УДК 343.9

КРИМИНОЛОГИЧЕСКИЙ ПОРТРЕТ КИБЕРПРЕСТУПНИКА И МЕТОДЫ ПРЕДОТВРАЩЕНИЯ ПРЕСТУПЛЕНИИ В СФЕРЕ ИНФОРМАТИЗАЦИИ И СВЯЗИ

Токанов Ерсин Ертисович
tokanovyersin@gmail.com
студент 3 курса юридического факультета ЕНУ им. Л.Н.Гумилева
Нур-Султан, Казахстан
Научный руководитель – к.ю.н., доцент Ашимова Э.А.

Высокие темпы развития в Казахстане информационно-коммуникационных технологий актуализируют вопросы защиты соответствующей инфраструктуры. Поскольку ее повреждение или разрушение может иметь значительные последствия для безопасности страны.

По оценкам экспертов Казахстан занимает 18-е место в мире по количеству получаемого спама и 7-е по опасности веб-серфинга. Почти половина пользователей Интернета в 2010 г., становились объектами атак со стороны хакеров, и эта цифра в 2011 г. увеличилась на 47%. По данным Kaspersky Security Network, Казахстан стал объектом 85% интернет-атак в Центральной Азии. При этом за последние три года наблюдается тенденция их роста пропорционально развитию цифровой инфраструктуры. Так, национальные компании «Қазақстан темір жолы» поэтапно переводит в цифровой формат свои сложные операции, «KEGOC» нуждается в фазовой информации от своих сетей, чтобы лучше управлять потоками энергии.Реализуется космическая программа, где большое значение играет контроль за спутниками связи. Вооруженные силы планируют развивать массовые электронные решения в аэрокосмической отрасли. Аналогичные технологии используются для мониторинга морских месторождений, судоходных путей нефтяных танкеров, экологических рисков и контрабанды на Каспии[1]. За последний год 34% казахстанцев подвергались кибер-атакам. Еще больший процент – 61% опрошенных специалистов в сфере IT – сталкиваются с угрозами кибербезо-пасности в своей деятельности. Наиболее часто встречающийся – вредоносный спам, ему подверглись 11% граждан. Каждый десятый житель республики столкнулся с атакой компьютерных вирусов. У 7% населения были взломаны аккаунты в социальных сетях. Такое же число респондентов (7%) подверглось кибер мошенничеству с банковскими картами[2].

Киберпреступность может быть определена как любое преступление, совершенное или использующее компьютер[3]. Киберпреступность охватывает все: от атак на объекты инфраструктуры, такие как водоочистные сооружения, интернет-провайдеры и железнодорожные сети, до

проникновения на электронные ресурсы корпораций и частных лиц[4]. Киберпреступность отличается от уличной преступности в нескольких отношениях. Во-первых, учитывая сложный и комплексный характер целей (нарушение безопасности в одном поставщике интернет-услуг может затронуть миллионы отдельных пользователей) масштаб киберпреступности с точки зрения потенциальных жертв часто превышает уличную преступность. Тем не менее, масштаб не единственная разница между киберпреступностью и обычной уличной преступностью. Самое большое различие связано с тем, что люди, живущие в отдельных странах, могут ориентироваться на отдельных лиц и организации по всему миру[5]. Кроме того, любой, имеющий доступ к компьютеру, может совершить киберпреступление[6]. Более того, жертвы киберпреступности часто не осознают, что стали жертвами преступлений[7]. Например, если чья-то украденная личная информация была предложена для продажи на криптомаркете, тогда, если жертва не была знакома с этими типами веб-сайтов, они не знали бы, что их личные данные были куплены кем-то другим.

Причина, по которой следует расследовать киберпреступность, заключается в том, что киберпреступники являются такими же жертвами сетевых атак, как и обычные граждане. Исследования показали, что чем больше времени вы проводите в Интернете, тем выше вероятность стать объектом интернет-преступности[8]. Поэтому знание того, как хакеры защищают себя, дает более глубокое понимание того, как обычные граждане могут защитить себя. Необходимо знать, какие стратегии используют преступники, чтобы лучше защитить себя

Криминологический портрет хакера:

Киберпреступники и их квалификация:

Возраст типичного киберпреступника колеблется от 20 до 35 лет. Большинство правонарушителей преимущественно мужчины, и они знакомы с системой, в которую пытаются проникнуть, или знают людей, знакомых с этими системами[9]. Большинство хакеров не имеют криминальной истории и имеют хороший социальный статус. Индивидуальные мотивы варьируются, но большинство людей сообщают, что они мотивированы деньгами или своим статусом[10]. Наконец, хакеры могут работать самостоятельно или в группе, однако, когда хакеры работают в группе, они редко организованы[11].

