ОСТОРОЖНО – КИБЕРПРЕСТУПЛЕНИЯ !

Улучшение сетевых технологий современности привело не только к ускорению формирования социума, но и к расширению источников угрозы для него. В век появления новых технологий и научных открытий в IT-сфере все большее количество людей попадают в сети мошенников, несмотря на уровень информированности населения в данной сфере.

Стремительно возрастает количество онлайн-общения, а параллельно с этим и активность злоумышленников, которые действуют анонимно, участились случаи манипулирования в сети Интернет (секстинг, кибербуллинг), произошла трансформация девиантных форм поведения в киберпространстве, появление новых молодежных криминальных субкультур в виртуальном мире.

Состояние правопорядка требует постоянного анализа киберпреступности, распространения информации о них среди различных слоев населения, в том числе несовершеннолетних, пожилых граждан, которые оказываются наиболее уязвимыми от уловок мошенников.

Преступность в информационной среде - одна из угроз, оказывающих значительное воздействие как на национальную безопасность Российской Федерации, так и на конкретного человека.

Сложность в раскрытии киберпреступлений в том, что зачастую киберпреступники действуют в условиях неочевидности, применяя современные IT технологии обладают достаточно высокой квалификацией, не оставляют следов присутствия и своего пребывания на месте совершенного правонарушения. Нередко «потерпевший» не думает о совершенном преступлении, а к моменту обнаружения проходит большое количество времени, так все возможные следы, по которым можно было выйти на правонарушителя полностью пропадают.

Представляется, что наиболее полное определение, отражающее стороны этого негативного явления, предложено в статье Д.Н. Карпова «киберпреступление – это акт социальной девиации с целью нанесения экономического, политического, морального, идеологического, культурного и других видов ущерба индивиду, организации, государству посредством любого технического средства с доступом в Интернет».

Из общественных способов совершения киберпреступлений можно отметить два вида: социальную инженерию и вирусные программы.

Прибегая к особенностям психологии личности, мошенники, как правил, выдают себя за другое лицо, вводя тем самым человека в заблуждение. Данный психологический способ применяется узким кругом специалистов в области информационной безопасности с целью описания способов «выуживания» личной данных, что основано на знании особенностей психологии человека, с применением шантажа и злоупотреблением доверия. Наиболее популярным способом социальной инженерии считается мошеннический фишинг, или «выуживание» у безграмотных пользователей интернета их конфиденциальных сведений.

Особенности и виды киберпреступлений

Финансовые преступления

Социально опасные действия, посягающие на финансово-экономические отношения, а непосредственно мошенничество с пластиковыми картами, кража денежных средств в момент совершения банковских действий и т.д.

Фишинг

Фишинг представляет собой выведение данных у доверчивых людей для доступа к банковским счетам. Он распространен в странах, где распространены услуги интернет-банкинга. В данный момент получил свое распространение целевой фишинг. Целевой фишинг практикуется на ограниченные группы пользователей и включает сообщения с социальным контекстом, призывающие потенциальных людей открыть исполняемый файл или перейти на сайт, который содержит вредоносный шифр.

Фарминг

Это процесс скрытого перенаправления жертвы на фальшивый IP-адрес.

Также небезопасным видом киберпреступления считается удаленное взламывание компьютера, за счет которого хакеры обладают возможностью читать и редактировать документы, сохраненные на файлах-серверах и на рабочих столах компьютеров, обладают возможностью вводить собственные вредоносные программы, а кроме того, собирать разного рода информацию, сведения, с помощью аудио и видео наблюдения.

Специфика второго типа киберпреступлений состоит в том, хакеры удаленно управляют компьютерами без ведома их пользователей, используя продвинутое и современное программное обеспечение.

Сайт, посвященный воздействию научно-технического прогресса на личность, «Человек и прогресс» приводит некоторые виды киберпреступлений:

Кибер-порнография

Порнографические сайты, которые позволяют посетителям размещать порнографические фильмы, видеозаписи и фото с гражданами, недостригшими совершеннолетнего возраста. Кроме того, к этому можно причислить также чаты знакомств, содержащие порнографическую информацию о пользователях и описание виртуального секса с несовершеннолетними гражданами.

Кибер-торговля наркотиками

это наркоторговля с применением новых технологий кодирования сообщения, которые передаются покупателям по электронной почте. В данных сообщениях наркоторговцы указывают в кодированном виде место и способ осуществления обмена товара на деньги.

