Секция «Уголовное право и криминология, уголовно-исполнительное право»

Понимание киберпреступности в «реальном мире»

Научный руководитель – Таилова Айша Габибовна

Касумович Исаков Магомед

Студент (специалист)

Всероссийский государственный университет юстиции (РПА Минюста России), Москва, Россия

E-mail: iskvv.14@mail.ru

Аннотация: Экспоненциальный рост использования интернета во всем мире связан с увеличением числа преступлений с использованием интернета и "облака", так как они обеспечивают увеличенный централизованный круг потенциальных жертв и новые возможности как для совершения преступлений, так и для уклонения от обнаружения и привлечения к ответственности. Увеличенное использование технологий социальных медиа означает, что один преступник теперь может достичь большего числа жертв, а стоимость и уровень навыков, необходимых для совершения киберпреступлений, снизились. Онлайн-сообщества предлагают готовые пакеты вредоносного программного обеспечения (т.е. вредоносных программ), которые можно продать неопытным лицам, и обучающий материал свободного доступа, что позволяет обычным пользователям интернета погрузиться в мир киберпреступности. Становится проще, дешевле и удобнее совершать киберпреступления в больших масштабах.

Обучение для повышения знаний и предоставления стандартизированных реакций на сообщения о киберпреступлениях, а также увеличение общественной активности и информационной поддержки, могут помочь улучшить уровень и опыт противодействия данной категории преступных.

Ключевые слова: киберпреступность, жертвы, киберсообщества, технология облака, рост использования интернета, противодействие преступности

Хотя всеобще согласовано, что киберпреступность существует, нет универсального определения того, что она означает. Термины, включая киберпреступность, компьютерные преступления, преступления в облаке и злоупотребление компьютерами, часто используются взаимозаменяемо и могут относиться к любой преступной деятельности, связанной с интернетом или компьютером. В этой статье любое преступное поведение с использованием интернета будет называться "киберпреступностью", если не указано иное в контексте конкретных исследований. Признавая, что киберпреступность является глобальной проблемой, эта статья будет сосредоточена в основном на пресечении киберпреступности в Англии и Уэльсе.

Широко признано, что киберпреступность весьма распространена и увеличивается. Согласно недавнему отчету, поставщики услуг интернета (ISP) ежедневно регистрируют около 80 миллиардов автоматизированных сканирований от онлайн-злоумышленников с целью выявления целей для киберпреступности, а за год, заканчивающийся в сентябре 2019 года, против домохозяйств в Англии и Уэльсе было совершено 1 миллион "злоупотреблений компьютерами"[1] (Национальное агентство по борьбе с преступностью [NCA], 2020). Онлайн-преступность растет не только по количеству, но и в процентном отношении ко всем преступлениям. Опрос о преступности в Англии и Уэльсе сообщает о растущей доле зафиксированных преступлений, отмеченных полицией как онлайн-преступления, при этом есть свидетельства, указывающие на то, что такие "флаги" остаются малоиспользуемыми (Офис национальной статистики [ONS], 2017, 2018, 2019a) [2].

В то время как традиционная преступность сокращается в западных странах, киберпреступность увеличивается за пределами этой скорости снижения. Также отмечается, что снижение традиционной преступности предшествует появлению и росту киберпреступности [3,с.776-784]. Это, в сочетании с различиями в характеристиках преступления и преступника, означает, что нельзя предполагать, что рост киберпреступности вызвал спад в офлайн-преступности, ни что те преступники, которые традиционно действовали офлайн, теперь перешли к совершению киберпреступлений[4,с.51-57]. Независимо от причин, преступность сейчас развивается и переходит в онлайн-пространство, усиливая нисходящий тренд в инцидентах традиционной преступности[5,с.796-797] .Этот рост и сдвиг к киберпреступности, вместе с взаимозаменяемым и часто смущающим терминологией, привели к недавним предложениям о том, что приставка "кибер-" может вскоре стать излишней, поскольку почти все преступления будут затронуты технологиями [6, с.153-154].