Основываясь на классификация хакеров и хакерских групп по уровню их квалификации и мотивов Сибрак создал обновленную типологическую модель, которая разделила мотивацию хакера на пять различных категорий: престиж, идеология, прибыль, месть и, наконец, отдых[12]. Для обеспечения гибкости типологии Сибрак также позволяет хакерским группам и хакерам иметь несколько мотивов для своих киберпреступлений. Это следует из предыдущих исследований, в которых предполагалось, что группы киберпреступности, как правило, не имеют строгого руководства, поэтому отдельные лица в группе могут инициировать деятельность по разным

причинам[13]. Престижные хакеры - это те, кто взламывает, чтобы завоевать уважение на форуме, веб-сайте или в другой форме сообщества. Сообщая о своих подвигах и методах этих хакеры надеются завоевать доверие своих сверстников, тем самым улучшая свое положение. К этой категории также могут относиться программисты, которые разрабатывают способы взлома хакерами систем. Они также могут завоевать уважение, предоставляя инструменты для хакеров в других категориях.

Следующая категория в типологии Сибрака - идеологические хакеры. Эти люди включают тех, кто называет себя хактивистами. Это означает, что эти люди связаны с более крупной причиной. Вместо того, чтобы использовать свои знания, чтобы заработать доверие или денежную выгоду, они используют свои навыки для так называемого большего блага[14]. В эту категорию входят такие группы, как Wikileaks, которые считают, что информация должна быть бесплатной для всех. В эту категорию также могут входить государственные субъекты, такие как те, кто создал вирус Stuxnet для атаки на иранскую ядерную программу.

Третья категория - это те, кто мотивирован прибылью. Основная задача этой группы - как заработать наибольшую сумму денег от частных лиц или от бизнеса. Эти хакеры в первую очередь нацелены на личную информацию, которая может быть продана в Интернете, такую как номера кредитных карт и номера социального страхования. Кроме того, они могут использовать эту информацию для мошеннических платежей или получения займов на имя физических лиц.

Четвертый тип хакеров - это те, кто жаждет мести. Эта группа считает, что они были в некотором роде обижены и хотят «отомстить» тем, кто обидел их. Ярким примером такого типа хакеров является группа Anonymous. Например, эта группа закрыла веб-сайт премьер-министра после того, как он попытался подвергнуть цензуре оскорбительный контент в Интернете[15].

Последний тип хакеров - рекреационные хакеры. Эта группа участвует во взломе, потому что они чувствуют необходимость бросить вызов самим себе или хотят расширить свои навыки. Рекреационные хакеры также пишут о своих подвигах, чтобы привлечь внимание. Это также группы, которые посещают соглашения о хакерстве, чтобы найти новые методы и установить связи в сообществе. В то время как эти группы могут хотеть знать хакерство для удовольствия, есть также те, кто взламывает, чтобы доказать свои способности своим сверстникам[16].

Киберпреступники также подвержены преступлениям, как и не преступники. Это связано с тем, что, хотя эти люди обладают большими техническими навыками и знаниями в области безопасности, ожидается, что киберпреступники проводят много времени в Интернете, и более активное знакомство предполагает больший потенциал для виктимизации[17]. Поскольку киберпреступники имеют больше знаний об эффективности меры безопасности, их знания и опыт работы с кибер-кражами позволяют лучше

понять преступность, связанную с использованием Интернета. Кроме того, киберпреступники используют ту же технологию, что и не киберпреступники. Следовательно, их компьютеры будут содержать те же уязвимости, которые позволяют их взломать.

Изучив, что такое киберпреступность и как она влияет на тех, кто является ее жертвой, можно понять, почему важно выяснить, какие превентивные методы эффективны против нее. Также важно понять “теорию рационального выбора” перед применением методов предотвращение. Это связано с тем, что теория рационального выбора является одной из основных теорий, лежащих в основе перспективы методов предотвращение.