Кибертерроризм

Это осуществление террористических действий в киберпространстве. К этому так же относится распространение посредством Интернета информации о терактах, которые могут быть совершены в будущем в конкретно указанное время.

Также выделяют такие виды киберпреступлений, как **азартные игры-онлайн** и **киберпреследование**.

Необходимо отметить, что жертвами киберпреступлений становятся в большинстве случаев несовершеннолетние граждане.

Последнее время самым страшным и необратимым процессом влиянием на детей стало массовое вовлечение их в ряде регионов в суицидальные группы.

Происходит влияние на детей как путем непосредственного взаимодействия в переписке в социальных сетях, так и через предложение просмотра видео, обсуждения телесериалов, в помощи решения домашнего задания, также могут предлагаться определенные онлайн-книги, рекомендации по прочтению литературы и прослушивание музыки. Впоследствии несовершеннолетние становятся жертвами тяжких преступлений (половых и других).

Одним из подобных ярких примеров современного времени считается интернет-игра для детей и подростков «Синий кит», окончательный этап которой является суицид участника.

Правоохранительными органами активно проводятся профилактические мероприятия по предотвращению подобных киберпреступлений, жертвами которых становятся несовершеннолетние граждане. Опасность этих асоциальных явлений разъясняется родителям, иным законным представителям детей, педагогам, воспитателям образовательных, социальных и других учреждений, непосредственно несовершеннолетним и молодежи с последствиями вовлечения в преступную деятельность, уголовной ответственности за указанные преступления.

Таким образом, киберпреступление — это комплекс правонарушений, запрещенных Уголовным кодексом Российской Федерации (далее – УК РФ), которые совершены в киберпространстве, где ключевыми непосредственными объектами преступного посягательства выступают:

- Конституционные права и свободы человека и гражданина;
- Общественные отношения в области компьютерной информации и информационных технологий;
- Общественные отношения в области экономики и финансовой деятельности;
- Общественные отношения в области правительства;
- Общественные отношения в области здоровья населения и социальной нравственности.
- При совершении киберпреступления лицо осознает общественную опасность деяния, предвидит наступления вредных для общества или отдельного лица последствий и желает наступления этих последствий, либо относится к ним безразлично. Киберпреступления исключают совершение их по небрежности или легкомыслию.

- Основная особенность, отличающая киберпреступления от иных противоправных деяний заключается в использовании компьютерных технологий и сети Интернет при совершении преступления. Компьютер или компьютерная сеть играют в данном случае ведущую роль
- Содержательное наполнение категории киберпреступлений должно соответствовать действующему уголовному законодательству.
- Уголовный кодекс Российской Федерации содержит главу 28 «Преступления в сфере компьютерной информации», включающей в себя четыре статьи с 272 по 274.1 УК РФ:
- - неправомерный доступ к компьютерной информации;
- - создание, использование и распространение вредоносных компьютерных программ;
- - нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей;
- - неправомерное воздействие на критическую информационную инфраструктуру Российской Федерации.
- Зачастую киберпреступления рассматриваются как синонимы компьютерным преступлениям, под которыми понимают только вышеназванные специальные составы УК РФ.
- Иногда к компьютерным преступлениям относят также мошенничество в сфере компьютерной информации (ст. 159.6 УК РФ). При этом основным непосредственным объектом мошенничества являются отношения собственности: именно поэтому ст. 159.6 УК РФ расположена в главе 21 УК РФ. Отношения по сбору, хранению и передачи компьютерной информацию выступают дополнительным объектом.
- В то время как в стст. 272 – 274.1 УК РФ эти отношения выступают основным непосредственным объектом.
- Учитывая, что помимо компьютера в настоящее время существует множество других устройств, позволяющих выйти в цифровую среду, категория компьютерных преступлений в понятийном аппарате представляется неполной, так как не охватывает, например, преступлений, совершаемых через мобильный телефон, не являющийся компьютером. Поэтому термин «киберпреступление» представляется универсальным.
- **Помимо преступлений в сфере компьютерной информации в ряде статей УК РФ содержится конструктивный либо квалифицирующий признак совершения деяния «с использованием электронных или информационно-телекоммуникационных сетей, в том числе сети «Интернет»».**
- Конструктивный признак использования высоких технологий при совершении преступления содержится только в ст. 137 УК РФ, уже

отмеченной ст. 159.6 УК РФ, а также в ст.ст. 171.2, 185.3, 258.1, 282 УК РФ.