Действительно, во всех серьезных и организованных преступлениях, которые расследуются сейчас, присутствует какое-то шифрование, и интернет используется для вербовки, подвергания жертвы и извлечения прибыли от традиционных офлайн-преступлений. С момента своего широкого распространения несколько десятилетий назад интернет облегчил совершение преступлений в разной степени, определенной Уоллом (2007) как киберпомогаемые, кибервозможные и киберзависимые преступления [7,с.156].

Типология Кирвана и Пауэра (2013) также включает интернет-возможные (т.е. кибервозможные) и интернет-специфические (т.е. кибер-зависимые) преступления, а также преступления против виртуальной личности[8,с.11]. Два общих концепта между типологиями кажутся надежными: текущая Национальная стратегия кибербезопасности признает только кибер-возможные и кибер-зависимые преступления, и что эти два типа взаимосвязаны. Кибер-возможные преступления определяются как традиционные преступления, которые усилены по масштабу или охвату за счет технологий (например, мошенничество), в то время как кибер-зависимые преступления - это преступления, которые были бы невозможны без интернета. Хотя эти преступления могут быть связаны с офлайн-преступлениями, такими как кража, грабеж, умышленное повреждение имущества или мошенничество, киберпреступления не являются синонимом офлайн-преступлений и воспринимаются жертвами, преступниками и властями по-разному .

Экспоненциальный рост использования интернета во всем мире связан с увеличением числа преступлений с использованием интернета и "облака", так как они обеспечивают увеличенный централизованный круг потенциальных жертв и новые возможности как для совершения преступлений, так и для уклонения от обнаружения и привлечения к ответственности. Увеличенное использование технологий социальных медиа означает, что один преступник теперь может достичь большего числа жертв, а стоимость и уровень навыков, необходимых для совершения киберпреступлений, снизились. Онлайн-сообщества предлагают готовые пакеты вредоносного программного обеспечения (т.е. вредоносных программ), которые можно продать неопытным лицам, и обучающий материал свободного доступа, что позволяет обычным пользователям интернета погрузиться в мир киберпреступности. Становится проще, дешевле и удобнее совершать киберпреступления в больших масштабах.

Этот процесс усугубляется развитием технологии облака, обеспечивающей увеличенное хранилище компьютерных данных и вычислительную мощность. Предоставляя онлайн-пул общих ресурсов, облако способствует доступу к готовому программному обеспечению для атак и ресурсам обработки, таким как ботсети, для проведения и автоматизации атак, представляя собой онлайн-среду, в которой преступники могут легко и анонимно охотиться, действовать и распределять награбленное. По своей природе как общий центр данных, облачная технология увеличивает количество устройств, к которым можно получить до-

ступ через интернет, и, следовательно, количество возможностей для злоумышленников для эксплуатации. Эффект облака как усиливающего фактора не только приводит к большему доходу преступников, но и дополнительно снижает риск привлечения к ответственности. Таким образом, интернет и облачные вычисления предлагают спектр преступных вариантов - от воздействия сетевого компьютера на традиционное преступление до преступлений, автоматизированных и происходящих исключительно в виртуальной среде.

Пользователи сети интернет часто являются самым слабым звеном в компьютерной безопасности, и в зависимости от вида киберпреступления их слабости могут быть использованы различными способами - делая жертв инструментами своего собственного поражения. Средства эксплуатации включают социальную инженерию и обман, манипуляцию процессов принятия решений через воспринимаемую срочность или авторитет и использование предсказуемых привычек, связанных с использованием веб-сайтов, загрузками, использованием паролей и социальными или профессиональными контактами.

Жертвы могут поэтому винить себя или быть объектами обвинения со стороны других, кроме потенциально разрушительных последствий, таких как финансовые потери или ущерб репутации и карьере. Большинство жертв киберпреступности сообщают о эмоциональных последствиях, начиная от раздражения до депрессии, бессонницы, тревоги и панических атак[9, с.11-19].

