Keywords: international cooperation, law enforcement agencies, transnational crime, international organizations, interaction, international legal acts, forms of cooperation, legal assistance.

УДК 343.4

***В.В. Вабищевич**, аспирант кафедры уголовного права юридического факультета Белорусского государственного университета (e-mail: r999m@mail.ru)*

КРИМИНОЛОГИЧЕСКОЕ ПРОГНОЗИРОВАНИЕ И ПРЕДУПРЕЖДЕНИЕ ПРОТИВОПРАВНОГО ВМЕШАТЕЛЬСТВА В ПЕРСОНАЛЬНЫЕ ДАННЫЕ

Рассматриваются криминологические риски, способствующие росту преступных посягательств на персональные данные. Акцентируется внимание на том, что информационно-коммуникационные технологии внедряются и развиваются значительно быстрее, чем законодательные и правоохранительные органы могут реагировать на этот рост. Предлагаются меры, направленные на предупреждение и профилактику посягательств на персональные данные. Отмечается, что действующие нормы уголовного права не в полной мере учитывают специфику института персональных данных. Указывается на необходимость наладить освещение проблем последствий посягательств на персональные данные в средствах массовой информации для преодоления правового нигилизма руководителей учреждений и предприятий, а также отдельных граждан.

Ключевые слова: персональные данные, криминологические риски, защита информации, совершенствование законодательства, конституционные права, информационная безопасность.

Анонимность глобальных информационных сетей, быстрота передачи информации и доступность работы с ними позволяют использовать данные преимущества для совершения противоправных деяний. Структура киберпреступности, к которой преимущественно относятся посягательства на персональные данные, заметно отличается в разных странах и зависит от характера и степени развития информационных технологий, распространения сети Интернет, использования электронных сервисов, электронной коммерции и т. п. [1]

Президент Республики Беларусь подчеркнул, что технологичность открывает новые возможности для преступного вмешательства, несанкционированного получения и использования данных, в том числе личных, на что надо обратить внимание. И в этой связи необходимо не только принимать оперативные меры реагирования на подобные угрозы, но и действовать на их упреждение.

Угроза таких преступлений составляет серьезную проблему для общества, а борьба с ними является стратегически важной задачей для правоохранительных органов, особенно в части, касающейся реализации мер, направленных на эффективное противодействие росту киберпреступлений, своевременное установление лиц, совершивших преступные деяния, и получение доказательств, подтверждающих их совершение [2]. Знание типов личности преступников необходимо как для раскрытия уже совершенных ими преступлений, так и для их предупреждения [3, с. 64].

Исследователи к причинам и условиями посягательств на персональные данные относят различные обстоятельства. Г.Г. Зуйков, например, определяет совокупность условий и причин, которые вызывают совершение преступлений, и относит к ним следующие:

прямую причину посягательства;

условия, способствующие действию прямых причин и конкретному преступному деянию;

обстоятельства, формирующие прямые причины, а также условия, которые способствуют действию факторов, определяющих причину.

Прямой причиной, по мнению автора, обычно выступают антисоциальная направленность личности, а сами посягательства на персональные данные с субъективной стороны совершаются только умышленно [4].

С.И. Ушаков разделяет все обстоятельства, формирующие антисоциальную направленность, на субъективные и объективные условия, к которым относит непродуманную кадровую политику и ненадлежащее отношение к вопросу обеспечения защиты информации [5].

Е.А. Маслакова указывает, что довольно часто в компаниях, обрабатывающих большие объемы информации, отсутствуют отделы или службы по обеспечению информационной безопасности [6].

