МЕЖДУНАРОДНОЕ СОТРУДНИЧЕСТВО – НЕОБХОДИМОЕ УСЛОВИЕ ЭФФЕКТИВНОСТИ ОБЕСПЕЧЕНИЯ КИБЕРБЕЗОПАСНОСТИ НА НАЦИОНАЛЬНОМ УРОВНЕ

Якубов Александр Санджарович
доктор юридических наук, профессор

Азим Шухрат
заместитель начальника Исследовательского института Криминологии Республики Узбекистан,
доктор философии по юридическим наукам

Аннотация. *В статье описывается международное сотрудничество как необходимое условие эффективности обеспечения кибербезопасности на национальном уровне. В частности констатируется состояние киберпреступности и её криминальные проявления, приводится соответствующая статистика, причинённый ущерб, методы и разновидности кибератак, программы-вымогатели, которые представляют серьезную угрозу как для отдельных лиц, так и для организаций в целом.*
Ключевые слова: *киберпреступность, кибербезопасность, фишинг, интернет, организованная преступность.*

Abstract. *The article describes international cooperation as a necessary condition for the effectiveness of ensuring cybersecurity at the national level. In particular, the state of cybercrime and its criminal manifestations are noted, along with relevant statistics, the damage caused, methods and types of cyberattacks, and ransomware, which pose a serious threat both to individuals and organizations as a whole.*
Keywords: *cybercrime, cybersecurity, phishing, Internet, organized crimeprevention, socially oriented activities.*

Тенденции преступности сложны и противоречивы, что особенно наглядно выявляется при исследовании ее динамики за значительные промежутки времени. Влияние оказывают многие факторы. Одним из таких факторов выступает научно-технический прогресс и происходящие в его рамках интеллектуально-промышленные поистине революционные изменения, влекущие как появление новых сфер общественных отношений, так и усложнение уже функционирующих. При этом, что уже подтверждено практикой, научно-технический прогресс и все его составляющие обладают сильной деликтогенностью, постоянно вызывая к жизни всё новые и новые составы правонарушений, усложняя и делая более опасными уже традиционно известные. Это напрямую относится и киберпространству, в котором с геометрической прогрессией происходят постоянные трансформации, причем не только положительного свойства, но и отрицательно влияющих на функционирующие в социальной жизни общественные отношения. Всё это актуализировало проблему необходимости обеспечения охраны, профилактирования и предупреждения посягательств, осуществляемых в киберпространстве, общепризнанно обозначаемых большинством ученых и практикующих юристов как самостоятельное явление современности – киберпреступность.

Об усложнении криминогенной обстановки в киберпреступности и нарастании криминальных проявлений в этой сфере, свидетельствует значительный рост жертв от кибератак, причем как физических, так и юридических лиц, не говоря уже об имиджевых потерях государственных и других структур власти, суммы как прямых, так косвенных финансовых потерь и убытков. Так, в 2021 году количество кибератак во всем мире увеличилось на 125% по сравне

нию с 2020 годом, и в 2022 году растущий объем кибератак продолжал угрожать предприятиям и частным лицам. В 2023 году 50% предприятий Великобритании подверглись в той или иной форме кибератакам, против 39% в 2022 году. В первой половине 2022 года во всем мире произошло около 236,1 миллионов атак с использованием программ-вымогателей. Каждый год незаконно вскрывается около 1 миллиарда электронных писем, что затрагивает каждого пятого интернет-пользователя. Средняя сумма убытков предприятий от утечек данных ежегодно колеблется в пределах 4-4,5 миллионов долларов США и по существу ни одно из предприятий не застраховано от кибератак. Реальность угроз кибератак, возрастающая стоимость утечек данных, обусловили формирование достаточно трезвого и пристального внимания к сфере кибербезопасности. Так, почти 73% представителей малого и среднего бизнеса полагают необходимым уделять внимание этой проблематике, а 78% признали целесообразным увеличение средств и инвестиций в кибербезопасность.

