ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ
ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«РОССИЙСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ПРАВОСУДИЯ»

КАЗАНСКИЙ ФИЛИАЛ

УГОЛОВНАЯ ПОЛИТИКА В УСЛОВИЯХ ЦИФРОВОЙ ТРАНСФОРМАЦИИ

(СБОРНИК СТАТЕЙ)

КАЗАНЬ
2022

УДК 34 (343,344)
ББК 67
А 38

Ответственный редактор:
Ефремова М.Г., профессор кафедры уголовно-правовых дисциплин ФГБОУВО « Российский государственный университет правосудия», д.ю.н., доцент.

УГОЛОВНАЯ ПОЛИТИКА В УСЛОВИЯХ ЦИФРОВОЙ ТРАНСФОРМАЦИИ: сборник статей материалов Всероссийской научно-практической конференции «Уголовная политика в условиях цифровой трансформации» / Отв. ред. М.А. Ефремова. – Казань: Отечество, 2022. – 169 с.
ISBN

А 38 В сборнике представлены материалы Всероссийской научно-практической конференции «Уголовная политика в условиях цифровой трансформации», проходившей 19 мая 2022 г. в Казанском филиале Российского государственного университета правосудия.

Для преподавателей и аспирантов юридических вузов, институтов повышения квалификации, работников судебной системы и правоохранительных органов.

Статьи печатаются в авторской редакции.

УДК 34 (343,344)
ББК 67

ISBN

Содержание

ВЛИЯНИЕ ЦИФРОВОЙ ТРАНСФОРМАЦИИ НА УГОЛОВНО-ПРОЦЕССУАЛЬНОЕ ПРАВО

ную сферу общества, поскольку используются в манипулятивных, дискредитирующих и провокационных целях. Рядовой пользователь глобальных сетей зачастую не обладает медиаграмотностью, для значительной части граждан сложно распознать ложное сообщение. Указанное свидетельствует о необходимости борьбы с фейками, в том числе и на законодательном уровне.

Сбалансированное использование уголовно-политических инструментов криминализации общественно опасных деяний способно обеспечить эффективную защиту важнейших социальных ценностей, не допуская избыточного ограничения уровня свободы личности.

Таким образом, полагаю, введение уголовной ответственности за распространение заведомо ложной информации является социально и политически обусловленным в условиях современной ситуации.

Стяжкина С.А.,
доцент кафедры уголовного права и криминологии Института права, социального управления и безопасности Удмуртского государственного университета, к.ю.н., доцент

Социальная инженерия как способ неправомерного доступа к компьютерной информации

Статья посвящена социальной инженерии как совокупности техник и методов, используемых для манипуляции жертвой с целью получения конфиденциальной информации или для выполнения ряда действий, которые могут привести к нарушению информационной безопасности. Впоследствии данная информация может быть использована для неправомерного доступа к компьютерной информации.

Ключевые слова: социальная инженерия; компьютерные преступления; неправомерный доступ к информации; конфиденциальность информации; защита информации.

Styazhkina S.A.

Social engineering as a way of illegal access to computer information

The article is devoted to social engineering as a set of techniques and methods used to manipulate the victim in order to obtain confidential information or to perform a series of actions that can lead to a violation of information security. Subsequently, this information can be used for unauthorized access to computer information.

Keywords: social engineering; computer crimes; illegal access to information; confidentiality of information; protection of information.

Проблема защиты информации на сегодняшний день является одной из самых актуальных. Реалии современной жизни таковы, что информация является одним из самых ценных ресурсов, обладание которой приносит огромную прибыль. Развитие информационных ресурсов, активное использование информационно-телекоммуникационных сетей, широкое внедрение во все сферы общественной жизни достижений информационных технологий требуют быстрого и адекватного реагирования правовой системы на меняющиеся условия жизни. К сожалению, следует отметить, что не всегда законодательство успевает регламентировать изменяющиеся социальные отношения, в том числе и в сфере надлежащего обеспечения защиты информации.

Шквал преступлений, совершаемых в киберпространстве, представляет серьезную угрозу для информационной безопасности как государства, общества, так и отдельных граждан, и организаций. На сегодняшний день, только по данным официальной статистики, уже более четверти преступлений совершаются с использованием информационно-телекоммуникационных технологий. Но большая часть преступлений, совершаемых в киберпространстве, остается за рамками официальной статистики.

К сожалению, следует отметить, что в основе совершения большинства преступлений лежит виктимологический фактор. По данным компаний, специализирующихся на изучении и выявлении киберугроз, до 80% преступлений в сфере компьютерной информации совершаются с помощью социальной инженерии[1]. Термин «социальная инженерия» все чаще используется в контексте информационной безопасности.

