Научная статья
Научная специальность
5.1.4 «Уголовно-правовые науки»

УДК 343.9
DOI https://doi.org/10.26516/2071-8136.2023.3.70

СОВРЕМЕННЫЕ КРИМИНОЛОГИЧЕСКИЕ ХАРАКТЕРИСТИКИ ЦИФРОВОЙ ПРЕСТУПНОСТИ (ЦИФРОВОЙ ПРЕСТУПНИК И ЕГО ЖЕРТВА)

© Сидорова Е. З., 2023
Восточно-Сибирский институт МВД России, г. Иркутск, Россия

Освещен ряд актуальных криминологически значимых характеристик цифровой преступности (киберпреступности). Представлен криминологический портрет цифрового преступника, определены его характерные черты и выявлены отличия от обычного злоумышленника. Определены детерминанты цифровых преступлений (киберпреступлений), основные мотивы киберзлоумышленника. Составлен портрет потенциальной жертвы киберпреступлений, определена криминогенная роль поведения жертвы цифровых преступлений в механизме их совершения, а также приведена классификация таких потерпевших.

Ключевые слова: цифровые преступления, киберпреступление, потерпевший, криминологический портрет, детерминанты, цифровое пространство, виктимность, потерпевший, жертва, киберпреступник, ИТТ, социальная инженерия.

MODERN CRIMINOLOGICAL CHARACTERISTICS OF DIGITAL CRIME (DIGITAL CRIMINAL AND HIS VICTIM)

© Sidorova E. Z., 2023
East Siberian Institute of the Ministry of Internal Affairs of Russia, Irkutsk, Russian Federation

A number of relevant criminologically significant characteristics of digital crime (cybercrime) are highlighted. A criminological portrait of a digital criminal is presented, its characteristic features are determined and differences from an ordinary attacker are revealed. The determinants of digital crimes (cybercrimes), the main motives of the cyber-criminal are determined. A portrait of a potential victim of cybercrime is compiled, the criminogenic role of the behavior of a victim of digital crimes in the mechanism of their commission is determined, and the classification of such victims is given.

Keywords: digital crimes, cybercrimes, victim, criminological portrait, determinants, digital space, victimization, victim, victim, cybercriminal, ITT, social engineering.

Введение

С развитием различных технологий мы постепенно привыкли к тому, что Интернет способен решить большинство наших повседневных задач (например, путем дистанционного доступа в интернет-магазины или необходимого делового общения в формате реального времени), помогает с архивизацией личных данных путем их помещения в цифровые хранилища информации, позволяет оперативно использовать банковские карты и т. п. Эти и многие другие составляющие нашей повседневной жизни позволяют охарактеризовать интернет-технологии с положительной стороны. Однако у каждого положительного явления имеются те или иные отрицательные стороны. Например, в тот момент, когда человек размещает информацию о себе в электронных архивах, он становится потенциальной жертвой цифрового преступления. Объясняется это тем, что человек становится уязвимым к совершению в отношении него преступления именно по причине переноса личной информации в Интернет. Тем самым криминогенная ситуация, связанная с цифровым пространством, ухудшается. У преступников с каждым днем появляется все больше новых инструментов, методов и средств для совершения преступлений в цифровой среде.

Актуальность данной темы обусловлена ростом цифровизации, из-за которого в обществе ухудшается криминогенная обстановка в сфере применения информационно-телекоммуникационных технологий (далее – ИТТ). Интернет как инструмент совершения преступления стал почти повсеместно доступным. Процент населения, использующего ИТТ, растет постоянно, а значит, пропорционально с этим увеличивается количество потенциальных жертв цифровых преступлений, например потерпевших от киберпреступлений, связанных с хищением денежных средств с банковских счетов граждан или с неправомерным доступом к компьютерной информации.

Цель данной работы – определение криминологически значимых особенностей современной цифровой преступности, при этом в исследова-

нии в большей степени акцентируется внимание на изучении криминологических особенностей цифрового преступника и его жертвы.

Материалы и методы исследования

В основе исследования лежат общенаучные методы познания: индукция, дедукция, обобщение, анализ, сравнение и т. п. В качестве основных материалов исследования автор определяет данные официальной статистики, а также материалы ранее проведенных исследований по аналогичной тематике.

Результаты исследования

В конце прошлого столетия появилось такое понятие, как киберпреступление. В современной научной литературе можно встретить также иные термины (цифровые преступления, интернет-преступления, компьютерные преступления и т. п.). Поскольку в настоящее время в научных кругах еще не устоялась та или иная формулировка описываемого нами явления, отметим, что в нашей работе данные термины будут использоваться как равнозначные. Вместе с тем определенные отличия у данных терминов присутствуют. Например, если говорить о «компьютерной» преступности, то, как правило, в данном случае подразумевается более узкий круг уголовно наказуемых деяний, чем в случае с термином «цифровая преступность». Компьютерная преступность – это совокупность компьютерных преступлений, где компьютерная информация является предметом преступных посягательств, а также преступлений, которые совершаются посредством общественно опасных деяний, предметом которых является компьютерная информация. Эти деяния посягают на безопасность сферы компьютерной информации, являются одним из наиболее опасных и вредоносных явлений современного мира [5, с. 1484].