При этом, несмотря на то, что 67% представителей малого и среднего бизнеса объективно признают, что у них нет внутренних условий по предотвращению утечки данных, они пытаются воздействовать на эти процессы посредством пользования услугами профессионалов, поставщиков таких услуг в сфере кибербезопасности. Об осознании важности такой деятельности свидетельствует тот факт, что если в 2020 году такими услугами пользовалось 74% предпринимателей, то к 2022 году эта цифра выросла до 89%. В криминологическом исследовании 2022 года, охватившем США, Канаду, Великобританию, Австралию и Новую Зеландию, 76% респондентов отмечали, что их организация пострадала в этом году как минимум от одной кибератаки, тогда как в 2020 году такие атаки отмечали только 55% респондентов. При этом, лишь 30% организаций из опрошенных констатировали наличие киберстрахования. В опубликованных источниках приводятся сведения об атаках на организации по континентам за 2021 год в процентном отношении по количеству: Азия - 26%; Европа - 24%; Северная Америка - 23%; Ближний Восток и Африка - 14%; Латинская Америка-13%.

Следует констатировать растущие издержки киберпреступности, поскольку методы атак становятся все более изощренными и профессиональными. Это побуждает организации по всему миру инвестировать дополнительные средства и ресурсы в современные меры безопасности, включая обновленные программы обучения персонала, введение штата специальных сотрудников по киберпреступности и др. По оценкам специалистов, средняя стоимость одного кибернарушения в 2020 году оценивалась в 4,35 миллионов долларов США. Констатируется, что киберпреступность обойдется мировой экономике примерно в 7 триллионов долларов США. В 2022 году прогнозируется, что к 2025 году эта цифра возрастет до 10,5 триллионов долларов США.

В мировом сообществе, с учетом накопленного опыта, констатируется несколько преступных проявлений киберпреступности. Самой распространённой киберугрозой, с которой сталкиваются организации и частные лица, является фишинг[1]. В 2021 году 323 972 интернет-пользователей сообщили о том, что стали жертвами фишинговых атак, что по разным оценкам составляет почти половину пользователей, пострадавших от утечки данных. В этот период констатировано около одного миллиарда электронных писем, которые затронули каждого пятого пользователя интернета.

Фишинг является наиболее распространенной формой кибератак, поскольку подтверждено, что ежедневно отправляется около 3,4 миллиарда спам-писем. Фишинг зачастую представляет собой атаку «входа», когда киберпреступники собирают конфиденциальную информацию (например, данные для ввода или номера кредитных карт), которую затем возможно использовать для запуска дальнейших атак. Установлено,

[1] Фишинг – вид интернет мошенничества, целью которого является получение доступа к конфиденциальным данным пользователя - логинам и паролям. Это достигается посредством проведения массовой рассылки электронных писем от имени популярных брендов, а также личных сообщений внутри различных серверов (например, от имени банков или внутри социальных сетей).

что фишинг является наиболее распространенной точкой входа для атак с использованием программ-вымогателей, когда рассылается спам будущим жертвам до тех пор, пока адресат не перейдет по соответствующей ссылке, которая может содержать программу-вымогатель или перенаправить ее на поддельный веб-сайт, где потерпевший вольно или невольно вводит свои данные для входа. Эти данные впоследствии используются для получения внутреннего доступа к сети, либо эскалации своей атаки и внедрения программы-вымогателя.

Одной из разновидностей кибератак являются программы-вымогатели, которые представляют серьезную угрозу как для отдельных лиц, так и для организаций, посредством которых, потерпевших вынуждают платить. В первой половине 2022 года по всему миру было зарегистрировано около 236,1 миллиона атак с использованием программ-вымогателей.

