Содержание:

Введение

Стремительное внедрение цифровых технологий во все сферы человеческой жизни в конце XX — начале XXI вв. предопределило возникновение новых общественных отношений. Наибольшую значимость и распространенность имеет технология Интернет, которая соединила людей по всему земному шару, сделала коммуникации дешевыми и беспрепятственными и открыла новые горизонты для всего мирового сообщества. Интернет в последнее время дал человеку безграничные возможности в области передачи, распространения и рассылки информации, позволил выполнять финансово-банковские операции, несмотря на расстояния и границы.

Использование Интернета упростило жизнь и оказало влияние почти на все сферы общества. Стремительное развитие средств коммуникации направлено на удовлетворение потребностей в любой точке мира, где есть Интернет. сформировалось определенное социальное сообщество. Важно отметить, что в этом кибернетическом пространстве осуществляется не только общественно полезная деятельность, значительно облегчающая жизнь индивида, но также совершаются противоправные деяния, которые несут в себе общественную опасность.

Объект исследования: Организованная, компьютерная интернет-преступность

Предмет исследования: Технологии совершения преступлений, особенности и методы борьбы с интернет-преступностью;

Цель курсовой работы – изучить современное состояние интернет преступности, в частности технологии совершения организованной киберпреступности, а также предложить ряд мер противодействию организованной интернет преступности

ГЛАВА I. ПОНЯТИЕ И ОТВЕТСТВЕННОСТЬ ЗА КОМПЬЮТЕРНЫЕ ПРЕСТУПЛЕНИЯ, СОВЕРШЕННЫЕ В СЕТИ ИНТЕРНЕТ

I.I. Понятие, интернет преступлений

Еще недавно об интернете мало кто слышал, сегодня в виртуальной «паутине» уже совершаются преступления. Интернет-преступления, киберпреступность - преступные деяния, которые совершены при помощи компьютера, интернет-сети. Из-за распространения информационных технологий подобные злодеяния из хулиганства, которое невозможно было расследовать, стали настоящим бедствием.

В мире киберпреступления приравнены к преступлениям, которые совершены в жизни, расширяется ответственность за совершения. Раскрыть такие преступления непросто из-за ряда специфических особенностей - например, из-за того, что преступник с жертвой проживают не в одной стране.

Согласно подписанной в начале XXI века Конвенции, интернет-преступления делятся на пять групп:

1 - Против конфиденциальности, доступности компьютерной информации;

2 - Совершенные при помощи компьютерных средств;

3 - Создание, распространение, хранение детской порнографии;

4 - Нарушение авторского права;

5 - Дискриминация людей по расовым, религиозным, физическим признакам, подстрекательство к насилию.

В России, не подписавшей Конвенцию, среди всех сетевых преступлений выделяются:

Кардинг - мошенничество, связанное с платежными картами. Для совершения подобного преступления не нужно наличие карты. Преступникам хватит реквизитов, получить которые можно, взломав сервер интернет-магазина или персональный компьютер, с которого проводились платежи.

В паре с кардингом идет фишинг - мошеннические действия, из-за которых в руках преступника оказываются конфиденциальные данные пользователя, логины, пароли. Чаще всего жертве приходит сообщение от фальшивых магазина, социальной сети, банка или почтовой службы. В нем мошенники под любым предлогом стремятся заставить жертву перейти по ссылке на сайт. Тот выглядит в

точности как настоящий, но для входа требуется ввести логин, пароль, которые тут же отправляются в чужие руки, а жертва перенаправляется по нужному адресу.

Взломом сайта называют незаконное получение доступа к нему при помощи кражи паролей или при отключении безопасности. Это одно из наиболее часто встречающихся преступлений, которое помогает получить данные с сайта. Впоследствии злоумышленник может использовать эти данные или IP-адреса, передавать через него какую-либо информацию или выманивать деньги, если речь идет о магазине.

Понятие спам, на сегодняшний день достаточно известно: навязчивые письма, рекламирующие услугу, призывающие к посещению сайта. Зачастую такая массовая рассылка рекламы неопасна, но случается, что вместе со спамом приходят его опасные «варианты».

Чаще всего в спаме можно встретить:

• рекламу, на получение которой пользователь не подписывался. Помимо простых продуктов рекламировать могут запрещенную продукцию (порнографию, наркотики, контрафакт);

• сообщения о выигрыше: уведомление о крупном выигрыше в лотерею или получении дорогого приза. Для получения приза жертве нужно либо заполнить анкету, указав личную информацию, либо перевести небольшую сумму денег для пересылки приза;

• «нигерийские письма»: представляет собой письмо, составленное жителем другой страны. В письме сообщается о том, что отправитель располагает огромной суммой денег, но воспользоваться ими лично не может.

Например, мошенник представляется адвокатом одинокого старика, который оставил состояние, и у которого нет наследников. Чтобы деньги не были переданы государству, отправитель предлагает получателю письма выступить в роли наследника. После получения деньг их разделят. Мошенник просит либо прислать ему необходимую информацию, включая номер счета, либо выслать небольшую сумму для оформления бумаг;

• письма счастья: пожелания счастья, шутки, «смертельные проклятия», предупреждения о вирусе, сбор голосов. В письмах содержится просьба переслать его контактам. Чаще всего они не несут угрозы, но некоторые могут оказаться

заражены вирусом.

Однако реже бывают следующие виды мошенничества:

• попрошайничество: сбор денег на лечение, просьба о финансовой помощи от благотворительных, церковных организаций. Важно помнить, что настоящая благотворительная организация не занимается рассылкой спама, а больные люди должны получать помощь от благотворительных организаций, а не через интернет;

• пропаганда: настраивание получателя против общественных, религиозных, других групп;

• клевета: распространение заведомо ложной информации с целью опорочить жертву;

• вымогательство: преступники обещают взломать компьютер, сайт или сервер, чтобы украсть данные;

• преследование: постоянная слежка за жертвой, угрозы, обвинения, мелкие неприятности - все это относится к преследованию;

• «кража личности» — наиболее серьезное преступление. Мошенник полностью копирует жертву, ее имя, ник, почту, данные, удостоверение, после использует это для получения незаконным путем каких-либо благ.