Социальная инженерия – это совокупность техник и методов, используемых для манипуляции жертвой с целью получения конфиденциальной информации или для выполнения ряда действий, которые могут привести к нарушению информационной безопасности[2]. Преступнику для получения информации не нужно взламывать логины, пароли, использовать вирусные программы, преодолевать сложные системы защиты. Методы социальной инженерии предполагают работу с жертвой, использование психологических приемов и методов воздействия на личность для получения необходимой информации. По мнению ряда исследований, именно человеческий фактор является самым слабым звеном в системе обеспечения защиты информационной безопасности. В арсенале преступников до-

1 URL: https://habr.com/ru/news/t/459278/.

2 Нарциссова С.Ю., Куликова Н.В. Проблемы социальной инженерии, информационной и кибербезопасности. М.: Инфра-М, 2021. С. 5.

вольно много различных способов и методов социальной инженерии: фишинг, вишинг, «троянский конь», «дорожное яблоко», «кви про кво» и т.д. Все они ориентированы на использование социально-психологических особенностей личности, особенно таких качеств и свойств, как легкомыслие, невежество, жадность, зависть, страх и т.д. Жертва под психологическим влиянием преступника сообщает всю необходимую информацию, с помощью которой лицо получает доступ к денежным средствам, находящимся на счетах, базам данных, персональным данным, сведениям, составляющим коммерческую, банковскую тайну и т.д.

Если с точки зрения механизма совершения преступления все достаточно ясно, то с позиций квалификации данных действий возникают вопросы. Следует отметить, что как в теории, так и в правоприменительной практике возникают серьезные проблемы и разногласия по вопросам квалификации действий, посягающих на различные виды информации, в том числе компьютерной.

Сама по себе социальная инженерия не является преступлением, это лишь способ, с помощью которого лицо получает доступ к конфиденциальной информации. Если при мошенничестве это выступает в качестве обмана как признака объективной стороны состава мошенничества, то в других преступлениях это не так очевидно и может вызвать трудности при их уголовно-правовой оценке.

В частности, в данной статье речь будет идти о таком преступлении, как неправомерный доступ к компьютерной информации (ст. 272 УК РФ). Следует отметить, что, несмотря на то, что данный состав преобладает в общей структуре преступлений в сфере компьютерной информации, тем не менее, на наш взгляд, он еще недооценен в правоприменительной практике. На сегодняшний день именно неправомерный доступ к компьютерной информации является одним из самых востребованных способов совершения других преступлений в киберпространстве, начиная от кражи, заканчивая экстремизмом.

Одной из проблем, возникающей при уголовно-правовой оценке, является определение объективной стороны рассматриваемого преступления. В частности, речь идет о понятии «неправомерного доступа» к компьютерной информации.

Общее понятие «доступа к компьютерной информации» содержится в Федеральном законе «Об информации, информационных технологиях и о защите информации» от 27.07.2006 № 149-ФЗ в ст. 2, где сказано, что «доступ к информации – возможность получения информации и ее использования». Более того, в Методических рекомендациях по осуществлению прокурорского надзора за исполнением законов при расследовании преступлений в сфере компьютерной

информации говорится, что «неправомерным считается доступ к конфиденциальной информации или информации, составляющей государственную тайну, лица, не обладающего необходимыми полномочиями (без согласия собственника или его законного представителя), при условии обеспечения специальных средств ее защиты.

Другими словами, неправомерный доступ к компьютерной информации – это незаконное либо не разрешенное собственником или иным ее законным владельцем использование возможности получения компьютерной информации»[1].

Здесь следует обратить внимание на признак неправомерности доступа. Неправомерный доступ означает незаконный либо не разрешенный собственником или законным владельцем. Можно сделать вывод, что существует два варианта неправомерного доступа. Первый это незаконный доступ. Незаконный означает, что доступ к информации запрещен действующим законодательством, т.е. речь идет об информации ограниченного доступа, это могут быть сведения, составляющие государственную тайну, налоговую тайну, банковскую тайну. Второй вариант неправомерного доступа предполагает доступ, не разрешенный собственником или иным владельцем. Здесь единственным критерием неправомерности будет выступать факт установления специальных средств защиты информации от свободного доступа, т.е. введение ограничений, не только технических, но и правовых. Предполагается, что законный владелец информации должен ограничить доступ к ней путем установления логинов, паролей, программного обеспечения, которые бы препятствовали свободному доступу к информации.