- В качестве признака, повышающего общественную опасность содеянного и влекущего более строгое наказание, совершение деяния с использованием электронных или информационно-телекоммуникационных сетей содержится всего в тринадцати составах уголовного закона: три состава в главе «Преступления против жизни и здоровья» (ст.ст. 110, 110.1, 110.2 УК РФ), один состав в главе «Преступления против семьи и несовершеннолетних» (ст. 151.2 УК РФ), один состав в главе «Преступления против общественной безопасности» (ст. 205.2 УК РФ), пять составов в главе «Преступления против здоровья населения и общественной нравственности» (ст.ст. 228.1, 242, 242.1, 242.2, 245 УК РФ), один состав в главе «Экологические преступления» (ст. 258.1 УК РФ), два состава в главе «Преступления против основ конституционного строя и безопасности государства» (ст.ст. 280, 280.1 УК РФ).
- Необходимо отметить, что в УК РФ содержится еще несколько составов, которые можно отнести к киберпреступлениям. Так, п. «г» ч. 3 ст. 158 УК РФ содержит особо квалифицированный состав – кража с банковского счета, а равно в отношении электронных денежных средств, ст. 159.3 УК РФ устанавливает ответственность за мошенничество с использованием электронных средств платежа, ст. 187 УК РФ в части неправомерного оборота электронных средств, электронных носителей информации, технических устройств, компьютерных программ, предназначенных для неправомерного осуществления приема, выдачи, перевода денежных средств. Отнесение данных составов к киберпреступлениям возможно благодаря предмету преступления, которым выступают либо безналичные денежные средства, либо электронные средства, либо электронные носители информации, то есть всё то, что появилось как результат развития информационных технологий и внедрения их в банковский сектор.
- При этом не только вышерассмотренные преступления могут быть совершены посредством высоких технологий. Так, например, незаконное приобретение или сбыт оружия может осуществляться, в том числе, через Интернет, однако в ст. 222 УК РФ, данный квалифицирующий признак не нашел отражения, как в ст. 228.1 УК РФ применительно к наркотическим средствам, психотропным веществам или их аналогам. Или, например, незаконная розничная продажа алкогольной и спиртосодержащей пищевой продукции, несмотря на законодательный запрет, осуществляется через Интернет. Специалисты Brand Protection Group-IB посчитали экономику теневого алкорынка: средняя посещаемость сайта, реализующего алкоголь с доставкой,

составляет 190 пользователей в сутки или 5 700 человек в месяц. При конверсии 0,7% и средней стоимости одной покупки в 1 100 рублей, 4 000 онлайн-магазинов зарабатывают от 174,5 млн. рублей в месяц. Таким образом, оборот нелегальной интернет-продажи алкоголя по итогам 2018 года составил порядка 2,1 млрд. рублей, что на 23% выше, чем годом ранее. Но в соответствующем составе преступления не предусмотрено усиление ответственности в случае незаконной продажи алкоголя посредством Интернет.

- Таким образом, на современном этапе развития информационного общества **киберпреступления необходимо рассматривать как умышленные деяния, совершаемые с использованием IT-технологий. К киберпреступлениям относятся специальные киберпреступления и общеуголовные киберпреступления.** Специальные киберпреступления – это преступления в сфере компьютерной информации. Общеуголовные киберпреступления – это иные преступления, совершаемые с использованием высоких технологий. К ним относятся преступления, в составе которых присутствует в качестве конструктивного или квалифицирующего признак совершения деяния с использованием электронных или информационно-телекоммуникационных сетей, в том числе сети «Интернет», а также преступления, составы которых в качестве предмета преступления называют электронные средства, электронные носители информации.

Способы общения (социальной инженерии) в Интернете

Известно, что в интернете нет жестов, интонации, мимики. Все общение построено на текстовых сообщениях. Существует ряд приемов, с помощью которых можно скрыто манипулировать сознанием человека:

Провоцирование.Это и есть троллинг. Выводя человека из себя, он в большинстве случаев некритично относится к информации. В этом состоянии можно навязать или получить нужную информацию.

Влюбленность. Это один из эффективных приемов. В этом состоянии человек, а особенно несовершеннолетние и молодые люди пребывают в эйфории, а манипулятору как раз это и необходимо, чтобы добиться расположения и своей цели.

Безразличие. Создается эффект безразличия манипулятора к определенной теме, а собеседник в свою очередь старается его переубедить, чем самым попадается в капкан и раскрывает нужную вам информацию.