Информацию о реакции правоохранительных органов на интернет-преступления можно найти в 28 главе Уголовного кодекса. Так, 272 статья регламентирует такие ситуации, когда преступник получил неправомерный доступ к любого рода компьютерной информации, являющейся личной или корпоративной собственностью.

Например, под эту статью попадают такие действия, как взлом странички в той или иной социальной сети, почтового ящика, самовольная смена чужого пароля, получение информации, закрытой для общего доступа. Максимальный срок наказания за такое достаточно серьёзное преступление - это лишение свободы на срок 2 года.

Совершение этих же действий не в одиночку, а группой лиц карается более сурово (максимальный срок наказания - 5 лет). Примечательно, что Уголовный Кодекс Украины предусматривает гораздо более тяжелые санкции за эти преступления, чем в нашей стране. Правда, на Украине законы часто не соблюдаются, и

преступники легко могут уходить от наказания, но, тем не менее, факт имеет место.

Система наказаний за интернет-преступления, как отмечается многими учеными, ещё проработана мало. Многих было бы справедливо привлекать не только по этой статье, но и по другим статьям УК.

Очень часто злоумышленники отправляют на страницу человека выбранного своей жертвой нецензурные выражения, порнографические картинки. Эти действия также наказуемы, и попадают под 213 статью Уголовного Кодекса, предусматривающую самое строгое наказание за это преступление - 2 года лишение свободы. Совершение этих же действий группой лиц также является квалифицирующим признаком, карается строже. Если же на страничке жертвы пишут различного рода оскорбления, то это уже 129 статья УК.

Актуальнейшим вопросам в интернет-пространстве является религиозная вражда. Известно, что команда хакеров из мусульманских стран взломала ряд европейских сайтов, разместив там призывы карать неверных. Действия этих людей можно квалифицировать статьей 282 УК. Одним из отягчающих обстоятельств, предусмотренных этой статьей, является попытка разжечь национальную вражду в самых экстремальных проявлениях, популяризировать расовую ненависть или совершить религиозную агрессию, может караться лишением свободы до 4 лет.

В случае, описанной выше, возможна квалификация и по 354 статье («Публичные призывы к неправомерному развязыванию войны»).

Люди, которые использую государственную символику на каком-нибудь постороннем сайте, могут привлечься по ст.329 УК РФ. Очень важно, чтобы государство совершенствовалось в защите прав людей в интернете, в защите виртуальной собственности. Предприниматели вряд ли будут охотно вкладывать свои деньги в развитие передовых информационных технологий той страны, чья законодательная база далека от совершенства в сфере контроля над интернет-пространством.

1.2. Ответственность за интернет преступления

Квалификация преступлений, применяемая в уголовном праве - это не только сложная, но и важная проблема для расследований и судебных процессов.

Понятие квалификация преступлений подразумевает выявление и юридическое фиксирование точного соотношения между физическими признаками и признаками состава преступного деяния, попадающее под юрисдикцию уголовно-правовой нормы.

Под квалификацией понимается последовательный логический процесс, который направлен на выяснение признаков, попадающих под юрисдикцию уголовно-правовой нормой.

Особенности квалификации преступлений, совершенных в сети интернет в том, что эти правонарушения сложно разграничить как между собой, так и с другими видами преступлений, предметом которых является информация, находящаяся на компьютерном носителе, системе ПК или компьютерных сетях. В этом деле поможет консультация юриста.

Ответственность за интернет преступления налагается:

• Создание и распространение, продажа порнографических материалов с участием несовершеннолетних в виде фотографий, видео караются законом в виде штрафа от ста до трехсот тысяч рублей ил двумя годами лишения свободы.

• Если же преступники осуществляли привлечение несовершеннолетних для создания порнографического материала, распространяли его, открыто демонстрировали, рекламировали, то за это предусмотрен тюремный срок до шести лет. Эти же деяния, организованные преступной группировкой по сговору наказываются сроком от трех до восьми лет.

• За неправомерный доступ к информации, повлекшее за собой ее блокировку, уничтожение, модификацию или копирование, сбоя в работе ЭВМ или их сетей предусмотрен штраф от двухсот тысяч рублей или в размере заработной платы или иного дохода виновного за период до восемнадцати месяцев, исправительные работы сроком от полугода до года или тюремный срок до двух лет. Если же это преступление совершенно не одним человеком, а группой по сговору или лицом, имеющим доступ к ЭВМ по служебному положению, то грозит штраф от ста до трехсот тысяч или период заработной платы или иного дохода от года до двух лет, или исправительные работы от года до двух лет, арест на срок от трех месяцев до полугода или срок заключения сроком до пяти лет.

• За создание программ, наносящих урон ЭВМ или их сетям, налагается тюремный срок на три года со штрафом до двухсот тысяч людей или в размере заработной

платы либо другого дохода до восемнадцати месяцев.

Если эти же действия были совершены по неосторожности, то это грозит тюремным сроком от трех до семи лет. Неправильное использование ЭВМ, их систем и сетей лицом, имеющим к ним доступ, и повлекшее за собой урон в виде уничтожения, блокирования, защищенной законом информации, грозит запретом на занятия этой деятельностью до пяти лет или исправительным работами сроком от ста восьмидесяти до двухсот сорок часов или тюремным заключением до двух лет.

Если эти же действия совершены по неосторожности, это грозит тюремным сроком до четырех лет и потребуется помощь юриста, чтобы раскрыть преступления через интернет.

За киберпреступления предусмотрены административное и уголовное наказание. К сожалению, в России законы мягче, чем в Европе, но все-таки наказать преступника возможно.

За преступления, совершенные в сфере компьютерной информации, отвечает глава 28 УК РФ. В ней говорится о:

• Неправомерном доступе к информации;

• Создании, распространении вирусов;

• Нарушении правил работы с информацией.