Теоретическая основа предложенных методов предотвращения

Рациональный выбор

Перспектива рационального выбора основана на двух концепциях: утилитаризм и традиционная теория экономического выбора[18]. Во-первых, эти две теории утверждают: все, что люди делают направлено на получение удовольствие и на минимизацию боли. Во-вторых, люди будут взвешивать свои варианты и выбирать тот, который больше всего удовлетворит их потребности. Разумный выбор объединяет эти две идеи, чтобы теоретизировать, что преступники будут принимать решения из этих двух теории разумно и со свободной волей. Это означает, что когда кто-то выходит на улицу и совершает преступление, он делает это, потому что приходит к выводу, что возможная выгода от этого преступления перевешивает возможные издержки поимки. Кроме того, когда они принимают это решение, на них не влияют никакие другие факторы, кроме их собственного процесса принятия решений[19].

Еще один важный аспект, на который следует обратить внимание, - это как правонарушители выбирают свои цели. Исследования, посвященные кражам со взломом, наиболее близким к киберпреступлениям, показали, что при взломе грабителей выбираются различные факторы[20]. Было установлено, что предпочтения, мораль и простота доступа связаны с выбором цели[21]. Исследование наркоторговцев также показало, что те, кого выглядело легко обмануть, стали мишенью[22].

Есть две важные идеи, которые можно отнять после изучения теории рационального выбора. Во-первых, преступники делают рациональный выбор. Во-вторых, эти выборы основаны на факторах, связанных с преступлением, которое они хотят совершить. Эти две идеи означают, что существует ясный способ отговорить преступников от совершения преступлений. Это означает, что существует четкий способ отговорить преступников от совершения преступлений. Для этого, согласно рациональному выбору необходимо перевесить издержки совершения преступления.

Следующая точка зрения, методов предотвращения направлена на увеличение трудности в совершении преступления. Есть основания полагать, что увеличение трудных задач по сравнению с ожидаемыми

вознаграждениями может привести к тому, что потенциальные преступники будут воздерживаться от совершения конкретного преступления. Нарушение рационального процесса принятия решений предотвратить преступления. Поскольку взлом часто является преступлением, предшествующим кибер-воровству, из этого следует, что если киберпреступников отговорили от взлома, кибер-воровство также должно уменьшиться.

Превентивные методы:

1. «Используйте Pegasus или Thunderbird (от Mozilla) или веб-приложения, такие как Hotmail или Yahoo (In Firefox)».
2. «Установите хороший антивирус / антишпион»
3. «Хорошая антишпионовская программа»

Основной целью предотвращения ситуационной преступности является устранение возможности для преступности. Чтобы упростить комплексный подход к сокращению возможностей, Кларк предлагает структуру, состоящую из 25 методов, которые нацелены на то, чтобы убедить потенциального преступника в том, что стоимость совершения преступления перевешивает выгоду от этого преступления, в то же время устраняя оправдания для преступной деятельности. Кларк также утверждает, что меры по сокращению возможностей имеют три компонента. Во-первых, они направлены на конкретную форму преступления. Во-вторых, это связано с какими-то изменениями в среде. Наконец, эти изменения делают преступление более рискованным для преступника или дают преступнику меньшее вознаграждение. Метод предотвращения ситуационной преступности не стремится объяснить преступление, но предотвращает его совершение[23].

Кларк предлагает, что есть пять аспектов, которые, если их изменить, могут предотвратить преступность, влияя на оценку преступником возможности совершения преступления, - увеличивая усилия, необходимые для совершения преступления, увеличивая риски обнаружения и задержания, уменьшая вознаграждение, которое может накапливаться из преступления, устраняя провокации, которые могут вызвать преступное поведение, и, наконец, устраняя оправдания, которые могут быть использованы правонарушителями для оправдания своих действий. В каждой категории Кларк предлагает конкретные методы сокращения возможностей, в результате чего в общей сложности 25 методов сокращения возможностей могут быть применяется, чтобы отговорить преступников от выбора и действий против целей.

Первой категорией, предложенного метода предотвращения ситуационной преступности является увеличение усилий, которые требуются преступнику для совершения преступления. В эту категорию входят пять методов: целевое усиление, контроль доступа к объектам, выходы на экран, отклонение нарушителей и инструменты управления. Ужесточение целей подразумевает затруднение доступа потенциальных жертв к преступникам.

Следующая категория повышает риск обнаружения и задержания. Для этой категории первым методом является продление попечительства. Третий метод - уменьшить анонимность, например, используя настоящие имена в качестве пользователей на компьютере. Далее, это использование менеджеров мест, в том числе камеры видеонаблюдения или несколько кассиров на заправочной станции. Наконец, это усилить формальное наблюдение. Это означает, что у вас должны быть такие системы, как охранная сигнализация.

