

Hojiyev Xagani Mohubbat o'g'li
O'zbekiston Respublikasi Ichki ishlar vazirligi
Davlat ekspert-kriminalistika markazi bosh eksperti

KIBERXAVFSIZLIK NUQTAI NAZARIDAN INSON HUQUQLARINI TA'MINLASH

Hajiyev Khagani Mohubbat oglu
Chief Expert of the State Expert criminalistics Center of the Ministry of Internal
Affairs Republic of Uzbekistan

PROMOTING HUMAN RIGHTS IN THE CONTEXT OF CYBERSECURITY

Гаджиев Хагани Мохуббат оглы
Главный эксперт Государственного Экспертно-криминалистического Центра
Министерства внутренних дел Республики Узбекистан

ОБЕСПЕЧЕНИЕ ПРАВ ЧЕЛОВЕКА В КОНТЕКСТЕ КИБЕРБЕЗОПАСНОСТИ

Новый Узбекистан – это государство, главной целью которого является обеспечение свободной, благоустроенной и благополучной жизни нашего многонационального народа. Это государство, развивающееся в строгом соответствии с общепризнанными нормами в области демократии, прав и свобод человека, опирающееся на принципы дружбы и сотрудничества с международным сообществом[1].

Стоит отметить, что наряду с развитием и совершенствованием информационно-коммуникационных технологий, наблюдается увеличение количества угроз в киберпространстве, которые могут нанести значительный ущерб правам человека. На сегодняшний день потерпевшими от лиц, совершающих противоправные действия в виртуальном пространстве, могут стать не только люди, предприятия, корпорации, но и целые государства. Необходимо учитывать, что безопасность тысяч пользователей, связанная с персональными данными, банковскими счетами, недвижимостью и т.д. может оказаться в зависимости от нескольких преступников. 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. Таким образом, обеспечение кибербезопасности на сегодняшний день приобретает первостепенное значение.

Т. Тропина признает, что на данный момент новые кибернетические технологии разрабатываются и вводятся намного интенсивней, чем

законодательство или правоохранительные органы способны реагировать на данный рост[2].

Киберпреступность – это преступность, совершаемая в киберпространстве. В целях определения сущности и понятия киберпреступности, необходимо прежде всего установить понятие «киберпространства». Авторы «модельного закона» о киберпреступности Международного Союза Электросвязи (2009 г.) определяют киберпространство как «физическое и нефизическое пространство, созданное и (или) сформированное следующим образом: компьютеры, компьютерные системы, сети, их компьютерные программы, компьютерные данные, данные контента, движение данных, и пользователи»[3].

Ю.В. Гаврилин определяет «киберпреступление» как спектр преступлений в сфере информационных технологий, будь это преступления, совершённые с помощью компьютеров, или преступления, предметом которых являются компьютеры, компьютерные сети и хранящаяся на этих носителях информация[4].

Кибербезопасность можно определить, как деятельность, в соответствии с которой определяется возможность защиты от вредоносного воздействия, путем применения способов и механизмов предотвращения несанкционированного доступа технического, нормативно-правового характера, а также при помощи форм международного сотрудничества. Защита использования информационно-коммуникационных систем от действий, направленных на получения личной и финансовой выгоды[5].

Известен тот факт, что совершаемые киберпреступления наносят значительный ущерб, не только личности, но и экономике различных государств. К примеру, в Германии за 2016 год зарегистрировано около 83 тысяч фактов совершения киберпреступлений, ущерб от которых превысил 51 млн. евро[6], в Великобритании киберпреступниками совершается более чем тысячи кибератак ежечасно. Киберпреступники используют ряд различных схем и программ с целью вымогательства. Различные методы шифрования данных, злоумышленники используют с целью вымогательства денег за выдачу ключей расшифровки[7].

В Республике Узбекистан за 2019 год, в информационных системах и веб-сайтах национального сегмента сети интернет выявлено 268 инцидентов, 816 уязвимостей и порядка 132 000 угроз кибербезопасности.

Использование данных уязвимостей позволяет злоумышленнику получить удаленный доступ к информационной системе или веб-сайта, а также к файлам и информации, что в свою очередь **может привести к утечке персональных данных 2 026 824 граждан Республики Узбекистан**[8].

