

Киберпреступность как угроза современному информационному обществу

*Преподаватель Информатики и ИКТ
Голуб И.Н.*

Аннотация: в данной статье исследуются детерминанты киберпреступности, проводится анализ правовой, научной и иной информации по теме, разрабатываются концептуальные методы воздействия, влияющие на снижение киберпреступности как правового явления, дается вывод по изложенному материалу.

Ключевые слова: *киберпреступность, Интернет, информация, информационные технологии, кибербезопасность.*

Стремительное развитие информационных технологий, повсеместное внедрение новейших разработок в обыденную жизнь граждан и корпораций неизбежно приводит к многочисленным последствиям, как положительным, так и отрицательным. По имеющимся исследованиям, вывод из строя электронно-вычислительной системы в результате преступления может привести даже самый крупный банк к полному разорению за четверо суток, а более мелкое учреждение – за сутки. Ярким примером данного положения может служить прекращение торгов всего лишь на два часа в Нью-Йоркской фондовой бирже, произошедшее 9 июня 2001г, из-за сбоя в работе нового компьютерного обеспечения, в результате чего общий ущерб составил порядка 1,5 млрд долларов США [1].

На сегодняшний день мировое информационное сообщество стремится создать безопасную и благоприятную среду для взаимодействия людей с помощью современных технологий. Несмотря на попытки обезопасить данные, находящиеся в информационном обороте, с каждым годом наблюдается рост числа преступлений, совершенных в сфере компьютерной информации. Спецификой данного явления как киберпреступность является высокий профессионализм субъекта преступления в сфере компьютерных технологий. При разработке защитных систем преступник подстраивается под них, что позволяет ему обходить многочисленные барьеры в виде программных средств. Из этого следует необходимость дальнейшего совершенствования не только информационной защиты, но и применения иных мер, способствующих предупреждению совершения такого рода преступлений.

Актуальность исследования выражается в стремительном развитии информационных технологий, что обуславливает разработку разнообразных защитных комплексов в борьбе за безопасное использование продукта научно-технического прогресса.

Целью исследования является разработка концептуальных теоретических положений в сфере киберпреступности с учетом собственного анализа актуальной правовой, научной и иной информации по данному исследованию с учетом обновленного законодательства, составление информационных буклетов по итогам проведенного структурированного изучения темы.

Задачами исследования будут выступать: анализ информации по теме, выявление способов защиты от киберпреступности с помощью наиболее общедоступных методов, разработка профилактических мер в данной сфере.

Гипотеза исследования: предполагается, что при успешной разработке комплекса защитных средств, применяемых в борьбе с киберпреступлениями их число значительно снизится.

Для начала следует указать на дефиницию киберпреступности. Под ней понимается родовое понятие, охватывающее как компьютерную преступность в узком значении этого слова (где компьютер является предметом, а информационная безопасность - объектом преступления), так и иные посягательства, где компьютеры используются как орудия или средства совершения преступлений против собственности, авторских прав, общественной безопасности или нравственности (например, компьютерное мошенничество и т.п.) [2]. Последние нередко именуются «связанными с компьютерными преступлениями». Примыкают к киберпреступности и некоторые действия, направленные на поддержание условий для ее существования и развития (использование электронной почты для коммуникации, создание собственных сайтов, направленных на распространение криминальной идеологии, а также обмен криминальным опытом и специальными познаниями).

Из истории компьютерных правонарушений известно, что впервые о них заговорили в период с 1969 по 1973 г., первоначально у правонарушителей были меркантильные интересы. Так, в одной из заметок Д. Фролов приводит следующие примеры: Альфонсе Конфессоре осуществил налоговое преступное деяние в необходимую ему сумму 620 тыс. долларов и в 1969 г. предстал перед североамериканским трибуналом. В 1973 г. казначей нью-йоркского Ситибанка, применив служебный компьютер, перебросил на собственный счет два миллиона долларов. Можно считать, что с данных правонарушений началась хроника компьютерных преступлений [3].

