

ния преступлений в области компьютерных технологий: 1) слабая изученность компьютерных преступлений с точки зрения криминологии; 2) постоянная модернизация и эволюция технических средств, а соответственно, и способов совершения преступлений в области цифровых технологий; 3) проявление большого интереса к изучению устройства и функционирования электронно-вычислительных машин со стороны молодежи, что может рассматриваться одновременно как позитивное и негативное явление; 4) недостаточность разработки теоретической модели преступлений в телекоммуникационной сфере.

К условиям, способствующим совершению цифровых преступлений, криминологи относят следующие: 1) чрезвычайно слабая регламентация отношений, которые возникают при применении и использовании информации и электронно-вычислительных устройств; 2) отсутствие норм в уголовном законодательстве, закрепляющих компьютерные преступления; 3) неготовность к борьбе с цифровой преступностью правоохранительных органов; 4) отсутствие обеспечивающих защиту компьютерной информации технических средств от воздействия преступных элементов; 5) полное или частичное отсутствие следовой информации о совершении преступления; 6) трудности, возникающие при установлении времени, места и способа совершения противоправного деяния.

Голубятников Д.А.

Московский областной филиал

Московского университета МВД России имени В.Я. Кикотя (пос. Старотеряево)

Научный руководитель Е.Н. Гордеева, кандидат педагогических наук

Основные детерминанты киберпреступности

В современном постиндустриальном обществе все большее значение приобретает использование информационных технологий, функционирование которых основано на принципах цифрового кодирования. Достижения научно-технологического прогресса внедряются во все сферы общественной жизни: дистанционная регистрация на общегосударственных и муниципальных информационных ресурсах, оплата коммунальных платежей, осуществление банковских операций, приобретение товаров и услуг, получение образования и т.д. Вполне естественно, что полноценное функционирование всех институтов общества невозможно без использования электронно-вычислительной техники, способной посредством серверного соединения подключаться к глобальной информационной сети Интернет. Все большее количество транснациональных корпораций и частных организаций дифференцируют рабочие места, требующие, соответственно, компетентных специалистов с техническим

образованием, способных не только качественно выполнять поставленные перед ними задачи, но и устранять возникающие с определенной периодичностью технические неполадки. Отраслевое многообразие востребованных услуг настолько велико, что их реализация в большинстве случаев осуществляется в несколько этапов. Поставщики товаров и услуг все чаще прибегают к помощи специалистов в области и маркетинга и таргетинга. Разумеется, речь идет не только о производстве, распределении, обмене и потреблении материальных благ, но и об объектах интеллектуальной собственности, удовлетворяющих идеальные потребности человечества.

Изучение научных работ Т.А. Далгалы¹, К.Н. Евдокимова², М.К.Кумышевой³ позволило нам выделить наиболее часто встречающиеся типы киберпреступлений:

- мошенничество с использованием различных сервисов электронной почты;
- незаконное завладение и использование личных данных пользователей в целях шантажа и получения денежной компенсации;
- мошенничество в сфере осуществления электронных платежей и банковских переводов;
- незаконное завладение и продажа конфиденциальных корпоративных данных;
- интернет-рассылка вредоносного программного обеспечения (вирусов) с целью выведения персональной электронно-вычислительной техники из строя;
- несанкционированное получение доступа к каналам переговоров государственных организаций с целью завладения конфиденциальной информацией – кибершпионаж.

Приведенный типовой список не является исчерпывающим и постоянно дифференцируется ввиду высокой латентности и мобильности лиц, специализирующихся на совершении преступлений в указанной сфере.

Учеными-криминологами в результате многочисленных научных исследований установлены причинно-следственные связи между характеристиками личности, обуславливающими ее поведение, а также социальным положением и степенью вероятности подвергнуться насилию, стать жертвой различного рода хищений, причинения вреда здоровью, убийств.

¹ Далгалы Т.А. Киберкриминология: вызовы XXI века // Российская юстиция. 2020. № 10. С. 19-21.

² Евдокимов К.Н. Вредоносные компьютерные программы как орудие и средство совершения преступлений: онтологические и гносеологические аспекты // Российская юстиция. 2020. № 3. С. 56-58.

³ Кумышева М.К. Кадровое обеспечение противодействия кибертерроризму в Российской Федерации // «Черные дыры» в российском законодательстве. 2017. № 3. С.85-86.