Решение судьи зависит от обстоятельств преступления и ущерба. Закон же говорит о следующих наказаниях:

• Штраф до 100 тысяч рублей;

• Исправительные работы сроком до 5 лет;

• Тюремное заключение сроком до 7 лет.

Интернет-мошенничество будет проходить по статье 159 УК РФ «Мошенничество» — хищение чужого имущества путем обмана жертвы или злоупотребления ее доверием. При этом закон не делает разницы между онлайн-мошенничеством и совершенным в реальности. В качестве наказания могут быть назначены:

• Штраф до миллиона рублей;

• Исправительные работы сроком до 5 лет;

• Тюремным заключением до 6 лет.

Наказание за клевету определено по статье 129 УК РФ «Клевета»:

• Штрафом до миллиона рублей;

• Исправительными работами сроком до 240 часов.

Не так давно к этим законам присоединился и «пакет Яровой» — пакет законопроектов, направленных против террористической деятельности. Согласно этому проекту, все сотовые операторы и Интернет-провайдеры обязаны хранить передаваемые пользователями сообщения (тексты, музыку, изображения, видео) в течение полугода и информацию о том, что они были отправлены и получены - в течение 3 лет. В случае необходимости сотрудники полиции будут иметь возможность проверить переписку подозреваемых.

Вместе с «пакетом Яровой» были приняты некоторые изменения в УК РФ:

1 - Ответственность за призывы к совершению терроризма или его оправдание (статья 205 часть 2) наказывается штрафом до миллиона рублей или лишением свободы до 7 лет;

2 - Ответственность за несообщение о преступлении (статья 205 часть 6): если гражданин РФ не сообщит о готовящемся преступлении из списка, его ждет наказание - штраф до 100 тысяч рублей или год исправительных работ или лишения свободы.

II. ПОНЯТИЕ ОРГАНИЗОВАННОЙ КОМПЬЮТЕРНОЙ ПРЕСТУПНОСТИ В СЕТИ ИНТЕРНЕТ

2.1. Виды организованной компьютерной преступности в сети интернет

Глобальная паутина «Интернет», на данное время жизни является уже далеко не только структурой, обеспечивающей потребности гражданских деловых и личных

коммуникаций.

Киберпреступность – сложноустроенный механизм, не поддающийся традиционным криминологическим оценкам и описаниям, отсюда вытекают и определенные трудности при его изучении и борьбе с ним, этот вид преступности имеет уникальные отличия от любых ранее известных видов.

Правоохранительные органы многих стран продолжают выражать серьезную озабоченность в связи с ростом числа интернет-преступлений. При этом, если раньше мошенничеством и взломами в Сети занимались небольшие группы или одиночки, то теперь можно говорить о приходе в интернет самой настоящей организованной преступности. Именно так считает Лен Хиндс, глава британского Национального управления по преступлениям в сфере высоких технологий (NHTCU). О своем видении проблемы Хиндс рассказал в интервью агентству Reuters. По мнению руководителя NHTCU наиболее уязвимыми перед интернет-преступниками являются индивидуальные пользователи интернета, компьютеры которых, как правило, менее защищены, а сами пользователи зачастую слишком доверчивы.

Ряд основных особенностей упомянутого вида преступной деятельности:

— Неограниченная удаленность;

— Высокий уровень конспирации;

— Отсутствие государственных границ и ограничений.

Преступность в сети интернет также в определенной степени связана как с иными видами преступности, так и множеством негативных проявлений в обществе, так-как Интернет – это еще и мощнейший инструмент средств массовой информации.

Отмечаются тенденции роста организованной преступной деятельности, расширение территории и сфер преступного бизнеса, все более активное использование ее участниками современных научно-технических средств. Примерно с середины 90-х гг. XX века фиксировался резкий «рост организованной преступности, связанной с использованием электронных и телекоммуникационных средств, особенно компьютерных сетей». Согласно отчету Интерпола, опубликованном в 2012 году, показатель доли сетевых компьютерных преступлений, которые были совершены под руководством транснациональных организованных преступных групп, достигает 80%.

Киберпространство становится все более привлекательным для преступников, так как решается ряд задач, таких как, например, обеспечение высокого уровня конспиративной коммуникации профессиональных преступников и иных субъектов, возможность пропаганды противоправной деятельности и формирование ее положительного образа, вербовки новых сторонников, а также осуществление непосредственно самой преступной деятельности (мошенничество, торговля наркотическими средствами, распространение порнографии, экстремистская деятельность и т.д.). В последнее время сильно возрос уровень интеграции отечественных преступных формирований с транснациональными преступными сообществами, а катализатором данного процесса становится глобальная информационно-коммуникационная сеть. Таким образом, представляется целесообразным говорить о наличии преступных группировок и сообществ, которые совершают преступления в сети Интернет, как об особо социально опасном явлении, влияющем на безопасность нашего государства, к которому должны быть применены меры-антагонисты со стороны государственных органов.

В настоящее время, преступная деятельность в интернете активно трансформируется и развивается с огромными скоростями. Верно будет сказать, сетевая преступность идет в ногу с развитием сетевых технологий, а они на данный момент развиваются и «умнеют» стремительнее любых иных технологий, все это происходит на общей волне придания общественным отношениям криминального серого оттенка. Само криминогенное сетевое настроение диктуется далеко не тинэйджерами, которые применяют чужие данные для пользования интернет ресурсами либо осуществляют распространение программного обеспечения, зараженного вирусами в корыстных целях, а конкретными персонами организованных криминальных сообществ.

В современном мире доля преступных деяний, совершенных с использованием сети интернет интенсивно возрастает (в нашей стране за минувшее десятилетие общая масса зафиксированных преступлений такого типа выросла более чем в двадцать раз), прямо пропорционально растут и размеры причиняемого ущерба. Среднегодовая сумма ущерба лишь от интернет мошенничества в мире составляет 200 миллиардов рублей, Российская цифра составляет 50-60 миллиардов рублей. Подобные преступления привлекают к себе все больше внимания, ввиду их растущей опасности и масштабов. В свою очередь еще с 2012 года в МВД России эта проблема на повестке дня постоянно и уже сформировалось приоритетное направление по борьбе с преступной деятельностью, осуществляемой в Киберпространстве.