Когда мы говорим о цифровых преступлениях, то, как правило, предметом их совершения выступают персональные данные, а также электронные средства платежа. Еще одной чертой данных составов является совершение преступления с использованием компьютерных сетей или же ИТТ. На фоне глобализации всего цифрового пространства Интернет становится наиболее развитым методом совершения преступлений. Связано это именно с цифровизацией большей части населения и переносом баз данных в цифровое пространство, что, несомненно, является предпосылкой к росту киберпреступлений.

Согласно статистическим данным МВД России за период 2017–2021 гг., прослеживается тенденция роста мошенничества с применением ИТТ. Источником данных для анализа в рамках статьи является статистика Министерства внутренних дел РФ[1]. Если в 2017 г. количество таких преступлений составляло почти 81 тыс. случаев, зарегистрированных в отчетный период, то уже к концу 2021 г. оно увеличилось почти в 4,4 раза. Для иллюстрации описываемой тенденции роста данной категории преступлений построим соответствующий график динамики официально зарегистрированных мошенничеств, совершенных с применением ИТТ (рис. 1).

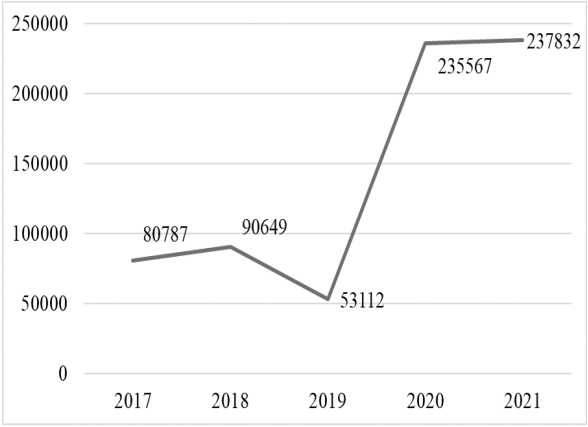

Рис. 1. Динамика преступлений, предусмотренных ст. 159 УК РФ (мошенничество), совершенных с применением ИТТ, Российская Федерация, 2017–2021 гг.

Опираясь на данные представленного графика, можно сделать следующие выводы:

1. С 2018 по 2019 г. наблюдался спад количества выявляемых и регистрируемых мошенничеств с использованием ИТТ почти в 2 раза примерно с 91 тысячи до 53 тысяч.

2. В период с 2019 по 2020 г. виден резкий статистический скачок регистрируемых показателей мошенничеств с применением ИТТ: данный показатель вырос примерно до 236 тысяч. Увеличение показателя составило 4,4 раза, т. е. выросло на 443,5 %. Вероятнее всего, статистический скачок указанного показателя явился результатом пандемии COVID-2019, когда были введены карантин и самоизоляция, люди были вынуждены использовать Интернет как средство заработка и жизнедеятельности.

Для определения криминологически значимых особенностей личности цифрового преступника и его жертвы, необходимо более углубленно изучить причины и условия цифровой преступности.

[1] Министерство внутренних дел Российской Федерации : офиц. сайт. URL: https://мвд.рф/ (дата обращения: 20.01.2023).

Исследовав общую криминологическую картину цифровой преступности (на основе данных официальной статистики), обратим внимание на детерминацию (причины и условия) данного вида преступности.

Под причинами преступности в криминологической науке понимаются некие обстоятельства, непосредственно обусловившие совершение преступления. В свою очередь, условия – это такие обстоятельства, которые способствовали совершению того или иного преступления, но прямо его не вызывали. При разграничении этих понятий следует отметить, что причины провоцируют преступность, а условия выступают только в качестве благоприятных обстоятельств. Взаимодействие данных факторов и их взаимное влияние друг на друга порождают в результате преступность.

Кратко напомним, какие существуют в научной литературе подходы к вопросу о причинности преступности. Существует три ключевых концепции криминологической причинности: социальная, биологическая, психологическая.

Данные концепции окончательно сформировались в 50–60-х гг. прошлого века, когда отечественная криминология стала позиционировать себя в качестве самостоятельной, непосредственно обособленной научной отрасли. Данные концепции объяснялись следующим образом: в основе биологической теории причинности преступности лежат заложенные природой (биологические) свойства и характеристики личности преступника; в основе психологической теории – субъективные детерминанты преступности; социальная концепция причинности преступности строилась на постулате об объективности процессов, лежащих в сфере социально-экономического устройства общества.

Если объяснять цифровую преступность, используя социальную теорию причинности, можно отметить, что в таком случае факторами преступности выступают имеющиеся социальные противоречия в обществе: экономические, политические, правовые, организационные, психологические, технические, медицинские и т. д.