Каждый год выше процент жертв кибермошенничества сообщает об эмоциональных последствиях, чем у жертв мошенничества вне интернета. Жертвы киберпреступности могут испытывать длительные психологические и эмоциональные последствия, включая посттравматический стрессовый расстройства (ПТСР), с сопутствующими влияниями на физическое здоровье. Жертвы также могут чувствовать стыд или нарушение их частной жизни или испытывать разрыв отношений после финансовой.

Потеря, утечка информации, сексторшнилимошенничество в сфере романтических отношений. Более серьезным является потенциальная физическая опасность, вплоть до угрозы жизни из-за встреч с незнакомцами в реальной жизни или атак на важные службы, такие как энергоснабжение и здравоохранение. Онлайн-сексуальная эксплуатация и торговля людьми - другие примеры крупномасштабных преступлений, которые были облегчены и увеличены благодаря Интернету, поскольку злоумышленники могут более легко получать доступ к жертвам, вербовать сообщников, анонимно распространять материалы и получать гораздо больше потенциальных клиентов, стимулируя спрос на совершение этих преступлений. Как и в случае многих других форм серьезной и организованной преступности, темная сторона Интернета позволяет продолжать многие из этих преступлений, несмотря на усилия правоохранительных органов.

Хотя большинство пользователей интернета сообщают о страхе перед киберпреступностью, важности информационной безопасности и опасениях в отношении конфиденциальности, лишь немногие пользователи переводят это в профилактические поведенческие меры, даже после столкновения с преступностью. Это расхождение между отношением к конфиденциальности и поведением известно как "парадокс конфиденциальности".

Этот парадокс, предположительно, вызван ложным чувством защищенности компьютера и чрезмерной зависимостью от программного обеспечения, при этом применение мер безопасности даже может повысить риск стать жертвой. Результаты исследования Янсена и Люкфельдта демонстрируют это, поскольку у большинства жертв фишинга было защитное программное обеспечение, но они признали, что неосторожно передали злоумышленникам свои защитные коды. Даже когда люди обладали осведомленностью о признаках безопасности на веб-сайтах (например, поврежденные изображения или необычные URL-адреса), это часто не приводило к осторожности. Эффект онлайн-дезингибиции помогает объяснить этот феномен; он относится к тому, как пользователи интернета кажется

раскрывают больше информации онлайн, чем они сделали бы в офлайне, иногда это приписывают дистанцированию от реального мира и восприятию анонимности и невидимости. Тенденция к чрезмерной самоотдаче онлайн может привести к тому, что личная информация становится легко доступной потенциальным киберпреступникам.

Этот диссоциативный способ поведения и результативное расхождение между поведением в онлайне и офлайне(названные "токсическая дезингибиция"; приводят к увеличению онлайн-антисоциального поведения, девиантности, преступности и насилия. По сравнению с традиционной преступностью, киберпреступность предлагает большую степень защитной анонимности с множеством способов для атакующего замаскировать свою личность онлайн, даже принимая новую личность. Это разделение идентичностей означает, что люди не испытывают поведенческих ингибиций в такой же степени, как в офлайн-контекстах, частично из-за снижения ощущения близости к жертве, что приводит к снижению чувства вины и страха перед возмездием. Киберпреступники также воспринимают риски попадания под уголовно- правовое преследование как относительно низкими, а возможные последствия санкций как малозначительными, что практически не действует как угроза от этого вида преступлений.

Недостаток адекватного сдерживания в сочетании с мотивирующими факторами, описанными позже, побуждают людей к совершению киберпреступлений.

"Обмен идеями и совместная работа, а также конкуренция считаются важными в пути к киберпреступности. Хакеры и другие киберпреступники создают отношения и сети как онлайн, так и оффлайн, причем хакерские сообщества обеспечивают «гильдийные социальные и учебные структуры». Культура хакерства акцентирует внимание на способностях и навыках, которые определяют социальный статус в этих сообществах, поощряя усвоение знаний и стремление к вызовам, вознаграждая успех статусом.