В свою очередь, история мировой преступности в информационной среде, в частности в сети Интернет, измеряется гораздо более коротким промежутком времени, в связи с чем в существующих криминологических исследованиях в сфере интернет-преступности зачастую не уделяется требуемого внимания проблеме виктимологии жертв киберпреступности. Так, криминологами при анализе отдельных видов киберпреступлений не всегда прослеживается взаимосвязь с другими видами преступлений, не рассматривается все явление в целом.

Интернет-преступность не носит однородный характер, и поэтому причины виктимности в зависимости от подвида деяний могут существенно различаться: неправомерный доступ к компьютерной информации (ст. 272 УК РФ) путем использования похищенных паролей доступа к различным интернет-ресурсам; умышленное уничтожение или повреждение имущества (ст. 167 УК РФ); распространение вредоносных программ (ст. 273 УК РФ); интернет-мошенничество (ст. 159 УК РФ) и др.

Проведенными криминологическими исследованиями выявлено, что пренебрежение средствами компьютерной защиты носит повсеместный характер, из чего следует вывод о том, что основным виктимологическим фактором является несоблюдение потерпевшим мер информационной безопасности, а не личное знакомство с преступником, антропологические характеристики жертвы или какие-либо другие факторы виктимизации.

К числу причин латентности можно отнести то, что значительная часть жертв не в состоянии обнаружить факт совершения преступления, так как многие из интернет-преступлений не оставляют следов: например, неправомерный доступ к персональным данным пользователя Интернет без причинения ему материального ущерба, являющийся достаточно распространенным в настоящее время.

Активными мерами в борьбе с этим видом преступлений являются разработка и внедрение системы виктимологической профилактики интернет-преступлений. Важно, во-первых, создать систему мер правовой пропаганды и повышения уровня правосознания граждан, во-вторых, выстроить эффективную криминологическую профилактику, направленную на повышение технического уровня пользователей с учетом соответствующей аудитории: интернет-пользователей, которые не используют средства защиты или не знают о существовании таковых, и профессиональных пользователей, которым необходимо получать информацию о новых внедрениях в сфере компьютерной безопасности. Рекомендуемые средства защиты должны ранжироваться в зависимости от ценности защищаемых компьютерных данных и навыков пользователя.

Резюмируя вышесказанное, необходимо обозначить, что выявление ключевых личностных характеристик жертв преступлений в сфере цифровых технологий позволяет значительно упростить процесс установления обстоя-

тельств, подлежащих доказыванию, а также пути следования злоумышленников в сети.

Герасимов Д.С.

Могилевский институт МВД Республики Беларусь
Научный руководитель О.А. Лукина, кандидат филологических наук, доцент

Судебный процесс над Катюшей Масловой в романе Л.Н. Толстого «Воскресение»: юридический аспект

«Воскресение» – это последний роман Льва Николаевича Толстого, написанный им в 1889-1899 гг.¹ В нем показана социальная панорама русской жизни конца XIX в. от высших до низших слоев: в романе фигурируют аристократы, петербургские чиновники, крестьяне, каторжники, революционеры и политические заключенные.

В первой части романа Л.Н. Толстой изображает судебный процесс над Катюшей Масловой. Цель данной работы – дать юридическую оценку действиям участников уголовного процесса.

17 января 188* в гостинице «Мавритания» произошло преступление: было найдено тело купца второй гильдии Ферапонта Емельяновича Смелкова. Через несколько дней вернулся его друг и выразил подозрения в отравлении купца и похищении бывших при нем денег. Был осуществлен судебно-медицинский осмотр трупа, в ходе которого обнаружилось присутствие яда в организме покойного купца. В качестве обвиняемых были привлечены Маслова, Бочкова и Картинкин.

Катюша Маслова была отправлена Смелковым из дома терпимости, где она работала, в гостиницу, чтобы привести купцу деньги. Она приехала и в присутствии работников гостиницы Евфимьи Бочковой и Симона Картинкина отперла чемодан и взяла из него 40 рублей серебром. При вторичном своем приезде по внушению Картинкина Маслова дала выпить купцу, как она думала, снотворное. На следующее утро купец умер, а деньги с чемодана пропали. Было возбуждено уголовное дело по факту смерти купца. Состоялся суд, который подробно описан Л.Н. Толстым в романе.

В XIX веке решение о виновности или невиновности обвиняемого принимали присяжные. Присяжные – люди без юридического образования (купцы, военные, учителя, дворяне и др.)

Устав от долгого суда, присяжные по недоразумению сделали Катюшу Маслову виновной в убийстве купца. «Все так устали, так запутались в спорах,

¹ Толстой Л.Н. Воскресение : роман. М.: ТЕРРА, 1993. 552 с.