Правовой фактор заключается в несовершенстве законодательства. Например, Владимир Левин в 1994 г. нанес крупный ущерб американскому банку Citibank, взломав его цифровое поле. Законодательство России на тот момент не предусматривало правовых норм, которые бы могли урегулировать данную ситуацию[1]. В подобных ситуациях и усматривается пробел в уголовно-правовой оценке общественно опасного деяния.

Экономический фактор выступает одной из причин преступности из-за наличия противоречий между потребностями и возможностями общества (например, расслоение общества по материальному положению).

Психологический фактор порождается нравственным кризисом в обществе и влечет за собой утрату общепринятых идеалов, доверия к правоохранительным органам, этническую и религиозную нетерпимость, алкоголизм, наркоманию, правовой нигилизм и т. д. [3, с. 124].

Следует также выделить некоторые ключевые детерминанты преступности:

– неблагоприятное влияние на личность в детстве и юности;

– низкое материальное положение;

– низкий уровень культуры и моральных установок;

– воздействие на психику средств массовой информации;

– воздействие различных криминальных субкультур (например, криминальная культура скинхедов, движения АУЕ[2]);

– миграцию населения (в таком случае люди находятся в более уязвимом состоянии и могут ради удовлетворения бытовых потребностей решиться на совершение противозаконного поступка).

Воздействие всех перечисленных детерминант на личность не будет являться основной причиной совершения преступления, потому что для его совершения необходимо волеизъявление самого субъекта, т. е. обстоятельства, влияющие на индивида, должны пройти через его сознание и волю. При одинаковом влиянии отрицательных обстоятельств отнюдь не каждый человек становится преступником, именно это и доказывает, что основу преступного поведения индивида составляют не только детерминанты, но и его внутреннее психическое отношение к совершаемому деянию.

Из вышесказанного можно сделать вывод о том, что основными причинами преступности являются низкая духовность человека (т. е. сознание и воля направлены на совершение аморальных действий), недостаточный уровень его правового сознания. Таким образом, в качестве главной причины цифровой преступности можно рассматривать низкое духовное развитие человека, поскольку целью умышленных цифровых

[1] Подстава века, или Таинственная история взлома Ситибанка. URL: https://habr.com/ru/company/macloud/blog/552866/ (дата обращения: 20.01.2023).

[2] Признано экстремистской организацией.

преступлений является, как правило, удовлетворение какого-либо корыстного интереса.

Переходя к криминологическому портрету злоумышленника цифровых преступлений, дадим определение термину «личность преступника».

По мнению Ю. М. Антоняна, личность преступника есть совокупность интегрированных в ней социально значимых негативных свойств, образовавшихся в процессе многообразных и систематических взаимодействий с другими людьми [4, с. 45]. Также одним из главных отличий личности преступника от законопослушного гражданина является его бездуховность, о чем говорилось ранее. Кроме того, исследования показывают, что процент импульсивности у личности преступника выше, чем у законопослушного гражданина. Данная импульсивность характеризуется слабой терпимостью и действием с агрессией при малейшем побуждении к этому. Стоит упомянуть, что именно такие индивиды применяют насилие различного рода при разрешении возникающих конфликтов.

Теперь обозначим наиболее характерные признаки личности киберпреступника:

1) высокий профессиональный уровень, поскольку для совершения подобного преступления преступнику, как правило, требуется наличие высокого уровня специальных знаний, умений и навыков;

2) наличие специального образования по направленности работы с ЭВМ или ИТТ;

3) уверенность в своей безнаказанности. Поскольку в настоящее время киберпреступления характеризуются высоким уровнем латентности, многие злоумышленники решаются на их совершение в надежде остаться безнаказанными;

4) осознание того, что для совершения цифрового преступления не потребуется больших временных или материальных затрат (при условии наличия специальных познаний в цифровой сфере). Из-за своих особенностей киберпреступления не требуют больших временных или материальных затрат, что влечет за собой завладение крупными денежными средствами, электронными средствами платежа, бездокументарными ценными бумагами или цифровой валютой по типу биткоина, догикоина и т. д.

При изучении личности цифрового преступника следует понимать, что цифровые преступления появились относительно недавно, в начале 90-х гг. прошлого века. Это означает, что субъектами данных преступлений, как правило, выступают относительно молодые люди, которых начали интересовать ЭВМ и ИТТ по мере их распространения среди населения. Исходя из стереотипов, сложившихся в результате воздействия киноиндустрии, обычно представляют, что преимущественно хакеры – это молодые люди, которые не нашли своего места в обществе, потому что не обладали привлекательной внешностью или коммуникативными навыками или считали, что не обладают. Преступники уходят в цифровой мир, чтобы быть там теми, кем захотят, или же для осуществления своей мести в киберпространстве, например для завладения персональными данными обидчика. Выполнение этих действий требует высокого профессионализма в сфере ЭВМ и ИТТ, и таким образом хакеры также самоутверждаются в киберпространстве, повышая свою самооценку и приобретая авторитет среди сверстников.

