ҚЫЛМЫСТЫҚ ҚҰҚЫҚ ЖӘНЕ КРИМИНОЛОГИЯ, ҚЫЛМЫСТЫҚ-АТҚАРУШЫЛЫҚ ҚҰҚЫҚ / УГОЛОВНОЕ ПРАВО И КРИМИНОЛОГИЯ, УГОЛОВНО-ИСПОЛНИТЕЛЬНОЕ ПРАВО

УДК 34.03:[002:004]
МРНТИ- 10.19.65

КАЛИЕВ АСКАР АБУЖАНОВИЧ[1]
[1]*Академия правоохранительных органов при Генеральной прокуратуре Республики Казахстан, г. Астана, Республика Казахстан*

КИБЕРПРЕСТУПНОСТЬ – НОВАЯ ГЛОБАЛЬНАЯ УГРОЗА.

Түйін. Мақала авторы киберқылмыстың таралу себептерін, кибершабуылдың даму кезеңдерін, бар киберқауіптер туралы және интернеттегі қылмысқа қарсы күрес жөніндегі шараларды талқылайды.

Киберқылмысты дамытуға заманауи технологиялардың әсер ету мәселелері қаралды, осы саладағы ең көп таралған қылмыстардың мысалдары келтірілген.

Киберқауіпсіздік мәселелерімен айналысатын компаниялардың зерттеу нәтижелері зерттелді.

Түйінді сөздер: ақпараттық-коммуникациялық технологиялар, киберқылмыс, IT-технологиялар, интернет, желі, Интернет қылмыс, компьютерлік қылмыс, кибершабуылдар, ботнет.

Аннотация. В статье автором рассматриваются причины распространения киберпреступности, этапы развития кибератак, говорится о существующих киберугрозах и принимаемых мерах по борьбе с интернет преступностью.

Рассмотрены вопросы влияния современных технологий на развитие киберпреступлений, приведены примеры самых распространенных преступлений в данной сфере и исследования компаний, занимающихся вопросами кибербезопасности.

Ключевые слова: информационно-коммуникационные технологии, киберпреступность, IT-технологии, интернет, сеть, интернет-преступность, компьютерная преступность, кибератаки, ботнет.

Annotation. In the article the author examines the reasons for the spread of

cybercrime, the stages of the development of cyber attacks, talks about existing cyber threats and measures taken to combat Internet crime.

The issues of the influence of modern technologies on the development of cybercrime are considered, examples of the most common crimes in this sphere are given.

The research results of companies dealing with cybersecurity issues are examined.

Key words: information and communication technologies, cybercrime, IT-technologies, the Internet, a network, Internet crime, computer crime, cyberattacks, a botnet.

Стремительное развитие информационно - коммуникационных технологий способствовали широкому распространению интернета, который открыл человечеству не только новые возможности для саморазвития, но и создал благоприятные условия для совершения преступлений в сети.

Существует много различных определений такого вида преступления как киберпреступность.

Некоторые исследователи понимают киберпреступность, как несанкционированное проникновение в работу компьютерных сетей, компьютерных систем и программ, с целью видоизменения компьютерных данных [1].

Специалисты Международного союза электросвязи относят к киберпреступности все преступления, совершенные в киберпространстве [2].

Нет единого подхода к данному термину и среди ученых. Одни считают киберпреступностью преступления, совершенные в рамках компьютерной сети, например, Суслопаров А.В. [3].

Другие относят к данному определению и преступления, совершенные при помощи сотовых телефонов, имеющих доступ к сети интернет. К ним можно отнести таких ученых как Дуленко В.А, Мамлеев Р.Р., Пестриков В.А. [4].

В исследовании, проведенном Управлением ООН по наркотикам и преступности по данной проблеме вовсе отмечено, что нет необходимости давать единое определение данному негативному явлению [5].