По соображениям криминологов при углублении в изучение образа существования современной сетевой преступности следует уделить внимание в первую очередь описанию и разбору умысла такой деятельности. Особым фактором является фиксация интенсивного роста именно организованной преступности, основанной на применении средств электронной коммуникации и компьютерных сетей. Организованные преступные группировки растут и развиваются, перетекая в более привычные преступные сообщества. Причем отдельную сложную проблему образует повышение доли сетевых компьютерных преступлений, совершаемых под руководством транснациональных организованных преступных групп (согласно опубликованному в 2012 г. отчету Интерпола, этот показатель достигает 80%. К этому стоит добавить повышение интеграции преступных сообществ, изменение и усложнение характера совершаемых преступлений, ведение в сетевой социальной среде криминальной пропаганды с целью привлечения новых сторонников, осуществление криминальной разведки непосредственно в сетевой информационном пространстве.

В связи с развитием информационных технологий и трансформацией электронной преступности требуется некое совершенствование системы безопасности и законодательной базы именно в этом направлении, по итогу меры пресечения преступной деятельности в сети должны в идеале опережать развитие преступности на один или два шага, иначе очень велика угроза того, что сетевая преступность окажется примерно в таком же положении, как и традиционная организованная преступная деятельность, борьба с которой сейчас ведется совсем не в желаемом ключе. На фоне происходящих социальных преобразований и изменения форм деятельности правоохранительных органов особая роль должна отводиться криминологическим исследованиям, которые в итоге должны привести к формированию новой концепции борьбы с преступностью в киберпространстве, обеспечить правоприменительную практику научно обоснованными рекомендациями.

2.2. Виды организованной компьютерной преступности в сети интернет

Отметим основные тенденции в области компьютерной преступности:

1. Вытеснение программами-вымогателями других модификаций вредоносного программного обеспечения (ВПО), таких как банковские троянские программы.

Программы-вымогатели становятся ключевой угрозой как для граждан, так и для предприятий. К наиболее распространенным типам ВПО относятся:

Программы-вымогатели («Cryptowall», «CTB-Locker», «Teslacrypt», «Locky», «Blackshades.NET»);

Банковское ВПО и троянские программы, предназначенные для сбора конфиденциальной информации («Dridex», «Citadel», «Dyre);

Инструменты удаленного доступа («DarkComet»);

Наборы эксплойтов («Angler», «Nuclear»»);

Программы-загрузчики

Среди крупнейших вызовов — злоупотребление криптовалютами, сексуальная эксплуатация детей в интернете и нестабильность преступных онлайн-рынков.

Сексуальная эксплуатация детей

В интернете продолжает расти количество материалов, содержащих сексуальную эксплуатацию детей.

Наиболее экстремальные материалы можно найти в так называемом даркнет (Darknet, Darkweb). Это скрытая, «темная» сторона интернета, контент которого не видят обычные поисковые системы.

Современные злоумышленники используют средства анонимности и шифрования. Таким образом их не могут обнаружить правоохранители.

Доступ все младших детей до интернета и соцсетей тем временем способствует росту количества случаев сексуального принуждения или вымогательства в отношении детей, отмечает Европол.

Даркнет и преступные онлайн-рынки

Экосистема рынка даркнета, является чрезвычайно нестабильной. Правоохранители закрывают такие незаконные онлайн-рынки, но постоянно появляются новые.

Даркнет продолжает способствовать онлайн-преступности и распространению нелегальных товаров и веществ.

Мошенничество с банковскими картами

Пока люди используют платежные карты с магнитными полосами — будет продолжаться так называемый скимминг. Это разновидность мошенничества, при котором проводят операцию с использованием платежной карты или ее реквизитов, не инициированная владельцем карты. Скимминг остается распространенной проблемой в многих странах ЕС. Похищенные данные карты обычно продают в том же даркнете.

Социальная инженерия

Социальная инженерия — это специальная методика манипуляции, которая помогает хакерам вытащить из человека необходимую информацию благодаря использованию ее психологии. Ее распространение продолжает набирать обороты, пишут авторы.

Фишинг — самая распространенная форма социальной инженерии. Его цель — получить личные данные или осуществить незаконные платежи.

Люди не так часто переходят по первым ссылкам-приманкой, которое видят, так что «на крючок» попадаются не часто. Но если попасть в «правильную» цель, то иногда может быть достаточно и одного человека, который сделает это, чтобы добраться до сети целой организации.

Злоупотребление криптовалютами

Мошенники все больше используют крипто вал юту для финансирования своей криминальной активности. Основная криптовалюта — биткойн.

Владельцы и пользователи криптовалют тем временем сами становятся жертвами многочисленных хакерских атак и кражи личных данных.

Криптоджекинг: новый тренд киберпреступлений

Криптоджекинг (cryptojacking) стал новой тенденцией в мире киберпреступлений.

Это новый способ майнить криптовалюту — когда майнери используют ресурсы чужих компьютеров в собственных целях.

Вредоносные программы.

Распространение вредоносных программ замедляется, но остается значительной угрозой.

В то же время нелегальное получение личных данных людей — одна из самых больших проблем. Злоумышленники часто используют полученные данные для дальнейшей преступной деятельности.

Хакерские атаки DDoS (отключение обслуживание систем) используют не лишь для финансовой выгоды, но также и для идеологических и политических целей.

Атаки DDoS становятся более доступными и дешевыми.

Рекомендации Европола говорят, среди прочего, о важности проведения кампании осведомленности среди людей о киберпреступности. Так, наибольший успех в борьбе, например, с социальной инженерией иметь образование потенциальных жертв.

Европол рекомендует усилить сотрудничество между частным сектором, гражданским обществом и учеными для борьбы с детской сексуальной эксплуатацией онлайн. Решение проблемы даркнету требует международной стратегии.

