инфраструктуры (NTPC) обеспечивает оценку угроз, предупреждение о кибератаках и расследование кибератак.

В Канаде для реагирования на киберугрозы в 2001 году создано Управление защиты критической инфраструктуры и мобилизационной готовности, а также принято соответствующее законодательство, способствующее расследованию преступлений, связанных с использованием высоких технологий.

Как было отмечено выше, отсутствие специальных познаний в области новых компьютерных технологий у сотрудников правоохранительных органов не позволяют надлежащим образом квалифицировать и расследовать преступления данной категории.

С учетом актуальности проблемы и изучения международного опыта по созданию профильных организаций для обучения сотрудников правоохранительных органов методам расследования киберпреступлений, Академией правоохранительных органов в качестве пилотного проекта по одному из направлений Регионального Хаба ведется работа по созданию учебно-практического центра по подготовке сотрудников правоохранительных органов в сфере противодействия киберпреступности.

Основные направления центра - подготовка сотрудников правоохранительных органов к расследованию киберпреступлений, работа с электронными доказательствами и проведение оперативных мероприятий в компьютерных сетях и сети Интернет, обмен передовым отечественным и международным опытом не только среди правоохранителей, но судей, экспертов и адвокатов.

За последние два года Академией проведено более ***10*** обучающих мероприятий, посвященных вопросам противодействия киберпреступности для надзирающих и специальных прокуроров, а также сотрудников правоохранительных и специальных органов.

Как один из результатов, применение полученных знаний и навыков следователями и прокурорами способствовало снижению Интернет-мошенничеств на ***18,4%*** с 10 097 *(5 месяцев 2021г.)* по 8 240 *(за аналогичный период 2022г.)*.

Выражаем надежду, что в дальнейшем центр станет узнаваемой международной площадкой для команды профессионалов, объединяющей лучший международный опыт в сфере противодействия киберпреступности, имеющей собственные ресурсы для организации и проведения обучающих мероприятий на высоком уровне для сотрудников правоохранительных и специальных органов, судей, судебных экспертов и адвокатов Республики Казахстан, СНГ и Центральной Азии.

Такие меры повысят эффективность борьбы с киберпреступностью на протяжении всего уголовного процесса, начиная от принятия заявления до вступления судебного акта в силу.