Но наиболее полное определение киберпреступности, по нашему мнению, все же предложено в научной работе Тропиной Т.Л, которая определяет ее как совокупность преступлений, совершаемых в киберпространстве с помощью или посредством компьютерных систем или компьютерных сетей, а также иных средств доступа к киберпространству, в рамках компьютерных систем или сетей, и против компьютерных систем, компьютерных сетей или компьютерных данных [6].

Киберпреступность – это глобальная проблема, не имеющая границ.

По мнению руководителя Российской Ассоциации Электронных Коммуникаций С.Плуготаренко, в разных точках земного шара работают около 40 миллионов киберпреступников, ущерб от действий которых оценивается в 500 миллиардов долларов. При этом количество вирусных атак в мире растёт по 3 процента в месяц, атак на веб-сервисы - по 2,5 процента, а число краж денег с различных устройств или электронных кошельков - по 3,5 процента [7].

Более того несмотря на постоянный рост киберпреступлений, раскрываемость их по-прежнему остается очень низкой.

Так, по мнению специалиста по кибернетике и системе управления, автора многих публикаций в области развития информационно-коммуникационных технологий В.П.Филимонова, раскрываемость киберпреступлений в мире составляет не более 3-4% [8].

Учитывая значительный материальный ущерб, наносимый киберпреступниками экономике разных стран, их предпринимателям и гражданам, правоохранительные органы во всем мире выдвигают киберпреступность на первое место среди основных видов преступлений.

Чтобы оценить масштабы ее распространения в мире приведем статистику результатов проведенного в 2017 году компанией Symantec исследований по кибербезопасности, опубликованных в отчете Norton Cyber Security Insights Report. Согласно данного отчета только за 2017 год от действий киберпреступников пострадало около 1 млрд. пользователей всемирной паутины. Причиненный им материальный ущерб составил 172 млрд. долларов США [9].

Что же так повлияло на рост и широкое распространение киберпреступлений?

На наш взгляд, одними из основных причин являются увеличение количества пользователей интернета, безнаказанность, анонимность, безопасность и легкость заработка.

Так, например, риск распространения вредоносных программ (вирусов) возрастает с *увеличением количества пользователей* всемирной паутины, большинство из которых не придают особого значения защите своих персональных компьютеров, смартфонов или планшетов.

Этот факт признает один из ведущих экспертов в области информационной безопасности Е. Касперский, который называет рост числа пользователей интернета одной из главных причин, влияющих на рост киберпреступности.

По данным международного агентства We Are Social, опубликованном в отчете Global Digital 2018, в настоящее время в мире уже насчитывается более 4-х миллиардов пользователей сети, что соответствует 52 % всего населения мира [10].

Ожидается, что в текущем году число устройств, подключенных к сетям с интернет-протоколом (IP), будет почти в два раза превышать

численность всего населения мира [11].

Безнаказанность характеризуется отсутствием для преступника негативных последствий. С момента появления компьютера стали появляться первые в истории вычислительных систем электронные правонарушения, которые с ростом научно-технического прогресса постоянно эволюционируют.

При этом большинство стран не обладало той нормативной базой, позволяющей органам правопорядка привлекать виновных лиц к ответственности.

Современные киберпреступники выбирают местом совершения преступлений те точки земного шара, где менее развита нормативно-правовая база и широко используется сеть интернет.

Анонимность стала третьей по значимости причиной развития киберпреступности. Большая часть пользователей сети интернет предпочитают оставаться анонимными и это не случайно, поскольку деятельность многих из них остается вне правового поля.

Безопасность. Отсутствие систем информационной защиты или недостаточная их работоспособность подталкивало определенную группу людей, вовлеченных в среду развития IT-технологий, проникнуть в компьютерную систему, причиняя порой материальный ущерб ее владельцу. При этом риск быть пойманным на месте совершения преступления был минимальным или вообще отсутствовал в виду нахождения правонарушителя далеко от потерпевшего.

И завершающим условием «популяризации» киберпреступности стала *легкость заработка,* ставшей движущей силой по привлечению людей в преступную среду.