В 2017 году для борьбы с программами-вымогателями правоохранительными органами ЕС (EC3, полиция Нидерландов) в сотрудничестве с частным сектором был создан и запущен портал «No More Ransom» (nomoreransom.com). Целью этой инициативы является информирование общественности об опасностях, связанных с программами-вымогателями, и оказание помощи жертвам данного ВПО по восстановлению своих данных без уплаты выкупа злоумышленникам.

Продолжение роста коммерциализации криминальных услуг (crime-as-a-servece). «Черный рынок» компьютерной преступности предлагает широкий спектр товаров и услуг: наборы эксплойтов, украденные персональные данные и данные кредитных карт, информация о скомпрометированных серверах, продажа и аренда бот-сетей, услуги по проведению компьютерных атак типа «распределенный отказ в обслуживании» (DDoS-атак), услуги по взлому компьютерных сетей.

Активное использование злоумышленниками (в том числе террористическими группировками) в целях сокрытия преступной деятельности: невидимого поисковыми системами сегмента сети Интернет («darknet»), средств обезличивания («анонимайзеры») и шифрования данных, механизмов защиты коммуникаций и

транзакций, методов стеганографии, а также виртуальной криптовалюты (bitcoin). Всё это существенно затрудняет судебное расследование преступлений.

Появление организованных преступных группировок, использующих скомпрометированные данные платежных карт, в основе которых лежит технология беспроводной высокочастотной связи малого радиуса действия (Near field communication, NFC). Ряд группировок разрабатывает и реализует (в «darknet») программное обеспечение, позволяющее загрузить на Android-устройства данные скомпрометированных NFC-карт и использовать их для оплаты покупок в любых магазинах, поддерживающих технологию NFC. Это является показателем скорости, с которой злоумышленники адаптируются к появлению новых технологий и начинают использовать их в своих целях.

Появление фишинговых кампаний, где в качестве элемента социальной инженерии используется рассылка писем от имени генеральных директоров крупных компаний (т.н. «CEO fraud»). Фишинг подобного рода может приводить к существенным потерям (финансовым, репутационным) целевых организаций.

Рост интенсивности и сложности DDoS-атак. Если в 2016 году рекордная мощность DDoS-атак составляла 300 Гбит/с, то в 2017 году уже зафиксированы DDoS-атаки с трафиком свыше 600 Гбит/с. Кроме того, на «чёрном рынке» компьютерной преступности распространены предложения «DDoS-атака как услуга» (DDoS-as-a-service).

Данные остаются ключевым товаром злоумышленников. Атаки, целью которых является похищение данных, по-прежнему нацелены в первую очередь на получение финансовой информации, затем следуют данные медицинских учреждений и интеллектуальная собственность. Зачастую похищенные данные шифруются с целью получения выкупа.

Криптовалюта (bitcoin) остается инструментом, наиболее часто используемым компьютерными преступниками в качестве оплаты преступных услуг и получения выкупов от жертв программ-вымогателей.

Вредоносные программы для мобильных устройств по своему характеру, уровню сложности и способу распространения всё больше приближены к ВПО для обычных ПК.

В следствие груминга или приемов социальной инженерии дети всё чаще становятся жертвами сексуального насилия и вымогательства.

Банковские EMV-карты («чипованные»), блокирование операций в определенной географической зоне (geoblocking) и другие механизмы безопасности, внедряемые финансовыми институтами, в настоящее время снижают уровень мошенничества с банковскими картами в Европе, вынуждая преступников проводить мошеннические схемы в других регионах (Северной и Южной Америках, Юго-Восточной Азии). Вместе с тем продолжают развиваться и увеличиваться атаки на банкоматы.

Увеличивается число т.н. платежных операций без присутствия карты (Card not present transaction, CNP), при которых держатель карты не присутствует во время и в месте проведения оплаты. Это затрагивает различные типы сделок: оплата авиабилетов, покупки в интернет-магазинах, аренда автомобиля или жилья.

Появление новых направлений для проведения компьютерных атак в связи с ростом числа подключенных устройств из сферы «Интернет вещей». (персональные маршрутизаторы, веб-камеры, телевизоры и принтеры).

2.3. Способы и направления борьбы с организованной компьютерной преступностью в сети интернет

Представим перечень мер по противодействию современным вызовам и угрозам в сфере компьютерной безопасности:

• Развитие сотрудничества по обмену сведениями об инцидентах и вредоносных программах, а также при проведении исследований инцидентов между правоохранительными органами, частным и финансовым секторами, компаниями в сфере обеспечения информационной безопасности и научными учреждениями.

• Взаимодействие правоохранительных органов различных государств, в том числе, не входящих в Европейский союз.

• Предоставление государствами-членами Европейского союза образцов вредоносных программ в систему анализа ВПО (Europol Malware Analysis System, EMAS).

• Взаимодействие правоохранительных органов с провайдерами с целью своевременного обнаружения, блокирования и удаления противоправного контента.

• Повышение квалификации сотрудников правоохранительных органов (в частности, обучение методам сбора цифровых доказательств), своевременное информирование их о новых угрозах и обеспечение соответствующими ресурсами и средствами.

• Участие правоохранительных органов в кампаниях по повышению осведомленности пользователей сети Интернет о методах совершения компьютерных атак, способах защиты от них и базовых стандартах информационной безопасности (в том числе профилактическая работа в школах). Кроме того, описывается необходимость информирования потенциальных компьютерных преступников - людей, вовлекаемых в противоправную деятельность, о последствиях.

• Установление базовых стандартов информационной безопасности для автоматизированных систем управления производственными и технологическими процессами критически важных объектов (АСУ ТП КВО).

• Проведение тщательных расследований инцидентов и ВПО правоохранительными органами (а не просто сбор информации о жертвах).

• Выявление и блокирование правоохранительными органами интернет-ресурсов и форумов, на которых злоумышленники обмениваются информацией.

• Согласование законодателями и политиками совместно с представителями промышленности вопроса о применении пользователями шифрования в целях защиты конфиденциальной информации без ущерба для работы правоохранительных органов по расследованию угроз национальной безопасности.