Исследование материалов судебно-следственной практики за 2012–2017 гг. позволило получить следующую криминологически значимую информацию о личности компьютерного преступника в России. Типовой криминологический портрет личности российского компьютерного преступника в настоящее время выглядит следующим образом: мужчина до 35 лет, городской житель, имеющий среднее специальное или высшее техническое образование, не состоящий в браке (холост либо разведен), обладающий профессиональными навыками и опытом работы на компьютерных устройствах, специалист в области ИТТ либо безработный, который в силу своих профессиональных обязанностей имеет (имел) доступ к служебным компьютерным устройствам, компьютерным сетям и базам данных. В прошлом судимости не имел и к уголовной ответственности не привлекался. Между тем компьютерные преступления совершал неоднократно. Преступные деяния предпочитает совершать в одиночку, так как обладает низкой социальной коммуникативностью и по характеру является индивидуалистом, эгоцентричной личностью [3, с. 249].

Теперь обратимся к вопросу о характеристике тех лиц, которые, как правило, становятся жертвами цифровых преступлений. Потерпевший выступает одной из ключевых составляющих механизма самого преступления, поскольку именно потерпевший может мотивировать (осознанно или неосознанно) преступника совершить то или иное преступление.

Согласно толковому словарю С. И. Ожегова, под потерпевшим понимается человек, которому в результате преступления причинен моральный, физический или имущественный урон [8, с. 677].

Потерпевшего как участника преступления (или уголовного процесса, или судопроизводства) изучают такие научные отрасли, как криминология, уголовное право, уголовный процесс, а также профилирующая наука – виктимология (от лат. *victima* – жертва и др.-греч. «логос» – учение).

Сама виктимология зародилась относительно недавно, ее родоначальником считают американского криминолога Х. фон Хентинга, издавшего в 1948 г. книгу «Преступник и его жертва». Стоит упомянуть, что термин «виктимология» также был использован в 1947 г. психиатром Б. Мендельсоном [1, с. 315].

Виктимология как обособленная теория криминологии изучает жертву, т. е. характер и свойства поведения, а также ее роль и значение в совершенном преступлении. Черты личности индивида, ставшего жертвой преступления, непосредственно идентифицируют такую личность, помогают определить отличительные черты ее поведения при взаимодействии с преступником.

Понятие потерпевшего закреплено и в нормативных правовых актах, а именно в ч. 1 ст. 42 УПК РФ. Согласно данному термину, потерпевшим является физическое лицо, которому преступлением причинен физический, имущественный, моральный вред[1]. Однако существуют ситуации, когда само потерпевшее лицо не может представлять свои интересы в уголовном судопроизводстве. Это возможно, например, при убийстве такого лица, и в таких случаях право потерпевшего представлять свои интересы в суде переходит к его близким родственникам или близким лицам.

Одним из основополагающих терминов виктимологической науки является понятие «виктимизация», введенное в правовую литературу Л. В. Франком. Под виктимизацией он понимает процесс превращения лица в реальную жертву или конечный результат такого процесса. По его мнению, «виктимность определенного лица есть… не что иное, как реализованная преступным актом „предрасположенность“, вернее, способность стать при определенных обстоятельствах жертвой преступления, или, другими словами, неспособность избежать опасности там, где она объективно была предотвратима» [2, с. 242].

Важно понимать, что потерпевший сам может вызывающе себя вести или быть идеальной жертвой для преступника, имея телосложение, характер и иные свойства личности, подходящие для совершения в отношении него преступления. В таком случае возможно даже задаться вопросом, не отводить ли нам в таких ситуациях главенствующую роль в совершении преступления именно потерпевшему. Однако возможна и другая ситуация, когда жертва преступления не будет провоцировать преступника на совершение противоправного деяния, а лишь выступит частью совокупности детерминантов преступления.

Немалую роль в виктимности личности играют не только психофизиологические характеристики потенциальной жертвы, но и факультативные признаки объективной стороны преступления: место, время, обстановка и тому подобное, поскольку именно из-за совокупности всех этих факторов будет возможно совершение преступления.