Следующая категория - это уменьшение вознаграждений, которые могут получить правонарушители.

В данной научной работе был представлен криминологический портрет киберпреступника, а также методы защиты, предлагаемые хакерами для защиты от интернет-виктимизации через призму предотвращения преступных ситуаций. Были изучены криминологические категории киберпреступника. В заключение, метод предотвращение преступление с учетом теории рационального выбора был изучен как самый эффективный и верный способ борьбы с киберпреступностью.

Список использованных источников:

1. Н.А. Биекенов, Некоторые проблемы обеспечения кибербезопасности в Республике Казахстан // Сетевое издание "Zakon.kz". 2014. https://www.zakon.kz/4627688-nekotorye-problemy-obespechenija.html
2. Баратов Т.А., Как уберечь себя от киберпреступников // Сетевое издание "Zakon.kz". 2018. https://www.zakon.kz/4943608-kak-uberech-sebya-ot-kiberprestupnikov.html
3. Dogaru O., Criminological characteristics of computer crime // Journal of Criminal Investigations. 2012 №5(1), P. 92-98
4. Holt, T. J., & Bossler, A. M. An assessment of the current state of cybercrime scholarship // Deviant Behavior. 2013 №35(1), P. 20-40
5. Ibrahim, S. Social and contextual taxonomy of cybercrime: socioeconomic theory of Nigerian cybercriminals // International Journal of Law, Crime and Justice, 2016 №47, P. 44-57
6. Dovidio, R., The evolution of computers and crime: complicating security practice // Security Journal. 2007 №20(1), P. 45-49
7. Kshetri, N., Cybercrime and cybersecurity in india: causes, consequences and implications for the future // Crime, Law and Social Change. 2016 №66(3), P. 313- 338
8. Pratt, T. C., Holtfreter, K., & Reisig, M. D. Routine online activity and internet fraud targeting: extending the generality of routine activity theory // Journal of Research in Crime and Delinquency. 2010 №47(3), P. 267-296
9. Dogaru O., Criminological characteristics of computer crime // Journal of Criminal Investigations. 2012 №5(1), P. 92-98

10. Seebruck, R., A typology of hackers: classifying cyber malfeasance using a weighted arc circumplex model // Digital Investigation. 2015 №14, P. 36-45
11. Choo K. R., Organized crime groups in cyberspace: a typology // Trends in Organized Crime. 2008 №11(3), P. 270-295
12. Seebruck, R. A typology of hackers: classifying cyber malfeasance using a weighted arc circumplex model // Digital Investigation. 2015 №14, P. 36-45
13. Broadhurst, R., Grabosky, P., Alazab, M., & Chon, S. Organizations and cyber crime: an analysis of the nature of groups engaged in cyber crime // International Journal of Cyber Criminology. 2014 №8(1), P. 1-20
14. Seebruck, R., A typology of hackers: classifying cyber malfeasance using a weighted arc circumplex model // Digital Investigation. 2015 №14, P. 36-45
15. Zetter, K., 'Anonymous' declares war on Australia over internet filtering // Retrieved. 2009 https://www.wired.com/2009/09/anonymous-hacks-australia/
16. Seebruck R., A typology of hackers: classifying cyber malfeasance using a weighted arc circumplex model // Digital Investigation. 2015 №14, P. 36-45
17. Pratt, T. C., Holtfreter, K., & Reisig, M. D., Routine online activity and internet fraud targeting: extending the generality of routine activity theory // Journal of Research in Crime and Delinquency. 2010 №47(3), P. 267-296
18. Adler, F., Mueller, G. O., & Laufer, W. S, Criminology // New York: McGraw-Hill Higher Education. 2010
19. Adler, F., Mueller, G. O., & Laufer, W. S, Criminology // New York: McGraw-Hill Higher Education. 2010
20. Townsley, M., Birks, D., Ruiter, S., Bernasco, W., & White, G., Target selection models with preference variation between offenders // Journal of Quantitative Criminology. 2016
21. Breetzke, G. D., & Cohn, E. G., Burglary in gated communities // International Criminal Justice Review. 2013
22. Jacques, Allen, & Wright., Drug dealers' rational choices on which customers to rip-off // International Journal of Drug Policy. 2014
23. Clarke R. V., Situational crime prevention: successful case studies // Boulder: Lynne Rienner. 2010