Распространенным является шантажирование потенциальных жертв посредством угроз публикации конфиденциальных фотографий, видео или иной информации, связанной с сексуальными действиями, при условии невыполнения определенных противоправных действий (Sextortion). Так, по данным Департамента IC3 США, в 2021 году поступило более 18 тысяч жалоб, связанных с сексуальным вымогательством, а убытки пострадавших составили более 13,6 миллионов долларов США.

К числу разновидностей киберпреступности относятся финансовое мошенничество, мошенничество в розничной торговле и продаже потребительских товаров, любовные аферы, взлом деловой электронной почты, киберпреследования, киберклевета, кража личных данных, взлом социальных сетей, романтические аферы, и др.

Весьма распространенным стали атаки на «цепочки поставок». Цепочки поставок становятся все более взаимосвязанными и сложными по мере совершенствования технологий. Такая связь представляет определенные риски, если предприятия и организации незащищены должным образом, что повышает уязвимость безопасности партнёров. Киберпреступники нацелены на эти уязвимости, и до 40% киберугроз происходит косвенно, именно через цепочку поставок.

Здесь провоцирующими выступают как человеческий фактор – недостаточный мониторинг партнеров и поставщиков в режиме реального времени на предмет рисков кибербезопасности, так и недостаточное внимание компаний в инвестиции в систем безопасности, включая современное программное обеспечение и специальных подразделений, обеспечивающих безопасное функционирование предприятия.

В современной литературе киберпреступность условно подразделяют на две категории:

а) киберзависимая преступность, то есть преступления, которые можно совершить только с использованием технологий, когда устройства являются как инструментом совершения преступлений, так и его целью (вредоносные программы, взломы с целью удаления или повреждения данных и др.);

б) традиционная преступность, расширившая своё влияние за счет использования современных технологии (кибермошенничество, кражи и др.).

Достаточно распространённым преступлением, совершаемым с использованием интернета, является мошенничество. Риски, сопряжённые с возможностью быть вовлечённым в различного рода мошеннические схемы, возникают при инвестировании денежных средств на иностранных фондовых рынках с использованием сети интернет. Распространенной разновидностью мошенничества являются звонки по телефону, когда предпринимаются попытки у владельцев банковских карт получения конфиденциальной информации, осуществить перевод либо установить программы удаленного доступа.

Другой вид мошенничества осуществляется на интернет-аукционах, когда сами продавцы завышают ставки с тем, чтобы поднять цену выставленного на аукцион товара. Продажа доменных имён, как разновидность кибермошенничества заключается в массовой рассылке электронных сообщений, в которых, например, сообщается о попытках неизвестных лиц зарегистрировать доменные имена, похожие на принадлежащие адресатам сайты, с предложениями о регистрации ненужное адресатам доменного имени, с целью их опережения.

Для полноты криминологической характеристики киберпреступности важно акцентировать внимание на профессиональном характере преступных посягательств, на безопасность в сфере информационных технологий. Основываясь на этом предварительном замечании следует констатировать, что с криминологической, и с уголовно-правовой позиции, мы имеем дело с таким явлением современности, как организованная преступность. В литературе отмечается, что организованная преступность «… являясь одной из форм преступности, характеризуется высокой комплексной общественной опасностью и проявляется в системе деятельности всех преступных организаций данного региона за определенный период» [1, С.309], либо «…обладающая высокой степенью общественной опасности форма социальной патологии, выражающаяся в постоянном и относительно массовом воспроизводстве и функционировании устойчивых преступных сообществ (преступных организаций)» [2, С.17].

Представляется что, наиболее существенными признаками организованной преступности являются:

а) наличие преступных организаций (объединений) различной степени сплоченности, имеющих функционально - иерархическую структуру со строгой субординацией и координацией функций между лицами или группами;

б) наличие профессионалов, для которых преступная деятельность является основной формой существования и образа жизни;

в) устойчивый, планируемый, законспирированный характер преступной деятельности;

г) наличие систем обеспечения преступной деятельности, собственной безопасности и нейтрализации социального контроля;

д) значительные денежные фонды, инвестируемые в преступную деятельность, легальный бизнес, доходы от которого направляются на коррумпирование государственных чиновников, материальную поддержку осужденных и т.д.;

е) прогрессирующая тенденция к расширению сфер преступной деятельности и влияния преступных организаций;

ж) антиобщественная идеология, своего рода «кодекс» поведения.