Переходя к рассмотрению особенностей жертв цифровых преступлений, можно выделить следующие типы в зависимости:

1) от *состава цифрового преступления*, в результате совершения которого данные лица стали жертвой;

2) *демографических признаков*, которые могли способствовать совершению в отношении них преступлений (пол, возраст, место работы и т. п.);

3) *активности потерпевших*. В этом случае можно выделить:

– активных потерпевших, поведение которых связано не с нападением на будущего преступника или конфликтным контактом с ним, а с активным способствованием причинению вреда самим себе (сознательные подстрекатели, неосторожные подстрекатели, сознательные самопричинители и неосторожные самопричинители) [9, с. 114];

– пассивных потерпевших, не оказывающих сопротивления (не могущих или не хотящих это делать);

4) *роли вины самих потерпевших в совершении преступления*. Выделяются:

– антикриминогенная личность потерпевшего, противостоящая совершению преступления, т. е. лицо соблюдает личную безопасность и меры по предупреждению преступлений в отношении него (например, лицо не переходит по сомнительным интернет-ссылкам и не пользуется услугой самозаполнения окон на незнакомых сайтах, поскольку это могут быть фишинговые сайты; не распространяет персональные данные в сети Интернет и т. п.);

[1] Уголовно-процессуальный кодекс Российской Федерации : федер. закон от 18 дек. 2001 г. № 174-ФЗ (в ред. от 29 дек. 2022 г.) // КонсультантПлюс : справочная правовая система.

– криминогенная личность потерпевшего. В этом случае потерпевшее лицо, наоборот, побуждает и мотивирует преступника совершить преступление. Например, лицо загружает в общий интернет-доступ личные данные по определенному типу (номер банковской карты, паспортные данные и т. п.), чем злоумышленники могут воспользоваться и совершить киберпреступление;

– нейтральная личность потерпевшего, когда потерпевший не способствует совершению преступления, но и не предпринимает никаких дополнительных мер безопасности в Интернете.

Говоря о криминологических особенностях жертв преступлений цифровой направленности, следует выделить их криминогенную роль в совершении противоправных деяний. Как уже подчеркивалось, именно жертва может зародить мотивацию совершения преступления у злоумышленника своими личностно-волевыми характеристиками, умственными и физическими особенностями, а также своей безынициативностью в вопросах обеспечения личной безопасности, в данном случае личной цифровой безопасности.

Своим поведением лицо может вызвать у субъекта преступления желание совершить определенный волевой акт, т. е. зародить у злоумышленника некий импульс совершить данный поступок, зная, что данное деяние запрещено нормативными правовыми актами, а также общепринятыми нормами поведения в обществе, нормами морали и нравственности.

В виктимности жертв цифровых преступлений можно выделить две ключевые составляющие:

1. *Возраст и пол потерпевшего.* Так, чаще всего жертвами цифровых преступлений становятся люди, менее защищенные в цифровом пространстве. Как правило, это дети в возрасте 3–12 лет. Такие лица из-за особенностей возрастного и психологического характера еще не могут сами обеспечить безопасность своих интересов, в том числе в сети Интернет, и вместо них потерпевшими будут выступать их родители. Приведем гипотетический пример. Ребенок 10 лет, используя смартфон, переходит по ссылкам на различные интернет-сайты во время серфинга по Интернету (поясним, что серфинг в Интернете – это средство получения денег: пользователю платят деньги за просмотр или переход на конкретный веб-ресурс) и случайно заходит на фишинговый сайт или же становится жертвой спам-сообщений, где, например, говорится о том, что данный телефон был подвержен кибератаке и для сохранения всех данных с этого телефона необходимо отправить телефонный номер и номер банковской карты, в том числе с кодом с обратной стороны банковской карты, для успешного переноса данных из телефона в облачное хранилище. Ребенок в силу психофизиологических особенностей своего возраста и отсутствия опыта не способен идентифицировать данное деяние в качестве преступления, в связи с чем подвергается собиранию у него персональной информации родителей. Подобная ситуация может произойти и со взрослыми людьми (как правило, речь идет о лицах в возрасте старше 50 лет). Приведем еще один пример. На телефон 60-летней женщины поступает звонок от якобы работника банка. Такой псевдоработник сообщает о срочной необходимости перевода всех денежных средств на другой лицевой счет, и сделать это нужно, по его словам, как можно скорее. Для этого мнимый сотрудник собирает у женщины необходимую информацию для перевода денежных средств с ее личного счета на счет преступника.

Приведем пример из правоприменительной практики.

Сорокалетняя жительница Курска дорого заплатила за урок, который ей преподали телефонные мошенники. С самого начала женщина продемонстрировала фантастическую доверчивость и поверила всему, что услышала в телефонной трубке. Человек, который представился сотрудником главного офиса банка, предложил курянке застраховать свои вклады от кражи. Никого не смутило, что вся процедура прошла дистанционно. Затем собеседник заявил, что с одного из застрахованных счетов деньги уже были похищены, но страховка покроет ущерб. Взволнованную женщину заставили пойти в банк и закрыть свой счет на сумму более 1,6 млн руб. Ей объяснили, что это деньги, возмещенные по страховке, и их нужно вернуть, переведя через банкомат на несколько специальных счетов. И только потом с чеками о переводах прийти в отделение банка и получить свои деньги назад.

