

УДК 174.4

ФОРМИРОВАНИЕ ПРОФЕССИОНАЛЬНОЙ ТРУДОВОЙ ЭТИКИ СТУДЕНТОВ ИТ-СПЕЦИАЛЬНОСТЕЙ

Ткалин А.А., студент гр. ИС.205, V курс
Научный руководитель: Верчагина И.Ю., к.и.н., доцент
Кузбасский государственный технический университет
Имени Т.Ф. Горбачева, филиал в г. Белово
г. Белово

В связи с распространением цифровых технологий в России и в мире ежегодно растет количество преступлений, связанных с использованием информационных технологий. Хотя в Уголовном кодексе РФ глава 28 «Преступления в сфере компьютерной информации» появилась ещё в 1997 г. и первоначально включала в себя статьи 272-274 УК РФ, только в 2012 году в УК РФ были введены статьи, регламентирующие уголовную ответственность за различные виды кибер-мошенничества (ст. 159.3 и 159.6 УК РФ), формально не относящиеся к главе 28 УК РФ.

Так, по данным Генеральной прокуратуры РФ в нашей стране стабильно растет число преступлений, совершенных с использованием сети Интернет и средств мобильной связи. В 2023 году данная категория преступлений выросла на 39,3% по сравнению с аналогичным периодом 2022 г. Только за период с января по июнь 2023 года зарегистрировано более 210,8 тыс. различных мошенничеств. В структуре хищений данного типа значительная доля (79,1%) мошенничеств, совершенных дистанционно, с использованием информационно-телекоммуникационных технологий или в сфере компьютерной информации (166,8 тыс.). Темп их прироста относительно первого полугодия 2022 года увеличился на 40,5% [1]. Помимо увеличения числа данных преступлений еще одним тревожным фактором является их относительно невысокая раскрываемость: если раскрываемость краж составляет 48%, то раскрываемость мошенничеств - 22,8% [1].

Очевидно, что наиболее сложные среди данной категории преступлений невозможно совершить без профессиональных знаний в сфере информационных технологий, т.е. привлечения специалистов ИТ-профиля. Помимо таких общественно опасных деяний как преступления, специалисты ИТ-профиля могут быть вовлечены в иные виды деятельности, не влекущей уголовной ответственности, но причиняющей существенный вред общественным отношениям. Современные исследователи называют данный вид деятельности «киберагрессией», включающей в себя такие виды как флейминг, хейтинг, троллинг, киберсталкинг и кибербуллинг. Некоторые из данных «моделей поведения» могут осуществляться за денежное вознаграждение и восприниматься лицами, их совершающими, как «работа». Среди перечисленных видов кибе-

рагрессии наибольшую известность получил троллинг, понимаемый как размещение в сети интернет провокационных и агрессивных сообщений (комментариев).

Относительно высокий уровень анонимности в сети интернет и зачастую значительная территориальная удаленность пользователей друг от друга приводит к тому, что одним из важнейших факторов, определяющих поведение интернет-пользователей, являются их нравственные, этические установки. Еще большее значение нравственные категории приобретают для лиц, имеющих профессиональные знания и навыки в сфере ИТ. В тех странах, где интернет получил распространение еще в конце 1980-х – начале 1990-х гг., проблемы информационной и компьютерной этики стали частью общественной и научной дискуссии. Так, первый кодекс компьютерной этики был разработан в США еще в 1979 году, а его принятие было связано с осознанием того масштаба влияния, которое оказывают специалисты ИТ-профиля на благополучие всего общества. Позже были разработаны и приняты подобные кодексы во многих других организациях США, связанные со сферой ИТ.

В рамках данного исследования нами был проведен опрос, посвященный оценке сформированности категорий профессиональной этики у студентов, обучающихся по специальности среднего профессионального образования 09.02.07 «Информационные системы и программирование». Согласно учебному плану, на данной специальности СПО не предусмотрены дисциплины, непосредственно направленные на формирование норм профессиональной этики. Хотя такой результат как «соблюдение требований этических норм» заложен в рамках целого ряда учебных дисциплин, он не является определяющим. Аналогичным образом выглядит ситуация в рамках направления подготовки «Прикладная информатика».

Исследование проводилось с использованием двух методов, количественного и качественного: методом работы в фокус-группе и методом анкетирования. В работе фокус-группы приняло участие 7 студентов 3 курса (возраст участников 18-20 лет), в анкетировании – 30 студентов 2 курса указанной специальности. Работа фокус-группы была построена с помощью метода виньеток, т.е. студентам предлагались гипотетические ситуации, а участники эксперимента озвучивали свою реакцию на данную ситуацию. Всего было сформировано 9 ситуаций, причем первая и последняя фактически дублировали друг друга с целью выявления противоречий в ответах и устойчивости полученных оценок.

Первая предложенная ситуация была связана получением высоко оплачиваемой работы, но противоречащей взглядам и ценностям опрашиваемых. Последняя (9) ситуация фактически повторяла первую («если вам предложат работу администратора телеграм-канала с достаточно высокой оплатой, но содержание которого не соответствует вашим взглядам, согласитесь ли вы?»). Пять из семи опрошенных согласились выполнять работу, не соответствующую их моральным принципам, «если данная работа не будет криминальной» или «если это будет касаться политики». Только два участника отказались в

категорической форме. На аналогичный вопрос, фактически проверяющий устойчивость выбора, опрошенные ответили так же: трое отказались категорически, четверо опрошенных готовы выполнять данную работу, если им будет обеспечена личная безопасность и «в зависимости от контента».