• Со стороны промышленности необходимо проведение работ по устранению существующих недостатков безопасности в программном обеспечении и аппаратных средствах, а также учитывание современных угроз безопасности при разработке новых устройств, в том числе из области «Интернет вещей».

• Внедрение эффективных каналов для предоставления компаниями-жертвами в правоохранительные органы онлайн-отчетности о совершенных в их отношении компьютерных преступлениях. В частности, говорится о необходимости участия операторов критической инфраструктуры в реализации директивы «Сетевая и информационная безопасность» (Network and Information Security, NIS), предложенной Европейской комиссией в феврале 2016 года в рамках стратегии в области кибербезопасности для ЕС.

В качестве примера успешного сотрудничества всех заинтересованных сторон создана Объединенная целевая группа по борьбе с компьютерной преступностью (Joint Cybercrime Action Taskforce, J-CAT). Целью данного альянса является трансграничное расследование компьютерных преступлений и скоординированное совместное противодействие ключевым угрозам компьютерной безопасности, в числе которых: разработка и распространение ВПО, создание бот-сетей, интернет-мошенничество, несанкционированное проникновение в компьютерные сети и др.

Кроме того, в качестве примера удачного решения государственно-частного партнерства упоминается про создание «в некоторых странах специальных подразделений финансовых CERTs – “FinCerts”, сосредоточенных на вопросах финансового сектора».

Большинство стратегий кибербезопасности и борьбы с киберпреступностью являются относительно краткими документами (10-20 страниц) без достаточной детализации. Основное внимание сосредотачивается на соответствии рассматриваемых вопросов, подтверждении воли к действию и изложении общих решений о том, что следует сделать в целях повышения кибербезопасности. Большинство стратегий не дают описания конкретных решений и мер. Идея стратегии заключается в том, что она дает решение определенной проблемы или задачи. Она не должна быть привязана к конкретному случаю, но обязана давать четкий порядок действий по решению определенной задачи. Так, в Стратегии кибербезопасности Германии 939 указано, что правительство планирует организовать инициативы и изучить будущие сферы ответственности провайдеров. Однако эта стратегия оставляет открытым вопрос о том, кто возглавит этот процесс, и как будет достигаться поставленная цель.

Преимуществом краткой базовой стратегии является незначительное время, необходимое для ее разработки. Определение крайне общих принципов также значительно снижает потребность в регулярных обновлениях. Общая стратегия может оставаться неизменной в течение многих лет, прежде чем возникнет необходимость в ее доработке. Но такой подход связан с определенными внутренними проблемами. Очевидно, справедливо утверждение о том, что разработка развернутого подхода не требует объединения всех возможных мер и действий в одном документе. Однако составление целого ряда документов может привести к недостаточной согласованности различных мер. Опыт показывает, что ввиду сложности угроз, даже мелкие конфликты или несоответствия в рамках различных мер могут значительно снизить эффективность как профилактики, так и реагирования на инциденты. Стратегия дает максимальный результат только при

условии полного согласования и последовательности всех компонентов.

Возможный компромисс заключается в дополнении предельно общей стратегии конкретными (и, следовательно, более детальными) последующими планами действий. Такой подход дает возможность на общественном уровне продемонстрировать предпринимаемые усилия в форме публикаций стратегии кибербезопасности и борьбы с киберпреступностью, сохранив статус секретности конкретных мер. Необходимость представить обзор действий в сфере кибербезопасности и борьбы с киберпреступностью может быть неотложной для правительства, при этом наличие стратегии кибербезопасности может оказаться условием для привлечения инвесторов в страну. В то же время раскрытие данных о мерах, принимаемых в целях усиления кибербезопасности и идентификации правонарушителей, не всегда является приемлемым, так как может предоставить злоумышленникам поле для обнаружения слабых мест действующей системы.

Разработка законов с целью признания преступлением определенных действий или внедрения новых инструментов расследования нехарактерны для большинства стран. По общему правилу, страна в первую очередь разрабатывает ту или иную политику. Политику можно сравнить со стратегией, предусматривающей различные средства для решения конкретной проблемы. В отличие от более общей стратегии борьбы с киберпреступностью, которая может затрагивать разных участников, политика заключается в реагировании государства на определенную проблему. При этом государство не обязательно должно реагировать путем принятия законодательных актов, так как у него есть и другие инструменты для достижения целей политики. И даже если принимается решение о необходимости введения в действие законов, такие законы не обязательно должны относиться к уголовному праву. Они также могут содержать нормы, в которых больший акцент уделяется профилактике преступности. В этом отношении разработка политики позволяет государству всесторонне реагировать на ту или иную проблему. Так как борьба с киберпреступностью не может ограничиваться исключительно принятием законов, но предусматривает различные стратегии и различные меры, разработанная политика может гарантировать отсутствие конфликтов в ходе реализации этих различных мер.

В рамках различных подходов, направленных на гармонизацию законодательства о киберпреступности, слишком мало внимания уделяется не только интеграции этого законодательства в национальную правовую систему, но и его включению в существующую политику или вообще разработке такой политики. В результате некоторые страны, которые просто приняли законодательство о

киберпреступности, но не разработали стратегию борьбы с киберпреступностью, равно как и государственную политику по этому вопросу, столкнулись с серьезными трудностями. Такие трудности были вызваны недостаточной проработкой мер по профилактике преступности, а также частичным совпадением различных мер.

Разработанная политика дает возможность согласовать полномочия различных государственных ведомств по тому или иному вопросу. Нет ничего необычного в том, что полномочия отдельных министерств будут пересекаться - в отношении киберпреступности это, скорее, закономерность, так как данная проблема носит междисциплинарный характер. Вопросы борьбы с киберпреступностью могут относиться, например, к компетенции Министерства юстиции, Министерства связи или Министерства национальной безопасности. В процессе разработки политики можно определить роль различных государственных ведомств.

Как указано выше, разработанную политику можно использовать для определения составных частей конкретного подхода. Таковые могут включать укрепление институционального потенциала (например, полиции и прокуратуры), конкретные поправки в законодательство (модернизация законодательства).