Так, в Германии были проведены виктимологические исследования, в ходе которых изучался опыт пострадавших от интернет-преступлений. Опрошенные респонденты отметили ряд последствий:

ущерб, нанесенный использованием вредоносного программного обеспечения через Интернет (компьютер был до такой степени заражен вирусами, «червями» или «троянами», что это повлекло за собой потерю данных или материальный ущерб);

неправомерное использование персональных данных при пользовании Интернетом (номер банковской карты, данные кредитной карты, право доступа к компьютеру);

намеренное и неоднократное преследование и обременение своим присутствием или вниманием (сталкинг), а также психологическое насилие посредством фотографирования, постановки в неловкое положение, угроз [7].

В связи с создавшейся тенденцией такого вмешательства видится необходимым рассмотреть возможность проведения виктимологических исследований и в Республике Беларусь, что позволит законодателям и правоприменителям более четко сформулировать элементы составов преступлений.

В целом к условиям, способствующим совершению посягательств на персональные данные, можно отнести следующие.

1. Информационно-коммуникационные технологии внедряются и развиваются значительно быстрее, чем законодательные и правоохранительные органы могут реагировать на этот рост.

Эмпирическое исследование интернет-преступности обусловлено эволюцией преступного профессионализма – использованием новых компьютерных технологий при совершении деяний, признаки которых не содержатся в уголовно-правовых нормах [8].

Только в Беларуси в рамках Евразийского экономического союза в системе законодательства отсутствует специализированный нормативный правовой акт, посвященный охране персональных данных. Беларусь не присоединилась к Конвенции Совета Европы «О защите частных лиц в отношении автоматизированной обработки данных личного характера».

В Уголовном кодексе Республики Беларусь (далее – УК) отсутствуют специальные составы преступлений, предусматривающие в качестве непосредственного объекта защиту персональных данных, а действующие редакции статей УК, так или иначе связанные с посягательством на персональные данные, не претерпели существенных изменений с 1999 г., т. е. с момента принятия уголовного закона.

Однако О.А. Зигмунт отмечает, что проблема отставания уголовного законодательства от криминальной действительности, порождающей высокую латентность и незащищенность граждан в информационной сфере, наблюдается и в европейских государствах, и в России [9].

2. Глобальность и трансграничность информационных систем.

Возможность манипуляций преступника с идентичностью (использование чужих имен, адресов, паролей и т. п.) создает ситуации, когда он находится на одном континенте, преступление непосредственно совершается на другом, а последствия преступления наступают на третьем.

Так, Т.Л. Тропина, В.А. Номоконов отмечают, что угроза киберпреступности превратилась в острую проблему, требующую координации действий на международном уровне. С того момента, когда государство включается в информационный обмен посредством сети Интернет, оно само и его граждане становятся уязвимыми для посягательств из любой точки земного шара [1].

3. Количество пользователей и анонимность сети Интернет.

С увеличением количества пользователей увеличивается возможность использования сети для совершения преступлений, а также растет потенциальная возможность стать их жертвой. Анонимность сети Интернет затрудняет обнаружение преступников.

4. Латентность, в том числе искусственная.

Преступные манипуляции с персональными данными, которые хранятся в автоматизированных информационных системах, являются достаточно латентными, что ограничивает применение мер юридической ответственности к потенциальным преступникам. Как отмечает Д.А. Ястребов, опросы следователей и судей, предпринимателей и потерпевших от неправомер-

ного доступа к компьютерной информации, в том числе персональным данным, позволили выявить такую тенденцию, как рост латентности данного вида преступлений [10].

Автор подчеркивает, что одним из путей преодоления латентности преступлений в сфере высоких технологий является преодоление правового нигилизма руководителей учреждений, предприятий, организаций, а также отдельных граждан путем освещения проблем компьютерной преступности в средствах массовой информации.

К причинам искусственной латентности компьютерной преступности в первую очередь относят нежелание потерпевшей стороны сообщать в правоохранительные органы о преступных посягательствах на их компьютерные системы.

5. Низкая грамотность в правовой и информационной сферах.