Для более точного понимания сути компьютерных преступлений необходимо их теоретическое раскрытие, основываясь на актуальном законодательстве. Конвенция Совета Европы о киберпреступности говорит о четырех типах компьютерных преступлений «в чистом виде», определяя их как преступления против конфиденциальности, целостности и доступности компьютерных данных и систем:

1. Незаконный доступ — ст. 2 (противоправный умышленный доступ

к компьютерной системе либо ее части);

2. Незаконный перехват — ст. 3 (противоправный умышленный перехват не предназначенных для общественности передач компьютерных данных на компьютерную систему, с нее либо в ее пределах);

3. Вмешательство в данные — ст. 4 (противоправное повреждение, удаление, нарушение, изменение либо пресечение компьютерных данных);

4. Вмешательство в систему — ст. 5 (серьезное противоправное препятствование функционированию компьютерной системы путем ввода, передачи, повреждения, удаления, нарушения, изменения либо пресечения компьютерных данных).

Исходя из данного описания киберпреступлений можно отметить, что именно эти 4 типа будут составлять основу для дальнейшей дифференциации и определения новых видов киберпреступлений. С данными типами преступлений коррелирует и содержание сети Интернет с точки зрения морали и нравственности. Из этого вытекает серьезная проблема «наполнения» данными разного рода всемирной сети. Предназначенные для удаления материалы включают детскую порнографию и высказывания на почве ненависти, а также содержание данных, связанное с диффамацией и критикой правительства, что вызывало в ряде случаев озабоченность в отношении соблюдения прав человека. Почти 24 процента общего объема глобального потока данных в Интернете представляют собой, по оценкам, нарушение авторских прав, причем наиболее высокий уровень загрузки материалов совместного пользования ("peer-to-peer" или "P2P") отмечается в странах Африки, Южной Америки и Западной и Южной Азии [4].

Важно упомянуть, что явление киберпреступности носит международный характер. Это означает, что для эффективной борьбы с различными киберпреступлениями и их производными необходима слаженность многочисленных развитых и развивающихся стран, совместная разработка законодательства в данной области, определения дальнейшего вектора развития в области профилактики киберпреступности. Стоит, однако сказать, что далеко не все страны обладают достаточными возможностями для борьбы с такого рода преступностью. На это указывает статистика: "отстающими" странами стали Таджикистан, Туркменистан, Сирия и Иран. Самый высокий процент заражений мобильным вредоносным ПО показал Иран - 52,68% пользователей было заражено в 2019 г. [5]. То есть существует очевидная взаимосвязь между экономическим уровнем развития страны и ее показателем в сфере наличия эффективных систем для предупреждения и борьбы с киберпреступлениями. То есть, для получения в процессе разработки наиболее результативных методов в сфере предупреждения и сдерживания киберпреступности необходима дальнейшая интеграция различных стран (в том числе и по уровню экономического развития). Важность этого тезиса заключается во взаимопомощи между странами на мировом уровне. Так, если у наименее развитой страны не имеется достаточно средств и методов для

борьбы с киберпреступлениями, ей на помощь должны приходить более развитые страны с целью поддержания должного уровня киберпреступности в стране.

Рассматривая российское законодательство в сфере киберпреступности, следует начать с указания на составы преступлений. Так, в УК РФ существует отдельная глава, в которой устанавливаются составы преступлений в сфере компьютерной информации: статья 272. Неправомерный доступ к компьютерной информации, статья 273. Создание, использование и распространение вредоносных компьютерных программ, статья 274. Нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей и статья 274.1. Неправомерное воздействие на критическую информационную инфраструктуру Российской Федерации [6].

Также в 2016 году утверждена новая Доктрина информационной безопасности России. В ней определены стратегические цели и основные направления обеспечения информационной безопасности, проанализированы основные информационные угрозы и дана оценка состоянию информационной безопасности. Результаты мониторинга реализации настоящей Доктрины отражаются в ежегодном докладе Секретаря Совета Безопасности Российской Федерации Президенту Российской Федерации о состоянии национальной безопасности и мерах по ее укреплению [7].