Курянке среди других позвонил и некий сотрудник следственных органов, который подтвердил, что расследует дело против неизвестных мошенников, и убедил следовать инструкциям людей из банка и отправлять наличность. Постепенно аферисты, желая сэкономить, перевели диалог в бесплатные мессенджеры. Потерпевшей стали рассказывать, что на ее имя пытаются оформить кредит злоумышленники. Чтобы этого не произошло, отправили в банк оформлять реальный заем. Все это время ситуация контролировалась дистанционно. Заявку на

крупную сумму в офисе не приняли, предложив только кредитную карту с лимитом 150 тыс. руб.

Телефонные аферисты заставили снять деньги и также перевести их, а когда поняли, что поживиться больше нечем – решили подшутить над жертвой. В мессенджере женщине прислали фото повестки от следователя. Она явилась в назначенный день в здание одной из силовых структур региона. Только там настоящие правоохранители открыли ей глаза на происходящее. Сейчас по факту мошеннических действий, совершенных неизвестными лицами, в УМВД России по г. Курску возбуждено уголовное дело. Злоумышленникам грозит наказание в виде лишения свободы на срок до 5 лет[1].

Несмотря на то что жертвами кибермошенников может стать любой человек, вместе с тем существуют определенные группы риска. В первую очередь это люди старшего возраста, которые зачастую недостаточно хорошо разбираются в современных технологиях и которыми легче манипулировать. Так, по данным Центрального банка России, на пожилых (60 лет и старше) приходится 27 % мошеннических действий, на возраст 50–59 лет – 20 %, 40–49 лет – 19 %, 30–39 лет – 17 %, 20–29 лет – 13 %, младше 20 лет – только 4 %. Еще один интересный факт: оказалось, что женщины чаще, чем мужчины, попадаются на удочку мошенников – более 65 %[2].

Таким образом, следует констатировать, что возраст и пол потерпевшего относятся к ключевым элементам виктимности граждан. Данные группы лиц имеют недостаточные знания работы с компьютерами и электронными сетями или имеют общий низкий или недостаточный уровень образования.

2. *Значительный разрыв в осведомленности о работе ИТТ и ЭВМ злоумышленника и потенциальной жертвы*. Данное положение объясняется тем, что рассматриваемый нами вид преступности зачастую требует от злоумышленника высокого профессионализма в сфере ИТТ и ЭВМ. В противном случае субъект подобного преступления не сможет его совершить по причине отсутствия у него специальных знаний. Описанные нами признаки портрета киберпреступника свидетельствуют о том, что работа с компьютерными сетями и ИТТ нередко является основным видом деятельности таких злоумышленников, в связи с чем цифровой преступник имеет значительное преимущество перед своей жертвой с точки зрения наличия у него специальных познаний в области цифровых технологий.

Виктимность жертв цифровых преступлений можно охарактеризовать как нейтральную и видовую. Нейтральной она является потому, что поведение жертвы не всегда обусловливает активизацию преступного поведения злоумышленника. «Безупречное» поведение будущей жертвы в сети Интернет никоим образом не сподвигает преступника совершить противоправные действия в отношении нее. Например, потенциальная жертва может получить сообщение в социальных сетях от знакомого человека, аккаунт которого взломали, т. е. жертва не осознавала и не была готова к тому, что от данного лица поступит фишинговое сообщение. Видовой же такая виктимность является потому, что все жертвы цифровых преступлений условно подходят под одни и те же критерии (низкий уровень цифровой грамотности, бдительности, образования, высокая доверчивость), т. е. речь идет о предрасположенности отдельных лиц при виктимогенной обстановке в совокупности с определенными обстоятельствами стать жертвой киберпреступления.

Наибольшей распространенностью в настоящее время обладают такие цифровые преступления, как кибермошенничество. Чаще всего при их совершении технические устройства работают исправно, защитные программы не подвергаются кибератаке, однако преступление все же совершается. Объясняется это тем, что проще «взломать» человека с помощью психологических приемов, чем подвергать взламыванию то или иное техническое средство. Таким образом, информационная безопасность включает в себя два аспекта: компьютер и человек. В данной совокупности наиболее уязвимым является именно человек, компьютерные сети более защищены, поскольку с развитием цифровой сферы растут протоколы безопасности, повышаются требования к антивирусным программам и создаются новые способы и методы защиты. Компьютер взламывается с помощью специальных технических средств и вредоносного программного обеспечения, а человек – с помощью методов социальной инженерии.

Впервые понятие «социальная инженерия» применил американский социолог Роско Паундом. Кевин Митник (известный киберпреступник, а ныне консультант по безопасности) еще в 1990-е гг. стал популяризировать данный тер-

[1] Жительница Курска перевела мошенникам 1,7 миллиона рублей и пришла по подставной повестке в правоохранительные органы // Управление МВД России по Курской области : офиц. сайт. URL: https://46.xn--b1aew.xn--p1ai/news/item/33816305 (дата обращения: 20.01.2023).

[2] 10 фактов о кибермошенничестве. URL: https://plus-one.ru/society/2021/06/30/10-faktov-o-kibermoshennichestve (дата обращения: 20.01.2023).

