Nigmatov Ruftullo Olimjonovich
Ichki ishlar vazirligi akademiyasi boshlig'ining o'rinbosari
O'zbekiston Respublikasi Falsafa fanlari doktori (PhD), dotsent

KIBERJINOYATCHILIK XALQARO XAVFSIZLIKKA TAHDID SIFATIDA

Nigmatov Ruftullo Olimjonovich
Deputy Head of the Academy of the Ministry of Internal Affairs Republic of Uzbekistan
Doctor of Philosophy (PhD), Associate Professor

CYBERCRIME AS A THREAT TO INTERNATIONAL SECURITY

Нигматов Руфтулло Олимжонович
Заместитель начальника Академии Министерства внутренних дел Республики Узбекистан доктор философии (PhD), доцент

КИБЕРПРЕСТУПНОСТЬ КАК УГРОЗА МЕЖДУНАРОДНОЙ БЕЗОПАСНОСТИ

Появление компьютеров и расширение глобальной сети Интернета привели к достижение значительных высот в разных областях науки, начиная от образования вплоть до генетики. Интернет в настоящее время является основным источником информации для большинства его пользователей. Однако, несмотря на упрощение процесса обмена информацией, с ее помощью была создана новая естественная среда для развития преступности, повысился риск утечки личной информации или даже попадания конфиденциальных данных в чужие руки.

Как справедливо отметил Джанет Рено, генеральный адвокат США при администрации Клинтона: «В то время как Интернет и другие технологии передачи данных предоставляют огромные преимущества человечеству, они, кроме того, открывают новые возможности для незаконного поведения»[1].

Но что такое киберпреступность? Киберпреступность в общем смысле слова означает совершение преступлений с использованием компьютера или сети Интернет. Интернет же характеризуется как «совокупность множества компьютерных и телекоммуникационных удобств, охватывающих оборудование и функционирующие программы, которые составляют взаимосвязанную всемирную сеть систем, обеспечивающих работу Протокола управления передачей данных/протокола Интернета, или любые предшествующие или последующие протоколы к такому протоколу для передачи данных всех типов по кабелю или радио»[2].

Другими словами, Интернет – это обширная компьютерная сеть или цепочка соединений компьютеров, которые соединены вместе. Это подключение позволяет отдельным пользователям подключаться к бесчисленному множеству других компьютеров для сбора и передачи информации, сообщений и данных. К сожалению, эта связь также позволяет преступникам обмениваться информацией и с другими преступниками, а также их жертвами.

По мнению экспертов ООН, термин «киберпреступность» охватывает любое преступление, которое может совершаться с помощью компьютерной системы или сети, в рамках компьютерной системы или сети, или против компьютерной системы или сети[3].

По данным международной службы по обеспечению безопасности в области киберугроз Symantec Security, каждую секунду в мире подвергаются кибератаке 12 человек, а ежегодно в мире совершается около 556 млн киберпреступлений, ущерб от которых составляет более 100 млрд долларов США[4].

В Интернете существует несколько вызывающих беспокойство видов деятельности, которые открывают для киберпреступников бескрайние возможности для осуществления их преступной деятельности. К примеру, существуют сертифицированные агентства, которым разрешено наблюдать за движениями человека в сети Интернет (использование определенных сайтов, переход на веб страницы по ссылкам, регистрация в мессенджерах). Тем не менее, при наличии множества невидимых глаз повсюду, любой может поставить под угрозу информацию других пользователей Интернета[5].

Хакеры и другие киберпреступники в виртуальном пространстве пытаются получить наиболее ценные личные данные с использованием минимальных затрат путем создания и внедрения вирусов, распространения спам-рассылок, фишинговых писем и т.д. Исходя из методов, используемых преступниками в виртуальном пространстве, можно выделить виды киберпреступлений. Также они отличаются по целям и объектам воздействия. Так, киберпреступления могут быть совершены:

1. С целью получения имущественной выгоды (фишинг, онлайн-казино, кардинг). К примеру, создаются специальные сайты, которые являются точной копией оригинального сайта именитого бренда, в котором просят для подтверждения личности ввести конфиденциальные данные (номер банковской карты, паспортные данные);

2. С политической целью – нанесение урона конституционным устоям государства, институтам гражданского общества для подрыва системы властных отношений. Вспомним, к примеру, случаи вмешательства в выборы в зарубежных государствах;

3. С идеологической точки зрения, под которым кроется распространение различной запрещенной информации с целью вербовки людей для совершения преступных действий (терроризм, экстремизм, сепаратизм). В сети Интернет, в том числе в социальных мессенджерах

террористы создают группы, в котором под видом законной деятельности происходит вербовка лиц для совершения в дальнейшем ими преступлений;

4. С целью оказания психологического давления на пользователей. В сети интернет до сих пор распространены так называемые «группы смерти», которые с целью доведения до самоубийства детей, дают им задания в виде «расцарапай свое лицо, нанесение себе шрамы, сбрось себя с 9 этажа». К примеру, игра «Синий кит».