Эксперты отмечают, что не все пользователи осознают необходимость сохранности личной информации. Очень часто потерпевшие даже не догадываются о преступных действиях, совершенных против них и направленных на нарушение конфиденциальности информации, так как в отличие от бумажных носителей информация никуда не исчезает. Кроме этого, до сих пор лицо, совершившее преступление в компьютерной сфере, как правило, рассматривают как гения и не относят к разряду типичных уголовников («эффект Робина Гуда») [10].

Порою пренебрежительность и неосведомленность владельцев компьютерной информации способствует привлечению внимания преступных элементов к ним. В связи с этим необходимо наладить освещение тяжести последствий совершения посягательств на персональные данные в средствах массовой информации для преодоления правового нигилизма.

6. Сложный процесс изобличения и наказания виновных.

«Компьютерный преступник» – это только один из видов субъектов посягательства на персональные данные. Е.В. Беляев определяет, что компьютерные преступники подразделяются на начинающих (школьники, студенты), закрепившихся (технические консультанты, системные администраторы), профессионалов (начальники отделов информационных технологий в банках, государственных учреждения). Они отличаются тем, что высокая техническая подготовленность – их основная черта, высокая латентность преступлений – основа их мотивации, внутренняя предрасположенность – основное условие становления на преступном пути. По данной причине портрет личности «компьютерного преступника» можно определить на 30–40 %, что делает изобличение и наказание виновных для правоохранителей достаточно сложным [11].

Для преодоления данной проблемы необходимо наладить повышение эффективности правоохранительной деятельности, требовательности к уровню профессионализма работников правоохранительных органов в сфере защиты персональных данных.

Некоторые авторы предлагают создавать на базе государственных учреждений специальные факультеты, где могла бы вестись подготовка специалистов в области компьютерной безопасности, а также предусмотреть постоянное функционирование системы переподготовки специалистов по профилактике и расследованию преступлений в сфере информационной безопасности [12, с. 116–127]. Координация действий заинтересованных структур в ее обеспечении позволит проводить профилактику преступлений и эффективно взаимодействовать при обнаружении признаков совершения преступления [13, с. 463].

Специалисты в России указывают на отсутствие четкого алгоритма взаимодействия подразделений полиции и других структур, что ведет к тому, что большая часть преступлений остается нераскрытой, оперативники не могут получить достаточных данных для квалификации преступления. Кроме того, кадровый состав суда, прокуратуры и полиции не имеет надлежащего уровня подготовки для профилактики таких преступлений и их эффективного расследования.

К особенностям посягательств на персональные данные можно отнести:

тенденцию к увеличению числа лиц женского пола, совершающих компьютерные преступления [14];

динамику повышения доли женщин среди лиц, совершивших преступления в сфере высоких технологий, обусловленного профессиональной ориентацией (секретарь, бухгалтер, контролер, делопроизводитель, кассир и др.) на использование компьютерной техники в работе [15];

рост посягательств на персональные данные, совершенных лицами до шестнадцати лет (например, подростки украли жесткие диски с личными данными учеников и использовали их в своих целях) [16].

По мнению известного американского специалиста по борьбе с фишингом (разновидность компьютерного мошенничества) Лэнса Джеймса, в XXI в. наибольшее распространение среди компьютерных преступников получили скрипткидди (script kiddies) [17, с. 42], особенностями которых является их юный возраст, непрофессиональные хакерские способности, наличие свободного времени, упорство в достижении поставленной цели, использование уже готовых кодов, разработанных специалистами [17, с. 43].

Таким образом, в соответствии с вышеизложенным можно сделать выводы:

Действующие нормы уголовного права не в полной мере учитывают специфику института персональных данных.

К криминологическим рискам, способствующим совершению посягательств на персональные данные, следует отнести: быстрый рост развития информационно-коммуникационных технологий по сравнению с реагированием законодательных и правоохранительных органов на этот рост; глобальность и трансграничность информационных систем; рост количества пользователей и анонимность сети Интернет; латентность; низкую грамотность граждан в правовой и информационной сферах; сложный процесс изобличения и наказания виновных лиц и др.