Еще в начале 2010 года Е. Касперский заявил, что киберпреступность превратилась в прибыльный и хорошо организованный бизнес [8].

Все эти факторы стали точкой отсчета при постепенном переходе основных традиционных видов преступлений в киберпространство.

И с каждым новым шагом, действия киберпреступников все более совершенствуется. Начиная от простейших взломов телефонной сети, первых компьютеров, разработки простейших вредоносных программ до захвата компьютеров по всему миру, блокирования операционных систем, хищение денег и личных данных.

Шагая в ногу со временем, киберпреступники всегда стараются найти способы обойти системы защиты от хакерских атак. И в большинстве случаев им это удается.

Так, в 2008 году вирус «Conficker» был установлен более чем в 12 млн. компьютеров по всему миру. Он проникал в операционную систему компьютера потерпевшего и передавал злоумышленнику все данные, хранящиеся на нем.

В 2011 году вследствие самой большой DDoS-атаки на сервера компании «PSN», были похищены личные сведения ее клиентов (реквизиты банковских карточек, анкетные данные, почтовые адреса).

В 2013 году наблюдалось снижение скорости работы интернета, пользователи которого несколько дней не имели возможность попасть на популярные сайты.

В 2016 году в разных странах на определенное время приостанавливалась работа некоторых финансовых организаций, что привело к значительным финансовым потерям.

2017 год стал запоминающимся в истории кибератак, когда большинство пользователей сети Интернет столкнулись с проблемой доступа к своим данным.

Компьютерные программы вымогатели-шифровальщики через почтовые сервисы и зараженные веб-ресурсы проникали в операционную систему и блокировали работу пользователей, передавая дальше вредоносный код по сети.

Для разблокировки системы злоумышленники требовали перечислить на их счет деньги и многие выполняли их условие.

Их жертвами стали крупные компании, организации и простые граждане.

В тот же период средства массовой информации разных стран отмечали факты утечки конфиденциальных сведений и рост интернет мошенничества.

Так, например, в результате кибератак на американскую компанию «Equifax», в руки злоумышленников попали личные сведения о ее клиентах *(анкетные данные, страховка и т.д.)* [12].

Современные киберпреступники уже активно используют новые технологии для совершения правонарушений в киберпространстве.

Например, применяемые ими такие инструменты как "ботнеты" (сеть зараженных вредоносной программой компьютеров, позволяющая удаленно управлять ими), захватывают сотни, а порой и тысячи компьютеров пользователей сети интернет, заставляя их подчиняться действиям преступников.

С началом популяризации криптовалюты, их целью стали обычные пользователи всемирной паутины, которые порой даже не догадывались, что оказывают им помощь в добыче виртуальной валюты и инфицировании других компьютеров.

Большую популярность в текущем году приобрел искусственный интеллект, заинтересованность в котором стали проявлять и киберпреступники. Используя специальную программу, которая сама выбирала получателя, они осуществляли рассылку фишинговых писем.

Такой метод оказался более эффективным и безопасным для злоумышленников. В своем отчете специалисты в области использования искусственного интеллекта описали основные риски, связанные с развитием машинного обучения [13].

Следующим шагом преступников, по мнению экспертов организации Cloud Security Alliance могут стать атаки на организации, оказывающие услуги в сфере облачных хранений информации,

большая часть которой составляет конфиденциальные сведения [14].

Если такие крупные компании как «Google», «Amazon» и «IBM», имеют возможность защитить свои ресурсы, то иные компании или простые граждане становятся более уязвимыми.

Приведенные данные, очередной раз доказывают актуальность вопросов противодействия киберпреступности и необходимость усиления мер безопасности.

Безусловно, каждое уважающее себя государство, обязано применять организационно-технические и правовые меры предупреждения кибератак и их последствий.

Так, одним из важных документов принятых в области защиты информационной безопасности в Казахстане является концепция «Киберщит Казахстан».