Следует указать в рассматриваемой теме на Федеральный закон от 27 июля 2006 г. N 149-ФЗ "Об информации, информационных технологиях и о защите информации" [8], который регулирует основные положения в сфере информации, устанавливает предписания и правила для определенных субъектов в сфере оборота информации, а также определяет их наиболее общую компетенцию. Так, согласно статье 16 данного Закона устанавливаются основные положения защиты информации, определяется федеральный орган, который уполномочен разрабатывать требования о защите информации. Исходя из анализа положений данного нормативного правового акта, можно утверждать, что данный закон устанавливает наиболее общие положения в сфере кибербезопасности.

Развитие законодательства и разработка инновационных проектов в данной сфере дает основания полагать, что в скором времени в России ситуация в области раскрытия киберпреступлений улучшится. Так, в рамках федерального проекта «Информационная безопасность» предусмотрены мероприятия, направленные на борьбу с киберпреступлениями. К примеру, создается отраслевой центр государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак (ГосСОПКА). Кроме того, ведется разработка киберполигона для обучения специалистов в этой области, а также создание национального удостоверяющего центра (он обеспечит устойчивость взаимодействия устройств в российском сегменте интернета) [9].

По данным ведомства, в 2022 году зарегистрировано на 27,6% меньше краж, на 29% – фактов мошенничества с использованием электронных средств платежа, на 22,5% – криминальных деяний в сфере компьютерной информации.

Обращаясь к актуальной статистике, следует указать, что общее количество инцидентов связанных с киберпреступностью в 2022 году увеличилось на 20,8%. Число успешных атак, направленных на веб-ресурсы организаций, увеличилось на 56%. Если в 2021 году веб-ресурсы компаний становились объектами атак в 17% случаев, то в 2022 году доля таких инцидентов составила 22%. Прирост доли инцидентов преимущественно произошёл в секторе СМИ, транспортной отрасли и госучреждениях в связи с атаками хактивистов, тогда как доля веб-атак направленных на ритейл, и раньше была высокой. Мы ждём, что в 2023 году продолжит расти число атак на веб-ресурсы организаций, в особенности это коснётся компаний, предоставляющих онлайн-услуги и собирающие большие объёмы данных о клиентах.

Логично говорить о том, что возможность полного искоренения киберпреступности невозможна в принципе, как и любой вид преступности – исходя из теории уголовного права. Таким образом, в этом плане необходимо наличие четких и конкретных мер по профилактике и борьбе с киберпреступностью на всех уровнях (международном и национальном).

Предупреждение преступности состоит из стратегий и мер, направленных на снижение риска совершения преступлений и нейтрализацию потенциально вредных последствий для частных лиц и общества. Обследования, в том числе проведенные в развивающихся странах, показывают, что большинство индивидуальных пользователей Интернета в настоящее время принимают основные меры предосторожности. Это использование различных антивирусных программ, переход только по проверенным интернет-ссылкам, воздержание от предоставления конфиденциальной информации непроверенным сайтам и пользователям (пароли от социальных сетей, номера мобильных телефонов, данные кредитной или дебетовой карты и т.д.).

По нашему мнению, одним из наиболее продуктивных способов борьбы с возрастанием киберпреступности будет являться пропаганда правил пользования информационными сетями для обычных граждан-пользователей Сети. Так, говоря о способах защиты в Интернете, следует указать на следующие положения: 1) используйте сложные и уникальные пароли для всех учетных записей; 2) не принимайте приглашения от незнакомцев в социальных сетях; 3) защищайте конфиденциальную и личную информацию; 4) обновляйте параметры конфиденциальности и антивирусное ПО; 5) всегда используйте безопасное подключение.