Вторая предложенная ситуация («допускаете ли вы для себя участие в троллинге как работу?») вызвала отказ у двух опрошенных, тогда как пять человек были готовы сотрудничать с троллинговыми группами с различными оговорками: «анонимно», «в отношении совершеннолетних», «если не связано с разжиганием ненависти». Использование пиратского контента не вызвало у опрошенных фактически никаких моральных колебаний, все семь участников готовы использовать пиратский контент и только двое опрошенных готовы оплачивать ИТ-продукцию «в зависимости от качества и личных финансовых возможностей». Четвертая и пятая модельные ситуации так же фактически дублировали друг друга и были направлены на выявление готовности использовать конфиденциальную информацию личного или коммерческого плана, полученную в рамках профессиональной деятельности (работы программистом в фирме, организации). Опрошенные в большинстве своем не готовы продавать доступную им по роду деятельности коммерческую и (или) личную информацию, но готовы ее сохранить и «использовать» в случае «конфликта на предприятии», «несправедливого увольнения», «для личного использования».

Наибольшие дискуссии в ходе фокус группы вызвал шестой и седьмой вопросы о допустимости работать в качестве программиста в пространстве Darknet при гарантированной безопасности, анонимности (сопровождение нелегальных сделок). Трое из семи опрошенных допускают для себя такую ситуацию с различными оговорками: «в сложной жизненной ситуации», «если это не торговля наркотиками», двое готовы передавать информацию в правоохранительные органы. Все участники группы считают, что государство не должно устанавливать ограничения на сайты с контентом для взрослых, а вся ответственность должна быть возложена на владельцев и администраторов сайта (установление возрастных ограничений, дисклеймеры, отказ от размещения видео со сценами насилия и т.д.). Последний вопрос, связанный с деятельностью хакеров, свидетельствует об однозначно положительной оценке их деятельности: все семь опрошенных фактически ее одобряют.

Интерес представляет и вторая часть исследования, проведенная с помощью количественных методов (анкетирование) среди студентов данной специальности. Наибольший разброс мнений вызвали вопросы с наиболее выраженной этической оценкой. Так, при ответе на вопрос «допускаете ли вы для себя работу в качестве «интернет-тролля» (написание негативных комментариев за деньги)» 87% опрошенных ответили нет и только 10% готовы заниматься данной деятельностью.



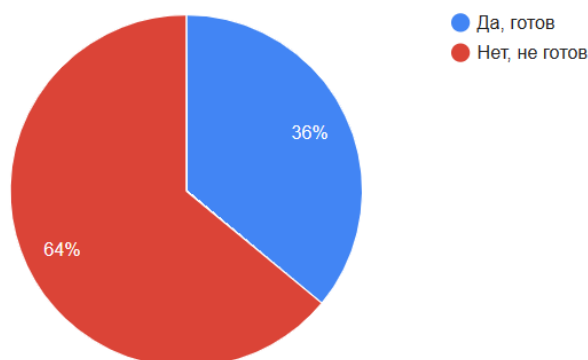
Фактические аналогичные ответы были получены на вопрос «допускаете ли вы для себя работу в качестве программиста в пространстве Darknet, если вам гарантирована безопасность, анонимность (например, сопровождение нелегальных сделок)», при ответе на которой 83% респондентов ответили, что не допускают для себя такой вид деятельности и только 17% рассматривают это как допустимую работу.



Такая модель поведения, как использование пиратского контента и допустимость хакерских атак, получила совершенно разную оценку среди участников фокус-группы и среди лиц, опрошенных с помощью метода анкетирования. В рамках фокус группы фактически никто из участников не осуждал использование пиратских сайтов и деятельность хакеров, тогда как проанкетированные ответили иначе: 53% опрошенных допускают использование пиратских сайтов, 47% - нет; 50% допускают хакерство и 50% выступают против данной деятельности. Подобное расхождение в оценках может свидетельствовать о том, что студенты, скорее всего используют пиратский контент (что косвенно подтверждают данные фокус группы), однако осознают моральную неоднозначность такого поведения.

Проанкетированные респонденты чаще признают готовность использовать информацию, полученную на работе, для дальнейшего использования (в т. ч. с целью извлечения прибыли, например, продажа базы данных): 36% готовы использовать такую информацию против 64% не готовых. Мнения по поводу государственных ограничений в сфере распространения информации

через интернет (прежде всего на сайты с порнографией, сценами насилия и т.д.) разделились поровну.



Подводя итоги проведенного исследования, можно сделать ряд выводов. Во-первых, количественные методы исследования дают несколько иную картину по сравнению с данными фокус-группы. Среди тех, кто отвечал на вопросы анкеты, более выражено негативное отношение к пиратским сайтам, деятельности хакеров по сравнению с участниками фокус-группы. При этом, такие формы поведения как модерирование сайтов с морально осуждаемым контентом воспринимаются большинством в обеих группах как негативное. Это позволяет нам сделать вывод о том, что профессиональная этика студентов находится в стадии формирования. Во-вторых, существует разница между моральными нормами (которые так или иначе усвоены большинством студентов) и оценкой своего поведения в потенциально возможных ситуациях.

Список литературы

1. Информационное агентство ТАСС (официальный сайт) [электронный ресурс] // <https://tass.ru/obschestvo/18417795> (дата обращения 18.03.2024)