В целях профилактики посягательств на персональные данные необходимо: наладить освещение их последствий в средствах массовой информации; рассмотреть возможность проведения виктимологических исследований; принять меры по повышению эффективности правоохранительной деятельности, требований к уровню профессионализма работников правоохранительных органов в сфере защиты персональных данных; наладить координацию действий заинтересованных структур в обеспечении компьютерной безопасности и др.

Список использованных источников

1. Номоконов, В.А. Киберпреступность: угрозы, прогнозы, проблемы борьбы / В.А. Номоконов, Т.Л. Тропина // Information Technology and Security. – 2013. – № 1. – С. 86–94.

2. Чекунов, И.Г. Криминологические и уголовно-правовые аспекты предупреждения киберпреступлений / И.Г. Чекунов // Росс. следователь. – М. : Юрист, 2013. – № 3. – С. 36–43.

3. Юзиханова, Э.Г. Криминологическая характеристика личности преступника, совершающего преступления против собственности в нефтегазовом комплексе / Э.Г. Юзиханова, С.А. Лысенко // Юрид. наука и правоохран. практика. – 2011. – № 3. – С. 61–65.

4. Зуйков, Г.Г. К вопросу о понятии причин преступления и условий, способствующих его совершению / Г.Г. Зуйков // Вопр. предупрежд. преступности. – № 2. – 2005. – С. 15.

5. Ушаков, С.И. Преступления в сфере обращения компьютерной информации / С.И. Ушаков // Теория, законодательство, практика. – Ростов н/Д, 2001. – С. 169.

6. Маслакова, Е.А. История правового регулирования уголовной ответственности за компьютерные преступления / Е.А. Маслакова // Информац. право. – 2006. – № 4. – С. 27.

7. Зигмунт, О.А. Кибер- и интернет-преступность в Германии и России: возможности сравнительного исследования / О.А. Зигмунт, А.В. Петровский // Юрид. наука и правоохран. практика. – 2015. – № 4. – С. 180–188.

8. Тропина, Т.Л. Борьба с киберпреступностью: возможна ли разработка универсального механизма? / Т.Л. Тропина // Междунар. правосудие. – 2012. – № 3. – С. 86–95.

9. Зигмунт, О.А. Компьютерная преступность в Германии / О.А. Зигмунт // Преступность и социальный контроль в обществе постмодерна : сб. материалов Междунар. Балт. криминолог. конф. : в 2 ч. – СПб. : Алеф-Пресс, 2015. – Ч. 1. – С. 157–159.

10. Ястребов, Д.А. Вопрос о латентности неправомерного доступа к компьютерной информации в Российской Федерации / Д.А. Ястребов // Юрид. мир. – 2008. – № 10. – С. 61–64.

11. Беляев, Е.В. Типы личности «компьютерного преступника» / Е.В. Беляев // Законодательство и экономика. – 2014. – № 5. – С. 74–77.

12. Подольный, Н.А. Отдельные проблемы расследования преступлений, совершенных с применением компьютерных технологий / Н.А. Подольный // Библ. криминалиста. – 2013. – № 5. – С. 116–127.

13. Россинская, Е.Р. Криминалистика / Е.Р. Россинская. – М. : Норма ; ИНФРА-М, 2012.

14. Попов, А.Б. Криминологическая характеристика личности, совершающего преступление, предусмотренное ст. 272 УК РФ / А.Б. Попов // Вестн. Тамб. ун-та. Сер. Гуманит. науки. – 2009. – № 8. – С. 411–413.

15. Дьяков, В.В. Указ. соч. 8. – С. 129–131.

16. Подростки украли жесткие диски с данными ЕГЭ. Но там оказались списки старшеклассников и перечень предметов [Электронный ресурс]. – Режим доступа: https://mel.fm/novosti/8217506-podrostki-ukrali-zhestkiye-diski-s-dannymi-yege-no-tam-okazalis-tolko-spiski-starsheklassnikov-i-pra. – Дата доступа: 04.06.2019.