Исходя из вышесказанного можно сделать следующий вывод. Стремительное развитие информационных технологий неизбежно вызывает комплекс различных проблем в сфере охраны информации. Для наиболее успешной разработки систем профилактических мер создаются международные организации по борьбе с киберпреступностью, разрабатывается национальное законодательство с учетом развития технологий, внедряются новейшие проекты в данной сфере (например, создание Киберполиции в системе МВД). Данные мероприятия являются внешними, то есть они направлены прежде всего на защиту субъектов информационного оборота. Но важным положением также будет являться и самозащита пользователей Сети, предусмотрительность и аккуратность во время эксплуатации продуктов информационного прогресса. В дальнейшем видится дальнейшее усовершенствование информационных средств для сдерживания совершения кибератак, разработка наиболее эффективных профилактических мер в данной сфере, увеличение профессиональных кадров в системе МВД для эффективного расследования киберпреступлений (программистов, IT-специалистов), усиление мер уголовной ответственности за совершение преступлений в области компьютерной информации. Необходимость защиты от киберпреступников очевидна. Для этого итогом нашей работы был разработан информационный буклет для студентов нашего колледжа с профилактическими рекомендациями пользования интернет-пространства. Наша безопасность в наших руках!

Библиографический список:

1. Криминалистика: учебник / Т.В. Аверьянова, Р.С. Белкин, Ю.Г. Корухов, Е.Р. Россинская. -3-е изд., перераб. И доп. – М.: Норма: Инфра-М, 2010. -944 с.
2. Киберпреступность — определение, классификация интернет угроз. [Электронный ресурс]. — URL: <http://elcomrevue.ru/kibeoprestupnost-cto-eto/>.
3. Т.А. Ханов А.Ж. Нуркеев. Современные подходы к определению компьютерной преступности и особенности компьютерных преступлений // Известия Алтайского государственного университета. – 2017. - №1.
4. Группа экспертов для проведения всестороннего исследования киберпреступности. Всестороннее исследование проблемы киберпреступности и ответных мер со стороны государств-членов, международного сообщества и частного сектора // UNODC Publications. – 2013.- № 12.

5. Кибербезопасность в России хорошо отрегулирована. [Электронный ресурс]. — URL: <https://www.comnews.ru/content/204880/2020-03-05/2020-w10/kiberbezopasnost-rossii-khorosho-otregulirovana>.
6. Уголовный кодекс Российской Федерации от 13 июня 1996 №63-ФЗ // СЗ РФ. 1996г. №25. Ст. 2954.
7. Информационная безопасность: Учебное пособие. Авторы: Ясенов В.Н., Дорожкин А.В., Сочков А.Л., Ясенов О.В. Под общей редакцией проф. Ясенева В.Н. — Нижний Новгород: Нижегородский госуниверситет им. Н.И. Лобачевского, 2017. — 198 с.
8. Об информации, информационных технологиях и о защите информации : Федеральный закон от 27.07.2006 № 149-ФЗ // СЗ РФ. — 2006. — № 31 (Ч. 1). — Ст. 3448.
9. По цифровым следам: в РФ раскрывается лишь четверть киберпреступлений. [Электронный ресурс]. — URL: <https://iz.ru/962966/elena-sidorenko/po-tcifrovym-sledam-v-rf-raskryvaetsia-lish-chetvert-kiberprestuplenii>.
10. Киберпреступность и киберконфликты : Россия. [Электронный ресурс]. — URL: https://www.tadviser.ru/index.php/%D0%A1%D1%82%D0%B0%D1%82%D1%8C%D1%8F:%D0%9A%D0%B8%D0%B1%D0%B5%D1%80%D0%BF%D1%80%D0%B5%D1%81%D1%82%D1%83%D0%BF%D0%BD%D0%BE%D1%81%D1%82%D1%8C_%D0%B8_%D0%BA%D0%B8%D0%B1%D0%B5%D1%80%D0%BA%D0%BE%D0%BD%D1%84%D0%BB%D0%B8%D0%BA%D1%82%D1%8B_:_%D0%A0%D0%BE%D1%81%D1%81%D0%B8%D1%8F