Данный программный документ предусматривает вопросы повышения уровня защищенности национальной информационно-коммуникационной инфраструктуры от внешних и внутренних угроз. Принимаются меры по усилению кадрового потенциала правоохранительных органов путем повышения их профессионального уровня в области расследования киберпреступлений.

Большинство таких преступлений остаются не раскрытыми, ввиду не полной готовности наших правоохранительных органов противостоять ее развитию и распространению.

На сегодняшний день следственно-оперативные подразделения органов внутренних дел испытывают недостаток кадровых специалистов, разбирающихся в IT-технологиях, что является одной из причин слабой раскрываемости интернет преступлений.

В этой связи, одной из задач деятельности Регионального Хаба по противодействию глобальным угрозам, созданного в Академии правоохранительных органов, является обучение и проведение научных исследований по противодействию киберпреступности.

В рамках работы Регионального Хаба, по вопросам информационной кибербезопасности были разработаны программы обучения разных уровней сложности, а также проведено 2 семинара-тренинга (в том числе международный), 1 круглый стол.

В октябре 2017 года на базе Регионального Хаба стартовал проект по подготовке национальных экспертов в области расследования преступлений, совершенных посредством сети интернет. После прохождения обучения эксперты из числа сотрудников правоохранительных органов смогут передавать знания своим коллегам.

В дальнейшем Региональным Хабом запланировано проведение ряда практико-ориентированных семинар-тренингов, призванных восполнить недостающие знания сотрудников правоохранительных органов в области борьбы с киберпреступностью и обеспечением информационной безопасности.

Также планируется создать единый образовательный центр обучения сотрудников всех правоохранительных органов в области противодействии киберпреступности. Данный центр будет сформирован по аналогии с международными центрами по борьбе с киберпреступностью, куда входят представители правоохранительных органов, комитета национальной безопасности и технических IT-специалистов.

Борьба с киберпреступностью требует консолидации всех сил и средств, выработки совместных решений, способных повлиять на ситуацию.

В частности, необходимо принятие адекватных мер со стороны граждан и частных компаний, без помощи которых принимаемые на сегодня меры малоэффективны.

Поскольку именно от их активности и от того, насколько они сами заинтересованы в безопасности своих данных, зависит эффективность принимаемых государством мер в области кибербезопасности.

К примеру, мы ездим на такси, некоторые водители из которых пренебрегают правилами безопасности, машины имеют технические неисправности. Многие это понимают, осознают опасность, но при этом пользуются их услугами, несмотря на имеющийся риск для жизни. Вот и киберпреступники пользуются нашим безразличием или невнимательностью, а порой и игнорированием рекомендаций поставщиков интернет-услуг.

Если взглянуть на причины успешного создания ботнета, то мы увидим, что в большинстве случаев мы сами способствовали действиям злоумышленников путем игнорирования элементарных правил безопасности, используя не обновленное программное обеспечение или необдуманно открывая различные интернет-ссылки, содержащие вредоносный код.

По результатам проведенных исследований компании «Group-IB», около 92% интернет-ссылок первых ТОП-10 страниц таких поисковиков как «Yandex» или «Google», могут нанести пользователям вред, в том числе привести к утрате конфиденциальной информации [15].

Данный вывод был основан на том, что определенная часть ссылок отсылает пользователей интернета на поддельный или на зараженный сайт, что в конечном итоге приводит их к потере финансовых средств или сбоям в работе операционной системы персонального компьютера.

Это в большей степени относится к пользователям услуги системы интернет-банкинга. Пытаясь найти в открытом интернете ссылку на какой-нибудь веб-ресурс банка, они рискуют попасть на поддельный или зараженный вредоносной программой сайт.

Профилактика киберпреступлений должна исходить не только от государства, но и от самих граждан, которые должны соблюдать элементарные меры информационной безопасности и правила поведения в сети.