Причем, на наш взгляд, следует разграничивать технический доступ и правовой. У лица может быть технический доступ к любой информации в силу его специальности, профессии, роду деятельности (инженер, системный администратор и т.д.), но правового доступа у него не будет, так как владелец информации может запретить ему получать и использовать информацию. Правовые запреты должны содержаться в локальных актах организаций, должностных инструкциях, договорах и т.д.

Существует большое количество способов неправомерного доступа к компьютерной информации. Многие из них связаны со взломом логинов, паролей, использованием вредоносных компьютерных программ и т.д.

---

1 Методические рекомендации по осуществлению прокурорского надзора за исполнением законов при расследовании преступлений в сфере компьютерной информации. URL: https://legalacts.ru/doc/metodicheskie-rekomendatsii-po-osushchestvleniiu-prokurorskogo-nadzora-za/.

Но существуют способы, которые не требуют познаний в сфере компьютерных технологий и программирования. Речь идет о социальной инженерии. Преступник получает все необходимые сведения для доступа от самого потерпевшего. Жертвы сами сообщают лицу пароли, логины и т.д., используя которые преступники получают доступ к компьютерной информации. В связи с широко распространившимися случаями использования методов социальной инженерии в целях совершения различного рода преступлений, «Сбербанк выступил с инициативой криминализировать в Уголовном кодексе Российской Федерации нормы, содержащие ответственность за кражу sim-карт, фишинг и социальную инженерию»[1]. Представляется, что с учетом положений действующего уголовного законодательства нет необходимости в криминализации подобного рода действий. Уголовный кодекс РФ позволяет адекватно оценивать и квалифицировать подобного рода действия исходя из имеющихся составов преступлений.

Представляется, что в случаях, когда методы социальной инженерии выступают способом получения неправомерного доступа к компьютерной информации, то и квалификация должна быть по ст. 272 УК РФ при условии, что лицо получило доступ и наступили неблагоприятные последствия, предусмотренные в диспозиции статьи, такие как модификация, уничтожение, блокирование или копирование информации. В случаях если лицу не удалось получить доступ, по причинам от него не зависящим (был изменен пароль, действия были пресечены и т.д.), то квалификация может быть как приготовление к преступлению или покушение на преступление. Но в силу малозначительности деяния лицо не должно подлежать уголовной ответственности.

Социальная инженерия – это методы собирания необходимых сведений для получения доступа к компьютерной информации. Это всего лишь приготовительный этап, когда преступник лишь планирует будущее преступление. Сами по себе сведения о ПИН-кодах, логинах, паролях, номерах карт не являются предметами уголовно-правовой охраны, они лишь открывают возможности доступа к охраняемой информации. Таким образом, и сама по себе деятельность по собиранию такой информации не может рассматриваться как самостоятельное преступление, требующее уголовно-правовой квалификации.

1 Янгаева М.О. Методы (техники) социальной инженерии, используемые при совершении преступлений в сфере компьютерной информации // Криминалистика: вчера, сегодня, завтра. 2021. № 2 (18). С. 147.

Список литературы:

1. Методические рекомендации по осуществлению прокурорского надзора за исполнением законов при расследовании преступлений в сфере компьютерной информации. URL: https://legalacts.ru/doc/metodicheskie-rekomendatsii-po-osushchestvleniiu-prokurorskogo-nadzora-za/.
2. Нарциссова С.Ю., Куликова Н.В. Проблемы социальной инженерии, информационной и кибербезопасности. М.: Инфра-М, 2021. С. 5.
3. Янгаева М.О. Методы (техники) социальной инженерии, используемые при совершении преступлений в сфере компьютерной информации // Криминалистика: вчера, сегодня, завтра. 2021. № 2 (18). С. 147.

Тарасов В.Ю.,
старший преподаватель кафедры правового обеспечения национальной безопасности МИРЭА – Российского технологического университета,
Щевелева К.В.,
преподаватель кафедры правового обеспечения национальной безопасности МИРЭА – Российского технологического университета

Современные тенденции противодействия распространению терроризма, экстремизма и реабилитации нацизма в сети Интернет

В данной статье, авторами рассмотрены тенденции распространения терроризма, экстремизма и реабилитации нацизма в сети Интернет, а также перспективные возможности противодействия терроризму, экстремизму и реабилитации нацизма. Авторами предложены меры уголовно-правового регулирования деятельности по реабилитации нацизма, пределов уголовной ответственности, сформулированы предложения по внесению изменений в уголовное законодательство РФ для создания единообразного подхода к пониманию оснований освобождения от уголовной ответственности, обоснована необходимость использования поощрительных норм уголовного права в профилактике данной категории преступлений.

Ключевые слова: реабилитации нацизма; освобождение от уголовной ответственности; профилактика; пределы уголовной ответственности; поощрительные нормы.