В идеале разработанная политика должна быть направлена на согласование различных действий, даже если они осуществляются разными министерствами и государственными учреждениями. Тот факт, что любое направление политики в целом требует одобрения кабинета министров, не только способствует составлению перечня различных государственных органов и министерств, которые должны заниматься конкретной проблемой, но и позволяет гармонизировать их деятельность.

Разработанная политика позволяет определить не только то, какие государственные ведомства должны решать проблему, но и каких других участников следует привлечь к этому процессу. К примеру, может потребоваться разработка руководящих принципов по привлечению к решению проблемы частного сектора.

Кроме того, такой подход должен предусматривать участие в решении проблемы разных сторон: государства, министерств и государственных учреждений, частного сектора, школ и университетов, лидеров, выбранных в силу обычая, общин, международных и региональных органов, органов охраны правопорядка, судей, таможенной службы, прокуроров, юристов, гражданских служащих и

неправительственных организаций.

Как подчеркивается ниже, гармонизация законодательства относится различными региональными организациями к числу приоритетных направлений деятельности. Однако гармонизировать требуется не только законодательство, но и стратегию и подготовку специалистов. Разработанная политика может использоваться для того, чтобы установить, что подлежит гармонизации, а также для того, чтобы определить, каким региональным и/или международным стандартам необходимо соответствовать.

Принимая во внимание глобальность киберпреступности, а также необходимость защитить интернет-пользователей в регионах от киберпреступников, следует отнести к приоритетным меры по расширению возможностей борьбы с киберпреступностью. Стратегии борьбы с киберпреступностью и особенно законодательство, разрабатываемое для решения проблем киберпреступности, должны, с одной стороны, соответствовать международным стандартам, а с другой стороны, учитывать специфику региона.

Должны существовать нормы, касающиеся самых распространенных и признанных международным сообществом форм проявлений киберпреступности, а также преступлений, характерных для конкретного региона (например, спам).

В целях обеспечения возможности сотрудничества органов охраны правопорядка различных стран определенного региона как в рамках самого региона, так и за его пределами, законодательство должно соответствовать как международным стандартам и примерам передового опыта, так и (до максимально возможной степени) существующим региональным стандартам и примерам передового опыта.

Разработанную политику можно использовать для определения ключевых вопросов, подлежащих законодательному урегулированию. К их числу может относиться, к примеру, перечень преступлений. Степень детализации может быть высокой и предусматривать детализацию норм, которые необходимо включить в законодательство о киберпреступности.

Должно быть предусмотрено положение, признающее преступлением намеренное и незаконное производство детской порнографии, ее продажу и иные действия, относящиеся к детской порнографии. В этом отношении особенно важно учитывать международные стандарты. Законодательство должно, кроме того, признавать преступлением обладание детской порнографией и получение доступа к веб-сайтам, распространяющим детскую порнографию. Следует предусмотреть

оговорку, позволяющую органам охраны правопорядка проводить расследование.

Принятие законодательства о киберпреступности - непростая задача, так как регулирования требуют различные сферы. Помимо норм материального уголовного и процессуального права законодательство о киберпреступности может регулировать вопросы международного сотрудничества, электронных доказательств и ответственность поставщиков услуг Интернета. В большинстве стран элементы такого законодательства, возможно, уже существуют, обычно в различных нормативно-правовых актах. Нормы, касающиеся киберпреступности, не обязательно должны содержаться в одном нормативно-правовом акте. Что касается существующих структур, то в рамках процесса принятия нового законодательства может потребоваться модернизация различных законодательных актов (например, внесение поправок в "Закон о доказательствах" в целях обеспечения возможности его применения в вопросах допустимости электронных доказательств в уголовном процессе) или исключение положений из устаревших законов (например, из "Закона об электросвязи").

Принять законодательство о киберпреступности с учетом уже существующих структур, безусловно, сложнее, чем просто дословно включить региональный стандарт или международные примеры передового опыта в отдельно взятый самостоятельный нормативно-правовой акт. Но в силу того, что в ходе такого подхода можно сохранить национальные правовые традиции, многие страны отдают предпочтение именно ему.

Разработанную политику можно использовать для определения того, какие составные части подхода следует интегрировать, а также для выявления действующих законов, требующих модернизации.

Несмотря на то, что угроза применения наказания потенциально сдерживает преступность, уголовное законодательство сосредоточено не на профилактике преступности, а на применении санкций за преступление. Однако профилактика преступности относится к ключевым мерам эффективной борьбы с киберпреступностью. Принимаемые меры могут варьироваться от технических решений (таких, как установка брандмауэров, предотвращающих нелегальный доступ к компьютерной системе, или антивирусного программного обеспечения, препятствующего инсталляции вредоносного программного обеспечения) до блокирования доступа к нелегальному контенту.

В прошлом решения по борьбе с киберпреступностью были сосредоточены на принятии законодательства. Однако как уже отмечалось в главе, посвященной стратегии борьбы с киберпреступностью, составные части всестороннего подхода к проблеме киберпреступности гораздо сложнее. Не так давно центром внимания стала роль регуляторных органов в борьбе с киберпреступностью.

Роль регуляторных органов в области электросвязи является общепризнанной. Появление Интернета разрушило прежние модели разделения обязанностей между государством и частным сектором. В этой связи наблюдается изменение традиционной роли регуляторных органов ИКТ и изменение фокуса регулирования ИКТ. Уже сегодня регуляторные органы ИКТ оказываются задействованными в решении проблемы киберпреступности. Это особенно актуально для таких сфер, как регулирование контента, безопасность информационных сетей и защита потребителей, поскольку пользователи стали более уязвимыми. Привлечение регуляторных органов к решению проблемы, таким образом, было вызвано тем, что киберпреступность подрывает развитие сферы ИКТ и сопутствующих продуктов и услуг.