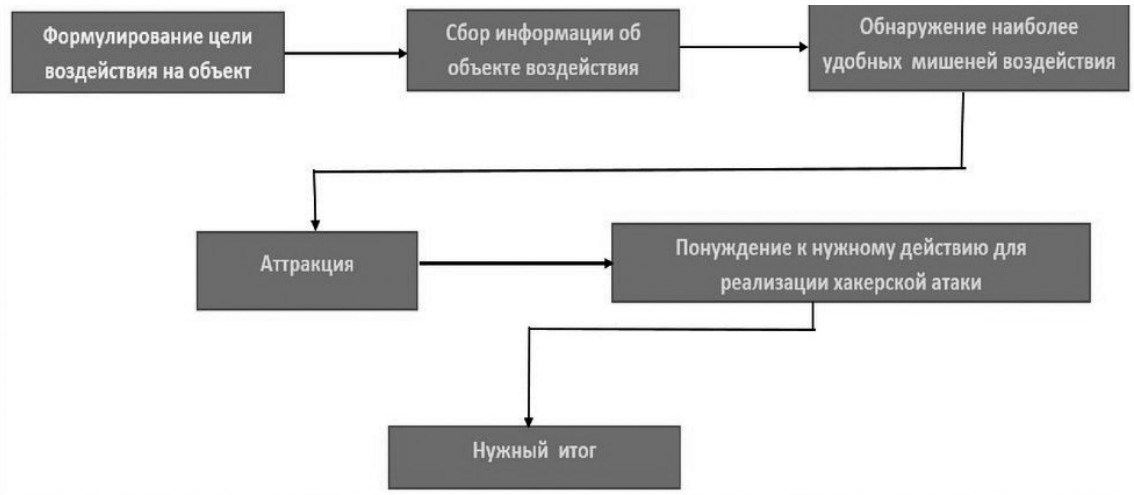

Рис. 2. Схема воздействия в социальной инженерии

мин. Он считал, что ни один технический код не сможет так обмануть человека, как психологические умения преступника [10, с. 134].

Социальная инженерия – это совокупность психологических, социологических методов и средств, направленных на создание благоприятных условий для выуживания, хищения засекреченных, конфиденциальных данных.

Для более детального познания работы социальной инженерии приведем схему воздействия в социальной инженерии, составленную белорусским психологом и социологом В. П. Шейновым, долго занимавшимся психологией мошенничества (рис. 2) [6, с. 112].

Ярким примером применения методов социальной инженерии является мошенническая схема, которая была реализована в апреле 2020 г. В отдел полиции по району Замоскворечье обратилась 80-летняя жительница, которая сообщила, что на мобильный телефон ей поступил звонок и что неизвестное лицо представилось местным участковым. Мужчина просил ей посодействовать в задержании группы мошенников, которая угрожает пожилым людям, вымогает у них вклады. Он попросил ее быть начеку.

На следующий день пенсионерке позвонили с другого неизвестного номера, неизвестные мужчины начали ей угрожать и требовать снять ее деньги в банке. После данного звонка москвичка сразу вспомнила о звонившем ей «участковом» и решила связаться с ним для задержания злоумышленников.

«Участковый», ответивший на звонок пенсионерки, сказал, что уже знает о них и они находятся в разработке для задержания. Затем попросил ее снять все деньги с банковского счета, выйти на балкон, сбросить деньги преступникам, чтобы их можно было задержать с поличным. Он сказал, что их задержат и деньги сразу вернут. Злоумышленники сразу подобрали пакет с деньгами и скрылись на автомобиле[1].

Согласно сравнительному исследованию, проводимому доктором психологических наук С. Ф. Сафуановым, для потерпевших в киберпространстве характерен следующий комплекс психологических особенностей: высокий уровень агрессии, низкая самооценка, неуверенность, апатия, вялость, нестабильное выражение эмоций, также респонденты проводимого исследования были напряжены и раздражительны.

Внутри группы жертв противоправных посягательств в Интернете выделяются жертвы «насильственных» и «ненасильственных» преступлений, отличающиеся уровнем ситуативной и личностной тревожности, агрессивности и характером локуса контроля. Жертвы «насильственных» противоправных посягательств в Интернете более агрессивны, тревожны и относятся к экстернальному типу, в отличие от группы жертв «ненасильственного» типа, которые имеют более низкие показатели по агрессивности, тревожности и относятся к интернальному типу [7, с. 89].

Обсуждения и заключения

Подводя итог, отметим следующее. Опираясь на ранее проводимые исследования, а также на анализ современных случаев совершения цифровых преступлений, мы предприняли попытку составить криминологический портрет классического цифрового преступника и его жертвы. Вместе с тем психологический портрет как циф-

[1] Москвичка выбросила с балкона 6 миллионов рублей, чтобы помочь лже-участковому задержать мошенников. URL: https://www.kp.ru/daily/27118/4198857 (дата обращения: 20.01.2023).