В киберпространстве могут взломать аккаунт, кроме того, могут произойти и иные правовые обстоятельства, связанные с утечкой личной информации, защитой персональных данных, приватностью частной жизни, личный архив фотографий может оказаться в общем доступе и

киберпреступник, находящийся где-то в другой стране, может потребовать перечисления денежных средств в обмен на возврат доступа к архиву данных.

Необходимо отметить, что подобные воздействия являются латентными, их трудно выявить и доказать, при этом определение ущерба является серьезной проблемой, как и выявление потерпевших. Вышеуказанное обуславливается тем, что проследить большое количество транзакций, инициируемых в ходе хакерского вмешательства и сопровождаемых перемещением электронных денег самого разного происхождения, требует существенных временных затрат, технологий и привлечения большого количества высококвалифицированных технических специалистов. Реализация подобных противоправных вмешательств, как правило, сопряжена с привлечением инсайдеров на уровне разработчиков программного обеспечения электронных платежных систем и привлечения хакеров высоко уровня. Такого рода вмешательства несут потенциальную угрозу национальной безопасности.

В целях противодействия данным преступлениям, а также предотвращения нарушений прав человека и избежание нанесения ущерба экономике страны, государства усилили способы и методы противодействия киберпреступлениям. Китай, США, Великобритания используют способы противодействия киберпреступлений путем установки программ массового наблюдения за гражданами, включающих прослушивание телефонных разговоров, чтение сообщений в мессенджерах и иных технических средств цифрового наблюдения.

Подтверждением факта того, что зарубежные спецслужбы могут получать доступ к личным данным граждан любых государств, является публикация материалов бывшего сотрудника ЦРУ и АНБ США Эдварда Сноудена о злоупотреблении некоторых государств системами массового наблюдения за гражданами[9].

С учетом возможности прямого доступа соответствующих государственных служб к базам данных, следует отметить, наличие положений о трансграничном доступе к компьютерным данным, которые содержатся в международных документах. К примеру, положения Конвенции о преступности в сфере компьютерной информации (Будапешт, 23 ноября 2001 г.) предусматривают возможность трансграничного доступа к компьютерным базам государств-участников Конвенции, посредством получения добровольного согласия лица, обладающего законными полномочиями раскрывать эти данные[10].

Сопоставительный анализ отчетов различных государств, предоставляемых в Комитет по правам человека ООН, на предмет соответствия норм внутреннего права, положениям международной защиты прав человека, показывает, что защита прав человека нуждается не только во внесетевой среде, но также и в виртуальной среде. Соответственно, при обеспечении безопасности и защиты от киберпреступлений, государства прежде всего должны пересмотреть

политику обеспечения кибербезопасности, как государственных учреждений, банков, так и физических лиц, способствуя тем самым уважению и защите основополагающего права на неприкосновенность личной жизни[11].

Глава XX¹ Уголовного кодекса Республики Узбекистан предусматривает ответственность за преступления в сфере информационных технологий. Данная глава рассматривает ряд противоправных деяний в цифровой сфере. Однако на современном этапе развития информационных технологий рамками одного Уголовного кодекса охватить всю сферу виртуальных общественных отношений, которые включают экономические, социальные сферы, вопросы национальной безопасности и т.д., не представляется возможным.

В Республике Узбекистан ведется работа по созданию Национальной стратегии кибербезопасности на 2020–2023 годы. Данный документ предназначен для урегулирования общественных отношений в сфере противодействия преступности в киберпространстве, создание единой системы национальной кибербезопасности и правовой базы в сфере защиты информационной безопасности всех субъектов виртуального пространства от кибератак, усиление комплексных мер по кибербезопасности в стране.

Стратегия направлена на регулирование борьбы с преступностью в национальном виртуальном пространстве, а также формированию правовых основ кибербезопасности.

Проект Указа Президента Республики Узбекистан **«О Государственной программе по реализации Стратегии действий по пяти приоритетным направлениям развития Республики Узбекистан в 2017–2021 годах в «Год развития науки, просвещения и цифровой экономики»** включает в себя вопросы регулирования борьбы с преступностью в национальном киберпространстве, формирования единой системы кибербезопасности и нормативно-правовой базы в области защиты критически важных объектов инфраструктуры от кибератак, комплекс мер по обеспечению кибербезопасности.