В то время как литература указывает на то, что интеллектуальные вызовы и любопытство являются сильнейшим стимулом для взлома систем безопасности, это не совпадает с фактической частотой взломов, что вызывает сомнения в надежности самоотчетов. Предполагается, что это отражает культурно признанные мотивы, а не истинные личные стимулы.

Второй по силе мотив, указанный в литературе, признание и уважение со стороны сверстников, оказался связанным с взломом: чем сильнее мотивирован взломщик желанием признания и уважения сверстников, тем чаще он пытается обойти системы безопасности[10,с.245-256].

Взлом веб-сайтов в первую очередь мотивируется высокой видимостью цели, подтверждая другие выводы о стремлении к статусу и репутации внутри хакерской субкультуры, так как эти цели достигаются через атаки на высоко значимые объекты. Взлом домашних страниц веб-сайтов мотивируется идеологией или чувством вызова, в то время как второстепенные страницы взламываются ради развлечения, чтобы быть лучшими, патриотически или без какой-либо конкретной причины. Эти преступники обычно гордятся своими преступлениями, желая, чтобы другие знали, что они были ответственны за них , возможно, потому что признание открывает доступ к лучшим онлайн-группам и хакерским сайтам, принося больше ресурсов и престижа.

Другие мотивации к совершению преступлений. Некоторые исследования показывают, что преступники становятся участниками киберпреступности из-за перспективы финансового выигрыша, и финансовое вознаграждение оказалось одним из самых важных мотивов для совершения виртуальных краж и мошенничества в интернете. Однако некоторые исследования считают деньги наименее мотивирующим фактором для хакеров.

Развлечение также оказалось важным фактором в мотивации к совершению мошенничества с личностью и хакерскими преступлениями. Причины совершения преступлений

включают в себя хакеров, обманывающих систему как «розыгрыш», командную игру и интеллектуальный вызов. Некоторые преступники заявляют, что чем сложнее был взлом, тем более приятным был опыт. В то же время некоторые исследователи предполагают, что легкость и отсутствие устрашения являются стимулами для взлома.

Большая часть исследований, дающих представление о вышеупомянутых мотивах, была проведена с использованием онлайн-форумов, источника информации, часто упоминаемого в соответствующей литературе. Хакерские форумы, как правило, позволяют хакерам "входить" в обширную социальную сеть и идентифицироваться с более крупным хакерским сообществом . Помимо привлечения через социальные контакты в оффлайн-мире, форумы помогают людям найти подходящих соучастников и играют роль в формировании и росте многих киберпреступных сетей[11, с. 11-19]. Это может быть связано с сочетанием вредоносного и безвредного контента на форумах. Пользователи, изначально заинтересованные в компьютерных играх или технологиях, могут обнаружить привлекательность хакерских или мошеннических действий, к которым они подвергаются, ради любопытства и вызова, а также для улучшения своего финансового положения и репутации внутри сообщества.

Текущая литература подчеркивает важность доверия, статуса и уважения в этих форумных сообществах и показывает, как такие форумы могут использоваться для помощи в обучении молодых правонарушителей, как предполагается в отчетах Национального уголовного агентства. Пользователям форумов о киберпреступности присваиваются группы, соответствующие их социальному статусу на сайте. Например, онлайн-черные рынки, в основном занимающиеся торговлей вредоноснымипрограммами, имеют иерархии от вступительных уровней членства, таких как новичок, до высокопрестижныхрангов модератора или администратора. Обучение и знания, по-видимому, центральны для этого уровня статуса в хакерской субкультуре, и качество информации или креативное использование материалов пользователями могут повысить их уровень статуса[12,с.11-19].

Исследования показали, что форумы не только отражают способности пользователей, но и активно используются многими людьми для изучения и обучения других тому, как взламывать и совершать онлайн-мошенничество, и есть доказательства, что это начинается с раннего возраста. Один преступник, интервьюированный Хатчингсом (2014), сообщил, что он обучил до 40 других людей взлому на онлайн-форумах и общался с более чем 200 другими. Такое использование онлайн-форумов подтверждается ценностями, демонстрируемыми их содержанием; продолжительное изучение, практика и значительные усилия требуются для того, чтобы стать хорошим хакером .