Спешка.Часто возникают ситуации, когда манипулятор, якобы, спешит куда-то и постоянно намекает на это, но при этом он целеустремленно продвигает нужную ему информацию.

Подозрительность. Прием подозрительности чем-то схож с приемом безразличия. В первом случае жертва доказывает обратное, во втором - жертва пытается оправдать «свою подозрительность», тем самым не понимая, что выдает всю информацию.

Ирония. Сходна с приемом провоцирования. Манипулятор иронирует, выводит человека из себя. Тот в свою очередь в гневе не способен критически оценивать информацию. В итоге в психологическом барьере образуется дыра, которой и пользуется манипулятор.

Откровенность. Когда манипулятор рассказывает собеседнику откровенную информацию, у собеседника возникают некие доверительные отношения, что подразумевает ослабление защитного барьера. Это и создает брешь в психологической обороне.

В социальной инженерии существует множество методов, и с каждым днем эта база пополняется новыми приемами. Некоторые атаки невозможно провести без использования современных технологий, другие основываются сугубо на психологии человека.

Фишинговые письма. Фишинговые письма обманом заставляют пользователей выдать свои личные данные (имена пользователей, пароли и данные кредитных карт) или установить файл с вредоносным содержанием. Одна из причин эффективности фишинга заключается в том, что люди склонны доверять сообщениям от важных или известных им отправителей. В этих целях злоумышленник легко манипулирует URL-адресом, например, такой URL-адрес http://www.company.com выглядит почти идентично как http://www.cornpany.com. Фишинг базируется на человеческих ошибках, а не на технологиях, поэтому повышение осведомленности в глобальном масштабе является главным способом борьбы с такой особенно эффективной формой социальной инженерии.

Лучшая защита от фишинговых сообщений – не идти на поводу у преступников, то есть не переходить по ссылкам, указанным в сообщениях, не вводить свои данные в поля формы, встроенной в сообщение. Вместо этого вручную вводите адрес проверенного сайта в адресной строке браузера и никогда не пользуйтесь автоматическим заполнением полей.

Подставной посыльный. Не менее распространенная атака заключается в том, что злоумышленник выдает себя за представителя фирмы, доставляющего товар покупателю. Вспомните, сколько раз “посыльных” пускали в офис компании, к которому у них нет доступа? А ведь простое проникновение в офис может привести преступника к полному доступу в систему. Обычно преступник может маскироваться под работника известной почтовой службы, доставщика пиццы, цветов или других товаров.

Последнее время стало распространенным обращение по телефону с предложением выкупа якобы заказанной ранее бытовой техники, мебели и др. В это время в квартире может оказаться пожилой человек, который в силу своей доверчивости и высокой ответственности принимает услугу и оплачивает предложенную сумму. Позже выясняется, что никакого заказа родственники не оформляли.

Виртуальное пространство обеспечивает анонимность пользователей, что в свою очередь создает благоприятную среду для появления новых киберпреступников. Низкий уровень раскрываемости данных преступлений,

а также проблематичности расследования уголовных дел данной категории, безнаказанность преступников не способствуют их профилактике и пресечению, а правосознание граждан относительно данного вида преступлений как показывает правоприменительная практика еще не до конца сформировано.

Преступники, скрываются на просторах сети Интернет, пресечь их незаконные действия гораздо сложнее, чем обычного мошенника. Более того, наряду с уже имеющимися способами обмана и выуживания информации, изобретаются новые и более изощренные способы совершения преступлений. Обычные люди становятся жертвами таких киберпреступников очень часто, а причина такой ситуации в недостаточной осведомленности граждан об угрозах, которые их подстерегают в любом техническом устройстве. Практика показывает, что у людей нет чёткого, формированного понимания, что такое киберпреступления. К сожалению, не многие понимают, что это угроза, но не предполагают какие могут последствия. В ряде случаев они находятся как-будто под гипнозом, выполняя механически предписание злоумышленника за обещанные бонусы, вознаграждения, выплаты, льготы и т.д.

В условиях распространения в России данного вида преступлений, в том числе в нашем регионе, необходимо активно распространять среди граждан правовую информацию, придавать гласности все случаи кибермошенничества в СМИ, соцсетях, предостерегать граждан от возможных преступлений с использованием информационных технологий, их последствия, призывать их быть бдительными. Только знания помогут гражданам уберечься от киберпреступлений, предупредить их близких людей и знакомых от возможного совершения преступлений в отношении них.

Прокуратура Амурской области