По мнению Э.Ф. Побегайло, к наиболее типичным признакам организованной преступности относятся: участие значительного числа лиц; устойчивость криминальных связей между членами групп; наличии специфических норм и правил поведения в среди её функционеров; специализация преступной деятельности; её предумышленный и заранее спланированный характер; иерархическая структура преступных групп и распределение ролей их участников; систематический преступный бизнес (промысел); межрегиональные связи; повышенная конспиративность; коррумпирование представителей власти и некоторые другие.

С позиции нашего анализа важно подчеркнуть, что киберпреступность в обязательном порядке характеризуется и международными связями.

Представляется правильным выделение двух разновидностей организованной преступности: общеуголовной и хозяйственно-экономической, последняя из которых, образуя разновидность профессиональной преступности, непосредственно свойственна и должна характеризировать киберпреступность.

Таким образом, преступления в сфере информационных технологий предполагают, как распространение вредоносных программ, взлом паролей, кражу номеров банковских карт и других банковских реквизитов, фишинг, так и распространение противоправной информации (клеветы, материалов порнографического характера, материалов, направленных на возбуждение межнациональной и межрелигиозной вражды и т.п.) через Интернет, а также вредоносное вмешательство через компьютерные сети в работу различных систем.

Как показывает практика, преступления в сфере информационных технологий имеют международный характер, поскольку, как правило, совершаются на территории нескольких государств, что актуализирует значение международного сотрудничества.

В качестве правовой основы международного сотрудничества в сфере борьбы с киберпреступностью может служить Конвенция Совета Европы о преступности в сфере

компьютерной информации (ETS №185), подписанная 23 ноября 2001 года в Будапеште [3]. Она открыта для подписания как государствами-членами Совета Европы, так и странами, которые не являются членами, но которые приняли участие в составлении и во вступлении других стран не членов.

Конвенция Совета Европы о компьютерных преступлениях (ETS №185) подразделяет преступления в киберпространстве на четыре группы.

Первую группу преступлений, направленных против конфиденциальности, целостности и доступности компьютерных данных и систем, входят: незаконный доступ (ст.2), незаконный перехват (ст.3), воздействие на компьютерные данные (противоправное преднамеренное повреждение, удаление, ухудшение качества, изменение или блокировка компьютерных данных) (ст.4) или системы (ст.5).Также в эту группу преступлений входит противозаконное использование специальных технических устройств (ст.6) - компьютерных программ, разработанных или адаптированных для совершения преступлений, предусмотренных в ст.ст. 2-5, а также компьютерных паролей, кодов доступа, их аналогов, посредством которых может быть получен доступ к компьютерным системам в целом или любой ее части. Нормы ст. 6 подлежат применению только в случаях, если использование (распространение) специальных технических устройств направлено на совершение противоправных деяний.

Во вторую группу входят преступления, связанные с использованием компьютерных средств. К ним относятся подлог и мошенничество с использованием компьютерных технологий (ст.ст.7,8). Подлог с использованием компьютерных технологий включает в себя злонамеренные и противоправные ввод, изменение, удаление или блокирование компьютерных данных, влекущих за собой нарушение аутентичности данных, с намерением, чтобы они распространялись или использовались в юридических целях в качестве аутентичных.

Третью группу составляет производство (с целью распространения через компьютерную систему), предложение и (или) предоставление в пользование, распространение и приобретение порнографии и детской порнографии, а также владение детской порнографии, находящейся в памяти компьютера (ст.9).

Четвёртую группу составляют преступления, связанные с нарушением авторского права и смежных прав.