Кроме того, на данный момент ведется работа над законом «О кибербезопасности», в котором устанавливаются: механизмы защиты информационных и коммуникационных технологий от современных киберугроз, внедрение современных мер кибербезопасности для систем различного уровня, права государственных органов, предприятий и организаций в сфере кибербезопасности и определяют их обязанности в этой сфере, унификация нормативно-правовых актов в этой области.

В заключении, необходимо отметить, что большинство развитых и развивающихся стран активно разрабатывают и принимают стратегии кибербезопасности поддерживающие и обеспечивающие реализацию стратегии: законы стандарты и другие регламентирующие документы. Одновременно в большинстве уже принятых или обсуждаемых документах

подчеркивается, что решение многих проблем обеспечения безопасности киберпространства требует тесного и активного международного сотрудничества. К сожалению, нормативная база обеспечения кибербезопасности Республики Узбекистан явно недостаточна развития в части, касающейся международного сотрудничества государств и взаимодействия специальных служб зарубежных стран с национальными органами по борьбе с киберпреступлениями.

Библиографические ссылки:

1. Интервью Президента Республики Узбекистан Шавката Мирзиёева главному редактору газеты “Янги Ўзбекистон” Салиму Дониёрову [Электронный ресурс]. – Режим доступа: <https://president.uz/ru/lists/view/4547>.
2. Tropina T. Self – and Co-regulation in Fighting Cybercrime and Safeguarding Cybersecurity. In: Jähnke at al. (eds., «Current Issues in ITU Security» – Duncker & Humblot, Berlin, 2012. – P. 155.
3. Номоконов В.А., Тропина Т.Л. Киберпреступность как новая криминальная угроза // Криминология: вчера, сегодня, завтра. – 2012. – № 1 (24). – С. 45–55.
4. Гаврилин Ю.В. Преступления в сфере компьютерной информации: квалификация и доказывание: Учебное пособие. – М.: ЮИ МВД РФ, 2003 – С. 245.
5. Права человека и кибербезопасность: виртуальная нереальность? [Электронный ресурс] – Режим доступа: <https://www.securitylab.ru/contest/504222.php>. – Дата доступа: 09.12.2020 г.
6. В 2016 году в Германии резко возросла киберпреступность. [Электронный ресурс] – Режим доступа: <https://www.dw.com/ru/v-2016-godu-v-germanii-rezko-vozroslo-kiberprstupnost> – Дата доступа: 09.12.2020 г.
7. Режим доступа: HM Government национальная стратегия кибербезопасности 2016–2021. [Электронный ресурс] – Режим доступа: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/643426/Russian_translation_-_National_Cyber_Security_Strategy_2016 – Дата доступа: 09.12.2020 г.
8. Кибербезопасность Республики Узбекистан: итоги 2019 года (обзор) - Режим доступа: <https://review.uz/post/kiiberbezopasnost-respubliki-uzbekistan-itogi-2019-goda> – Дата обращения: 09.12.2020 г.
9. УНП ООН Управление Организации Объединенных Наций по наркотикам и преступности. / Всестороннее исследование проблемы киберпреступности Проект, февраль 2013 года. – Режим доступа: http://www.unodc.org/documents/organized-crime/cybercrime/Cybercrime_Study_Russian.pdf – Дата обращения: 09.12.2020 г.
10. Серия Европейских договоров. / Конвенция о компьютерных преступлениях. Будапешт, 23.XI.2001 г. / – Режим доступа: <https://rm.coe.int/1680081580>. / – Дата обращения: 09.12.2020 г.

11. «Права человека и кибербезопасность: виртуальная нереальность? Электронный ресурс – Режим доступа: <https://www.securitylab.ru/contest/504222.php>. – Дата обращения: 09.12.2020 г.
12. Узбекистан разработает национальную стратегию кибербезопасности на 2020–2023 годы. – Режим доступа: <https://review.uz/post/uzbekistan-razrabotaet-nacionalnuyu-strategiyu-kiberbezopasnosti-na-2020-2023-god>. / Дата обращения: 09.12.2020 г.
13. А.Расулев. "ПРОТИВОДЕЙСТВИЕ КИБЕРТЕРРОРИЗМУ: МЕЖДУНАРОДНО-ПРАВОВЫЕ И УГОЛОВНО-ПРАВОВЫЕ АСПЕКТЫ" Review of law sciences, no. 4, 2018, pp. 92-95. doi:10.24412/2181-1148-2018-4-92-95