Как отмечала Д.Н. Карпова «из общеизвестных способов совершения киберпреступлений можно выделить два типа: социальную инженерию (не путать с социальной инженерией в социологии) и вирусные программы. Отличительной особенностью первого типа является телефонная или компьютерная атака на человека с целью получения личной информации. Прибегая к особенностям психологии личности, мошенники выдают себя за другое лицо, вводя тем самым человека в заблуждение. Социальная инженерия используется узким кругом специалистов в области информационной безопасности для описания способов «выуживания» личной информации, основанных на знании особенностей психологии человека, с применением шантажа, злоупотреблением доверием. Специфика второго типа киберпреступлений – вирусных программ – заключается в том, что они позволяют киберпреступникам удаленно управлять компьютерами без ведома их пользователей, применяя «продвинутое» современное программное обеспечение. Их называют ботами, а сеть компьютеров, зараженных вредоносным кодом, – ботнетам[6].

К первому типу можно отнести фишинг (от англ. fishing – ловля рыбы), часто используемый для выуживания и кражи конфиденциальных данных пользователей, включая учетные данные (логин, пароль) и номера платежных карт. Схема такова, что киберпреступник, маскируясь под лицо, которому пользователь доверяет (коллега по работе, банк, налоговые службы, администрация почтового ящика), обманом заставляет жертву открыть электронную почту или текстовое сообщение. Затем получателя обманом заставляют перейти по вредоносной ссылке (в которую уже внедрен вирус), что может привести к установке вредоносного ПО, замораживанию системы в рамках кибератаки или утечке конфиденциальной информации.

Вишинг (англ. vishing – voice (голос) + fishing (ловля рыбы)) – это одна из разновидностей фишинга, при которой злоумышленники вместо онлайн рассылок используют средства телефонной связи, используя те же приемы и технологии социальной инженерии, что и для фишинга. Цель выуживание конфиденциальной информации посредством телефонного звонка. Вишер представляется сотрудником банка и сообщает, что с его банковского счета были списаны денежные средства и для блокировки карты пользователь должен продиктовать номер банковской карты, пин-код либо свои личные данные.

Ко второму типу киберпреступлений относятся ботнеты, вирусы, шпионские программы обеспечения.

Ботнеты – это сети компьютеров, зараженных вредоносными программами (такими как компьютерные вирусы, регистраторы ключей и другое вредоносное программное обеспечение) и управляемые удаленно преступниками, как правило, для получения финансовой выгоды или для запуска атак на веб-сайты или сети. Если компьютер заражен этой вредоносной программой и является частью ботнета, он связывается и получает инструкции о том, какие действия ботнет должен осуществить в зависимости от целей киберпреступников.

К примеру, известная группа Thr34t Krew, одна из самых вредоносных групп ботов-пастухов в новейшей истории. В основном не идентифицированные антивирусными компаниями, их боты в течение нескольких месяцев распространялись по всему миру, запускали массовые распределенные атаки типа «отказ в обслуживании» (DDoS) и warez (украденные дистрибутивы программного обеспечения).

Многие ботнеты предназначены для сбора информации, такой как пароли, данные платежных карт, адреса, номера телефонов и другая личная информация. Затем полученные незаконным способом данные используются в корыстных целях, таких как кража личных данных, кибермошенничество, рассылка спам-писем (отправка нежелательной почты), атака на веб-сайты и распространение вредоносных программ.

Вирусы – это вредоносные программы, которые могут передаваться на компьютеры и другие подключенные устройства различными способами. Хотя вирусы во многом различаются, все они предназначены для распространения с одного устройства на другое и причинения вреда. Чаще всего вирусы предназначены для того, чтобы предоставить преступникам, которые их создают, какой-то доступ к зараженным устройствам.

Шпионское программное обеспечение – может быть загружено на устройство пользователя без его разрешения и ведома (обычно, при посещении небезопасных веб-сайтов или через приложений). Данные ПО могут управлять некоторыми функциями компьютера, например, открывать рекламу. В худшем случае шпионские программы могут отслеживать действия пользователя в сети Интернет, красть логины, пароли либо компрометировать учетные записи.

Исходя из вышеизложенного, стоит отметить, что киберпреступность представляет собой международную угрозу безопасности, так как в виртуальном пространстве не существует территориальных границ. Преступник, находясь на территории одной страны, может совершить преступления на территории другой.

Киберпреступность – один из самых больших рисков для процветания в эпоху Четвертой промышленной революции. Кибератаки в отношении целых государств, как правило, привлекают наибольшее международное внимание, но на самом деле киберпреступники наносят еще больший вред, как отдельным гражданам, так и субъектам предпринимательства, является барьером для цифрового развития.