17. Джеймс, Л. Фишинг. Техника компьютерных преступлений / Л. Джеймс ; пер. с англ. Р. В. Гадицкого. – М. : НТ Пресс, 2008. – С. 320.

Дата поступления в редакцию: 05.09.19

***V.V. Vabischevich**, Postgraduate student of the Department of Criminal Law of the Faculty of Law of the Belarusian state University*

CRIMINOLOGICAL PREDICTION AND PREVENTION OF ILLEGAL INTERFERENCE WITH PERSONAL DATA

Criminological risks contributing to the growth of criminal encroachments on personal data are considered. It is emphasized that information and communication technologies are being introduced and developed much faster than legislative and law enforcement agencies can respond to this growth. Proposals are made for measures aimed at preventing and preventing attacks on personal data. It is noted that the current norms of criminal law do not fully provide for all the specifics of the Institute of personal data. It is pointed out that it is necessary to establish coverage of the consequences of attacks on personal data in the media to overcome the legal nihilism of heads of institutions, enterprises and individuals.

Keywords: personal data; criminological risks; information protection; improvement of legislation; constitutional rights; information security.

УДК 343.8

***А.Г. Горбель**, адъюнкт научно-педагогического факультета Академии МВД Республики Беларусь*
(e-mail: alesya-radchenko@mail.ru)

КРИМИНОЛОГИЧЕСКАЯ ХАРАКТЕРИСТИКА ЖЕНЩИНЫ, СТРАДАЮЩЕЙ АЛКОГОЛИЗМОМ

Рассматривается криминологическая характеристика женщины отклоняющегося поведения, связанного с употреблением спиртных напитков. Излагаются причины и условия, ситуации в различных сферах жизнедеятельности, способствующие вовлечению лиц женского пола в употребление алкоголя. Представлены основные признаки, характеристики, свойства личности женщин, страдающих алкоголизмом, их социальные связи и позиции на уровне семьи, в сфере труда, неформального общения. Составлен обобщенный криминологический портрет указанного типа отклоняющегося поведения.

Ключевые слова: социальные отклонения, пьянство, алкоголизм, женщина, злоупотребляющая спиртными напитками, характеристики женщины, страдающей алкоголизмом, профилактика пьянства и алкоголизма женщин.

Поведение человека продиктовано определенными социальными и правовыми нормами. Отступление либо нарушение сложившихся социальных норм порождает социальные отклонения, которые проявляются в индивидуальных поступках и поведении личности. Из всего перечня таких отклонений [1, с. 7] наиболее распространенными являются пьянство и алкоголизм. Их опасность заключается в том, что злоупотребление спиртными напитками подрывает здоровье человека, влияет на количество самоубийств, характер административных проступков, состояние и динамику преступности, ведет к социальному заражению нации.

О распространенности указанного негативного явления в стране свидетельствуют следующие статистические сведения. В 2018 г. около 163 тыс. граждан состояли на учете с синдромом зависимости от спиртных напитков. Кроме того, около 90 тыс. находятся под наблюдением медицинских работников по причине злоупотребления алкоголем [2, с. 18]. Значительная часть граждан (из них более 15 % женщин) проходят медико-социальную реадаптацию в лечебно-трудовых профилакториях, функционирующих на территории Беларуси.

Несмотря на незначительный удельный вес «пьяной» преступности во всем массиве общественно опасных деяний – около одной пятой,– в последние годы около четырех пятых долей убийств и угроз убийством, фактов умышленного причинения тяжких телесных повреждений, сопротивления сотрудникам органов внутренних дел, а также половина изнасилований совершаются в состоянии алкогольного опьянения. На этой почве совершается более трех пятых долей грабежей и разбоев, хулиганств, угонов транспортных средств, более двух пятых – насильственных действий сексуального характера [3, с. 388; 352].