Соответственно, хакерские форумы обычно предоставляют инструменты для обучения пользователей основам взлома, созданию вредоносного программного обеспечения, учебных пособий по взлому Facebook и общей программировке. Эти учебные пособия были связаны с увеличением совершения киберпреступлений, так как те, кто узнал о компьютерной деятельности из таких форумов, оказались более склонны к взлому и созданию вредоносного программного обеспечения .

Из-за восприятия анонимности и удаленности от оффлайн-мира пользователи интернета испытывают ложное чувство безопасности, а онлайн-преступники психологически, социально и физически отдалены от своих преступлений и жертв. Они сталкиваются с меньшими и/или менее серьезными последствиями за свои действия и, скорее всего, повторяют эти преступления, ободренные своим опытом.

Жертвы киберпреступлений редко сообщают о своем статусе по сравнению с жертвами традиционных преступлений, что, по предположению, связано с воспринимаемым недопониманием и не готовностью полиции, а также жертвы и полиция выражают путаницу относительно того, к какой организации обратиться за помощью.

Обучение для повышения знаний и предоставления стандартизированных реакций на сообщения о киберпреступлениях, а также увеличение общественной активности и информационной поддержки, могут помочь улучшить уровень и опыт противодействия данной категории преступных.

Большее понимание о киберпреступлениях и их участниках также может улучшить подготовку к расследованию, а также повысить способность получения лучших результатов при допросах, формирования более точных выводов и выявления соответствующих доказательств по фактам совершения киберпреступлений.

Источники и литература

1) https://ru.wikibrief.org/wiki/National_Crime_Agency
2) The ONS Economic Statistics and Analysis Strategy provides users, stakeholders and researchers clarity on how was are working to improve UK economic statistics. https://www.ons.gov.uk/methodology/classificationsandstandards/economicstatisticsclassifications/onseconomicstatisticsandanalysisstrategyfinancialyearending 2019
3) Иванцов С. В., Борисов С. В., Узембаева Г. И. и др. Актуальные проблемы совершенствования системы мер криминологического предупреждения преступлений экстремистской направленности, совершаемых с использованием информационно-телекоммуникационных сетей // Всероссийский криминологический журнал. 2018. Т. 12. № 6. С. 776-784.
4) Глотина И.М. Киберпреступность как теневой бизнес // Вестник Челябинского государственного университета. 2016. №6 (388). . 51-57.
5) Куленко К.Н. Проблемы киберпреступности в РФ и пути ее решения // Научное обеспечение агропромышленного комплекса. 2017. С. 796-797.
6) Айсаханова Е.С. Причины и мотивы роста киберпреступности как глобального явления современности // Вестник Чеченского государственного университета. - 2017. -№4 (28). - С. 153-155.
7) Номоконов В.А., Тропина Т.Л. Киберпреступность как новая криминальная угроза // Криминология: вчера, сегодня, завтра, 1 (24), 2012 г.
8) Батурин Ю.М., Жодзишский А.М. Компьютерная преступность и компьютерная безопасность. — М., 1991. — С. 11.
9) Басараб М.А., Иванов И.П., Колесников А.В., Матвеев В.А. Обнаружение противоправной деятельности в киберпространстве на основе анализа социальных сетей: алгоритмы, методы и средства (обзор) // Вопросы кибербезопасности. 2016. Вып. 4 (17). С. 11-19
10) Гайфутдинов Р.Р. «К вопросу о типологии личности компьютерных преступников с учетом характера и мотивации их криминальной деятельности // Вопросы российского и международного права.» 2017. Т. 7. № 4А. С. 245-256
11) Басараб М.А., Иванов И.П., Колесников А.В., Матвеев В.А. Обнаружение противоправной деятельности в киберпространстве на основе анализа социальных сетей: алгоритмы, методы и средства (обзор) // Вопросы кибербезопасности. 2016. Вып. 4 (17). С. 11-19