Новые обязанности регуляторных органов ИКТ по борьбе с киберпреступностью можно рассматривать как часть более глобальной тенденции превращения централизованных моделей регулирования киберпреступности в более гибкие механизмы. В некоторых странах регуляторные органы ИКТ уже изучили возможность перенесения объема регуляторных полномочий с вопросов конкуренции и выдачи разрешений в области электросвязи на более широкие вопросы защиты потребителей, развития отрасли, кибербезопасности, участия в разработке и осуществлении политики по борьбе с киберпреступностью. При этом происходит большее применение ИКТ и, как следствие, все чаще возникают вопросы, связанные с киберпреступностью. Были созданы новые регуляторные органы, в полномочия которых входит решение проблемы киберпреступности, однако и ранее созданные регуляторные органы ИКТ расширили список поставленных задач и включили в него меры по противодействию киберугрозам. Но степень участия этих органов в решении проблемы и пределы их полномочий до сих пор являются предметом дискуссий.

Заключение

Полная ликвидация преступлений организованных преступных сообществ, совершенных в сети Интернет, в обозримом будущем является довольно сложной задачей, так как необходимо разрушить те определенные социальные и рыночные условия, которые ей способствуют. Это обусловлено рядом факторов, таких как, например, тотальная глобализация, одним из побочных эффектов которого является рост организованной преступности как особой группы преступлений, включающую в себя, в том числе и киберпреступность. Необходимо отметить, что одним из ключевых элементов, обеспечивающих стабильное существование организованных преступных сообществ, является деятельность по противодействию раскрытию и расследованию организованной преступной деятельности, которое является механизмом по уменьшению эффективности детальности правоохранительных органов, ведущих борьбу с преступностью. Следует подчеркнуть, что борьба с интернет-преступностью требует существенной доработки современного уголовного законодательства, а также изменения тактики борьбы с преступностью в области теоретического осмысления сложившихся криминалистических проблем.

Для того чтобы общество могло свободно развиваться с помощью информационных технологий в своей стране, государству просто необходимо постоянно совершенствовать законодательную базу в сфере всяческих преступлений в интернет-пространстве. Предпринимателям гораздо выгодней вкладывать деньги в развитие информационных технологий той страны, которая заботится о безопасности электронного бизнеса. В последнее время в России чувствуются перемены в сторону обеспечения сохранности и развития информационно-правовых аспектов в Интернете.

Список литературы

1. Указ Президента РФ от 31.12.2015 №683 "О Стратегии национальной безопасности Российской Федерации" // Собрание законодательства РФ. 04.01.2016. №1 (часть II). Ст. 212
2. Овчинский А.С. Информационные воздействия и организованная преступность: курс лекций. //А.С. Овчинский. — М., 2017. -164 с.
3. Основы борьбы с организованной преступностью: монография // под ред. В.С Овчинского, В.Е. Эминова, Н.П. Яблокова. - М., 2016,- 50 с.
4. Скляров С. В., Евдокимов К. Н. Современные подходы к определению понятия, структуры и сущности компьютерной преступности в РФ // Криминологический журнал Байкальского университета экономики и права. 2016. № 2. С. 24–25.

5. Комаров А. А. Интернет-мошенничество: проблемы детерминации и предупреждения: Монография. М.: Юрлитинформ, 2013. С. 91.
6. Осипенко А. Л. Организованная преступность в сети Интернет // Вестник Воронежского института МВД России. 2012. № 3. С. 10–16.
7. Осипенко А. Л. Организованная преступность в сети интернет. //Вестник Воронежского института МВД России. В: -2012.
8. Овчинский А.С. Информационные воздействия и организованная преступность: курс лекций. // А.С. Овчинский. — М., 2017. -164 с.
9. Дяблова Ю.Л., Тишутина И.В. К вопросу о роли специалиста в выявлении и преодолении противодействия расследованию организованной преступной деятельности // Известия ТулГУ. Экономические и юридические науки, 2013. № 4–2. С. 189.
10. Майоров А. В. Противодействие преступности – приоритетное направление уголовной политики государства // Вопросы современной юриспруденции: сб. ст. по матер. XXXIV междунар. науч.- практ. конф. № 2 (34). Новосибирск: СибАК, 2014.
11. Давыдов В. О. Выявление информации экстремистской направленности в электронных информационных сетях в целях раскрытия и расследования преступлений // Известия ТулГУ. Экономические и юридические науки, 2011. № 2–2. С. 90.
12. Тишутина И. В. Противодействие расследованию как элемент организованной преступной деятельности экстремистского характера // Известия ТулГУ. Экономические и юридические науки, 2015. № 3–2. С. 24.
13. The Tor Project. Why is it called Tor? [Электронный ресурс]. URL: https://www.torproject.org/docs/faq.html.en#WhyCalledTor
14. Tor: Луковый маршрутизатор второго поколения. [Электронный ресурс]. URL: https://web.archive.org/web/20141213142011/http://www.opennet.ru/soft/tordesign.pdf
15. Paul Syverson. Onion Routing: History. [Электронный ресурс]. URL: http://www.onion-router.net/History.html
16. Metrics wordmark - Relays and bridges in the network. [Электронный ресурс]. URL: https://metrics.torproject.org/networksize.html?start=2016-02-14&end=2016-02-01
17. Metrics wordmark - Direct users by country. [Электронный ресурс]. URL: https://metrics.torproject.org/userstats-relay-country.html
18. Уголовный кодекс российской Федерации от 13 июня 1996 г. № 63- ФЗ (ред. от 30.03.2016, с изм. от 16.07.2015) // СЗ РФ – 17 июня 1996 г. – № 25 – Ст. 2954.
19. Доход от нелегальной торговли в интернете. [Электронный ресурс]. URL: http://www.securitylab.ru/news/474253.php

20. Мониторинг Реестра запрещённых сайтов: статистика. URL: https://antizapret.info/index.php?search=onion.to
21. Жертва скрытого сервиса TOR подала иск против разработчиков анонимной сети TOR. [Электронный ресурс]. URL: http:// www.linux.org.ru/people/xusrol/?&offset=40
22. Создатели анонимной сети TOR удостоены награды. [Электронный ресурс]. URL: https:// www.pgpru.com/ forum/anonimnostjvinternet/ sozdatelianonimnojjsetitorudostoenynagradypioneeraward2012