К таким мерам относятся:

1) *Обеспечение тайны личных сведений*. При регистрации или переписке на одном из интернет-ресурсов не обязательно вводить свои настоящие анкетные данные, раскрывать сведения о себе и родных, адресе проживания, месте учебы, местах работы, номерах банковских карточек.

2) *Использование антивирусных программ*. Не доверяйте всем сообщениям, поступившим на почту, даже если они от друзей из списка контактов. Обязательно проверьте вложенный файл на наличие вредоносных программ.

3) *Игнорирование по возможности рекламных сообщений*, за которыми могут стоять киберпреступники, готовые похитить данные или причинить материальный ущерб.

4) *Соблюдение осторожности* при сканировании QR-кодов, при активации которых можно попасть на интернет-ресурс, зараженный вредоносной программой.

5) *Проявление бдительности*. Убедитесь в правильности вводимого адреса сайта. Использование даже одной неправильной буквы в адресе может привести на вредоносный сайт.

Все это свидетельствует об актуальности вопроса профилактики киберпреступлений, эффективным способом которой должно стать повышение информационной и компьютерной грамотности населения.

Основным же направлением борьбы с киберпреступлениями должны быть слаженные, скоординированные действия специальных международных организаций, правоохранительных органов многих государств и крупных IT-корпораций против любых попыток нанесения ущерба кибербезопасности.

Список литературы:

1. (http://thelocalhost.ru/cyberprest/) - интернет-источники.

2.ITU Toolkit For Cybercrime Legislation. ITU, 2009. – книга.

3.UNODC. Comprehensive Study on Cybercrime. February 2013. P. XVII. – книга.

4.Дуленко, В.А. Использование высоких технологий криминальной средой. Борьба с преступлениями в сфере компьютерной информации [Текст]: учебное пособие // В.А. Дуленко., Р.Р. Мамлеев., В.А. Пестриков. - Уфа: УЮИ МВД России. - 2007 - книга.

5.UNODC. Comprehensive Study on Cybercrime. February 2013. P. XVII. – книга.

6.Тропина Т.Л. Киберпреступность: понятие, состояние, уголовно-правовые меры борьбы: автореф. дис. ... канд. юрид. наук. - Владивосток. - 2005, С. 9 – автореферат.

7. Российская Ассоциация Электронных Коммуникаций (РАЭК). «Глобальные киберугрозы: возможно ли безопасное развитие цифровой инфраструктуры?»// (http://raec.ru/live/raec-news/9471/) – интернет - источники.

8.Филимонов, В.П. Киберпреступность уже засшкаливает!/ В.П.Филимонов // Русская народная линия, информационно-аналитическая служба //(http://ruskline.ru/special_opinion/2017/fevral/kiberprestupnost_uzhe_zashkalivaet/) – интернет-источники.

9.(http://hi-tech.org/press/blog/cybercrime) – интернет - источники.

10.(http://www.bizhit.ru/index/polzovateli_interneta_v_mire/0-404) – интернет - источники.

11.Тринадцатый Конгресс ООН по предупреждению преступности и уголовному правосудию, Доха, 12-19 апреля 2015 года. Cisco, "The zettabyte era: trends and analysis", Cisco Visual Networking Index (San Jose, California, 2014)//(http://www.unodc.org/documents/congress/Documentation/A-CONF.222-12_Workshop3/ACON F222_12_r_V1500665.pdf) - интернет - источники.

12.Антивирусная редакция «ESET». Взлом телеграфа. И еще 15 самых громких кибератак в истории. – (https://club.esetnod32.ru/articles/analitika/vzlom-telegrafa/) – интернет - источники.

13. (https://oit.boisestate.edu/cybersecurity/spear-phishing-alert/) - интернет-источники.

14.(https://www.securitylab.ru/blog/company/IT-GRAD/293467.php) – интернет -источники.

15.SecurityLab.ru. Group-IB: 92% пиратского ПО в интернете несут угрозу ПК и личным данным пользователей // (https://www.securitylab.ru/news/431428.php) – интернет - источники.