Хотя в мире предпринимаются попытки по укреплению национального потенциала государств, а также оказанию взаимодействия при раскрытии и расследовании киберпреступлений со стороны международных организаций. Глобальная программа Интерпола по киберпреступности и Инновационный центр в Сингапуре, Европейский центр по киберпреступности Европола и Совместная Целевая группа по борьбе с киберпреступностью являются явными результатами данных усилий, равно как и международные диалоги по вопросам политики, такие как Межправительственная группа экспертов открытого состава Организации Объединенных Наций по киберпреступности и Будапештская конвенция Совета Европы[9].

Эффективно противодействовать киберпреступности, как известно, можно, только приложив совместные усилия. Явным примером такого сотрудничества является заключение глобального антихакерского альянса известными провайдерами интернет-услуг. Данный альянс отличался системой раннего оповещения о хакерских атаках в Интернете. Также в 2011 году был создан некоммерческий Международный альянс обеспечения кибербезопасности (The International Cyber Security Protection Alliance – ICSPA), которая объединила правительства, международный бизнес и правоохранительные органы, включая Европол, и была предназначена для борьбы с киберпреступностью в глобальных масштабах. Ее финансирование осуществляется ЕС и рядом правительств других стран (в их числе Австралия, Великобритания, Канада, Новая Зеландия, США), а также компаниями частного сектора[7].

Однако, для эффективной борьбы с киберпреступлениями этого недостаточно. Главы всех стран-членов ООН должны взять на себя ответственность за обеспечение международной кибербезопасности.

Австрия в своем докладе, направленном в ООН отметила, что «киберпреступность представляет собой эволюционирующую проблему, которая затрагивает все страны, что требует эффективного и действенного подхода в целях: a) максимального увеличения числа стран, располагающих адекватным, совместимым внутренним законодательством, направленным на борьбу с киберпреступностью, которое также поддерживает международное сотрудничество; b) создания механизмов сотрудничества, укрепления доверия и развития навыков в целях обмена данными для проведения расследований, судебного преследования и сокращения масштабов киберпреступности»[8].

Исходя из вышеизложенного, предлагается: во-первых, принять единую международную Конвенцию по противодействию киберпреступности на базе ООН, которая была бы обязательной для исполнения всеми странами-членами ООН. Принятие конвенции будет способствовать борьбе с различными видами киберпреступлений, такими как незаконное использование криптовалюты, незаконный оборот наркотическими средствами, вербовка лиц для подрыва конституционных устоев государств, создание вирусных и шпионских программ обеспечения и т.д. Также данный

документ позволит установить территориальные границы государств в виртуальном пространстве.

Во-вторых, создать единую информационную базу данных, содержащую информацию о киберпреступлениях, совершаемых на территории стран-членов ООН с указанием способов совершения киберпреступлений, объекта посягательства, лиц, причастных к совершению преступления, IP-адресов злоумышленников, а также использованные для совершения киберпреступления инструменты, программы обеспечения и т.д.

В-третьих, необходимо на международном уровне решить вопрос совершенствования странами уголовных законодательств для успешной борьбы с киберпреступностью, а также повышения правовой грамотности населения.

Важно наладить оперативное сотрудничество мирового сообщества, так как без него невозможно восполнить правовой вакуум касательно вопросов обеспечения кибербезопасности в виртуальном пространстве и эффективно бороться с киберпреступностью.

Библиографические ссылки:

1. Casey E. Digital Evidence and Computer Crime: Forensic Science, Computers and the Internet. London: Academic Press, 2011: PP. 5–19.

2. Internet Tax Freedom Act of 1998: 112 Stat. 2681–2719. http://www.cbo.gov/doc.cfm?index=608&type=0.

3. Валько Д.В. Киберпреступность в России и мире: сравнительный анализ // Управление в современных системах. – 2016. – №3(10). – С. 29. https://cyberleninka.ru/article/n/kiberprestupnost-v-rossii-i-mire-sopostavitelnaya-otsenka/viewer

4. Е.М. Якимова. Международное сотрудничество в борьбе с киберпреступностью. Всероссийский криминологический журнал. 2016. https://cyberleninka.ru/article/n/mezhdunarodnoe-sotrudnichestvo-v-borbe-s-kiberprestupnostyu.

5. Maddox A., Barratt M.J., Allen M., & Lenton S. (2016). Constructive activism in the dark web: cryptomarkets and illicit drugs in the digital 'demimonde'. Information, Communication & Society, 19(1), 111–126.

6. Д.Н. Карпова. Киберпреступность: глобальная проблема и её решение. // Власть. 2015. Том 22. – № 8. – С. 46.

7. В Лондоне создан Международный альянс обеспечения кибербезопасности. URL: http:// www.vesti.ru/doc.html?id=499251.

8. Доклад Генерального секретаря ООН Антонио Гуттериша на 74-й сессии заседания ООН. 2019.

9. 3. 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