В начале 2002 года был принят Протокол № 1 к Конвенции о киберпреступности, в соответствии с которым к категории преступлений было отнесено 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.

В соответствии с положениями Конвенции, каждое государство-участник обязано создать необходимые правовые условия для предоставления следующих прав и обязанностей компетентным органам по борьбе с киберпреступностью: выемка компьютерной системы, её части или носителей; изготовление или конфискация копии компьютерных данных; обеспечение целостности и сохранности хранимых компьютерных данных, относящихся к делу; уничтожение или блокирование компьютерных данных, находящихся в компьютерной системе.

Конвенция также определяет создание необходимых условий для обязанности интернет-провайдеров проведения необходимого сбора и фиксации или перехвата 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 Республике Узбекистан сформирована правовая основа борьбы с киберпреступностью. В соответствии с Законом Республики Узбекистан от 25 декабря 2007 года (ЗРУ-137) [4, С. 532]. Уголовный кодекса был дополнен самостоятельной Главой XX[1], предусматривающей ответственность за преступления в сфере информационных технологий, а в некоторые другие статьи Особенной части были включены в качестве квалифицирующих и особо квалифицирую-

щих признаков преступления, совершаемые с использованием средств компьютерной техники, сетей телекоммуникаций, а также всемирной информационной сети Интернет.

По УК РУз преступлениями в сфере компьютерной информации являются: нарушение правил информатизации (ст. 278[1]), незаконный (несанкционированный) доступ к компьютерной информации (ст. 278[2]), изготовление с целью сбыта либо сбыт и распространение специальных средств для получения незаконного (несанкционированного) доступа к компьютерной системе, а также к сетям телекоммуникаций (ст. 278[3]), модификация компьютерной информации (ст. 278[4]), компьютерный саботаж (ст. 278[5]), создание, использование или распространение вредоносных программ (ст. 278[6]), незаконный (несанкционированный) доступ к сети телекоммуникаций (ст. 278[7]).

Данная группа посягательств является институтом Особенной части, отнесённой по родовой принадлежности к преступлениям против общественного порядка и общественной безопасности. Видовым объектом выступает общественная безопасность при непосредственном посягательстве на общественные отношения, связанные с безопасностью информации и систем обработки информации с помощью ЭВМ. Общественная опасность противоправных действий в области электронной техники и информационных технологий выражается в том, что они могут повлечь за собой нарушение деятельности автоматизированных систем управления и контроля различных объектов, серьёзное нарушение работы сетей телекоммуникаций, несанкционированные действия по уничтожению, модификации, искажению, копированию информации и информационных ресурсов, иные формы незаконного вмешательства в информационные системы, которые способны вызвать тяжкие и необратимые последствия, связанные не только с имущественным ущербом, но и физическим вредом людям.

В соответствии с Законом Республики Узбекистан от 13 июня 2017 года (ЗРУ-436) [5] такое преступление против жизни как доведение до самоубийства (ст.103 УК) была дополнена квалифицирующим признаком, повышающим ответственность, если доведение до самоубийства или покушение на него путём угроз, жестокого обращения или систематического унижения чести и достоинства личности лица осуществлялось с использованием сетей телекоммуникаций, а также всемирной информационной сети Интернет. Этим же Законом склонение к самоубийству (ст.103_1 УК) было криминализировано, а использование при этом сетей телекоммуникаций и всемирной информационной сети Интернет оценено законодателем как квалифицированный состав.

Корректировке подверглись и некоторые преступления в сфере экономики, представляющие хищения чужого имущества. В нормах, предусматривающих ответственность за хищение путем присвоения или растраты (ст. 167), мошенничество (ст. 168), кражу (ст. 169) предусматривается повышенная ответственность, если они совершены с использованием средств компьютерной техники или с несанкционированным проникновением в компьютерную систему.

Необходимость действенной охраны отношений в сфере хозяйственной деятельности обусловило установление уголовной ответственности за незаконную деятельность по привлечению денежных средств и (или) иного имущества (ст.188[1]) [6], где в качестве конструктивного и квалифицирующего предусмотрен признак «с использованием средств массовой информации либо коммуникаций, а также всемирной информационной сети Интернет».

Следует отметить как позитивное в законодательном процессе своевременное реагирование и установление уголовной ответственности за использование или хранение с целью распространения материалов, содержащих идеи религиозного экстремизма, сепаратизма и фундаментализма, призывы к погромам или насильственному выселению граждан либо направленных на создание паники среди населения, а также изготовление, хранение с целью распространения либо демонстрации атрибутики или символики религиозно-экстремистских, террористических организаций, а равно распространение таких сведений либо использование религии в целях нарушения гражданского согласия, распространение клеветнических, дестабилизирующих об-

становку измышлений и совершение иных действий, направленных против установленных правил поведения в обществе и общественной безопасности (ч. 1.2. ст. 244[1] УК), отягощённые тем, что эти действия осуществлялись с использованием средств массовой информации либо сетей телекоммуникаций, а также всемирной информационной сети Интернет (п.«г» ч.3. ст. 244[1] УК).

В современном, постоянно меняющемся мире, совершенствование технологий, необходим постоянный мониторинг как со стороны технических специалистов, так и со стороны правоведов. Совершенствующиеся методы криминальных проявлений в сфере кибербезопасности требуют своевременного реагирования и в первую очередь на законодательном уровне. Так, например, получающие всё большую распространённость технологии Deepfake, посредством которых с помощью искусственного интеллекта (ИИ) создают ложные видеообращения, генерации похожести голосов с целью осуществления мошеннических действий уже сегодня требует законодательного реагирования.

Общепризнанно, что преступления в сфере информационных технологий очень часто является международными. Учитывая это, следует обратить внимание на такой институт Общей части УК как действие уголовного закона в пространстве. В международной законотворческой практике наряду с территориальным, гражданства и универсальным принципами действия уголовного закона в пространстве, которые присуще и законодательству Узбекистана, предусматривается также и реальный принцип. Как отмечается в литературе, сущность реального принципа действия уголовного закона в пространстве состоит в том, что государство признаёт возможным привлечение к уголовной ответственности иностранных граждан и лиц без гражданств или без гражданства, постоянно не проживающих на его территории, за преступления, направленные против интересов этого государства даже если эти преступления не совершены на его территории и не предусмотрены международными договорами [7]. Поскольку при киберпреступности нередки случаи совершения посягательств на интересы республики Узбекистан и его граждан вне пределов и территории нашего государства необходимо распространить действия УК РУз и на такие криминальные проявления. На основании изложенного предлагается новая редакция ч.3 статьи 12 УК: «иностранные граждане и лица без гражданства, не проживающие постоянно на территории Республики Узбекистан, подлежат уголовной ответственности по настоящему Кодексу в случаях, если преступление направлено против интересов Республики Узбекистан, и в случаях, предусмотренном международном договором Республики Узбекистан, если они не были осуждены в иностранном государстве и привлекаются к уголовной ответственности на территории Республики Узбекистан».

Использованные источники

1. Уголовное право. Общая часть. – Т., Академия МВД Республики Узбекистан, 2005. – С.309.
2. Побегайло Э.Ф. Тенденции современной преступности и совершенствование уголовно-правовой борьбы с нею. М., 1990. – С.17.
3. The Convention on Cybercrime (Budapest Convention, ETS No. 185) and its Protocols https://www.coe.int/en/web/cybercrime/the-budapest-convention
4. Собрание законодательства Республики Узбекистан, 2007 г., № 52, ст.532.
5. Собрание законодательства Республики Узбекистан, 2017 г., № 24. Ст.487.
6. Собрание законодательства Республики Узбекистан от 23 сентября 2016 года № ЗРУ-411.
7. Уголовное право. Общая часть. – Т., 2005. – С.112.