рового преступника, так и его жертвы в настоящее время в научной литературе исследован недостаточно и нуждается, на наш взгляд, в более глубоком изучении, поскольку с развитием информационного общества меняются не только виды совершаемых цифровых преступлений, но и психологические характеристики жертв таких преступлений. В этой связи нам представляется необходимым проводить дальнейшие научные исследования по аналогичной тематике с целью формирования эффективных мер противодействия цифровой преступности в целом.

СПИСОК ЛИТЕРАТУРЫ

1. Афанасьева О. Р., Гончарова М. В., Шиян В. И. Криминология : учебник и практикум для вузов. М. : Юрайт, 2023. 340 с.

2. Емельянов И. Л. Виктимность и виктимизация: понятие, виды, проблемы профилактики // Известия Алтайского государственного университета. 2013. Т. 1, № 2 (78). С. 241–246.

3. Капинус О. С. Криминология : учебник для вузов. 2-е изд., перераб. и доп. М. : Юрайт, 2023. 1132 с.

4. Коломытцев Н. А., Одинцова Л. Н. Личность преступника как криминологическая проблема // Государство и право: теория и практика. 2016. № 3 (4). С. 42–53.

5. Кузнецов Д. А., Манохина О. В. Компьютерная преступность // Бюллетень медицинских интернет-конференций. 2015. Т. 5, № 12. С. 1484–1485.

6. Кузнецов М. В., Симдянов И. В. Социальная инженерия и социальные хакеры. СПб. : БХВ-Петербург, 2007. 368 с.

7. Сафуанов Ф. С., Докучаева Н. В. Особенности личности жертв противоправных посягательств в Интернете // Психология и право. 2015. Т. 5, № 4. С. 80–93.

8. Толковый словарь русского языка : 80 000 слов и фразеол. выражений / С. И. Ожегов, Н. Ю. Шведова ; Рос. акад. наук, Ин-т рус. яз. им. В. В. Виноградова. 4-е изд., доп. М. : Азбуковник, 1997. 940 с.

9. Христенко В. Е. Психология поведения жертвы. Ростов н/Д. : Феникс, 2004. 411 с.

10. Янгаева М. О. Социальная инженерия как способ совершения киберпреступлений // Вестник Сибирского юридического института МВД России. 2021. № 1 (42). С. 133–138.

REFERENCES

1. Afanas'eva O.R., Goncharova M.V., Shiyan V.I. *Kriminologiya* [Criminology]. Moscow, Yurajt, 2023, 340 p. (in Russian).

2. Emel'yanov I.L. Viktimnost i viktimizaciya: ponyatie, vidy, problemy profilaktiki [Victimization and victimization: concept, types, problems of prevention]. *Izvestiya Altajskogo gosudarstvennogo universiteta* [Proceedings of the Altai State University], 2013, vol. 1, no. 2 (78), pp. 241-246. (in Russian).

3. Kapinus O.S. *Kriminologiya* [Criminology]. Moscow, Yurajt Publ., 2023, 1132 p. (in Russian).

4. Kolomytcev N.A., Odincova L.N. Lichnost prestupnika kak kriminologicheskaya problema [Criminal identity as a criminological problem]. *Gosudarstvo i pravo: teoriya i praktika* [State and law: theory and practice], 2016, no. 3 (4), pp. 42-53 (in Russian).

5. Kuznecov D.A., Manohina O.V. Kompyuternaya prestupnost [Computer crime]. *Byulleten medicinskih internet-konferencij* [Bulletin of medical Internet conferences], 2015, vol. 5, no. 12, pp. 1484-1485 (in Russian).

6. Kuznecov M.V., Simdyanov I.V. *Socialnaya inzheneriya i socialnye hakery* [Social engineering and social hackers]. Saint-Petersburg, BHV-Peterburg Publ., 2007, 368 p. (in Russian).

7. Safuanov F.S., Dokuchaeva N.V. Osobennosti lichnosti zhertv protivopravnyh posyagatel'stv v Internete [Personality features of victims of unlawful attacks on the Internet]. *Psihologiya i pravo* [Psychology and Law], 2015, vol. 5, no. 4, pp. 80-93 (in Russian).

8. Ozhegov S.I., Shvedova N.Yu. *Tolkovyj slovar russkogo yazyka* [Explanatory dictionary of the Russian language]. Moscow, Azbukovnik Publ., 1997, 940 p. (in Russian).

9. Khristenko V.E. *Psihologiya povedeniya zhertvy* [Psychology of victim behavior]. Rostov-on-Don, Phoenix, 2004, 411 p. (in Russian).

10. Yangaeva M.O. Social'naya inzheneriya kak sposob sovershеniya kiberprestuplenij [Social engineering as a way of committing cybercrimes]. *Vestnik Sibirskogo yuridicheskogo instituta MVD Rossii* [Bulletin of the Siberian Law Institute of the Ministry of Internal Affairs of Russia], 2021, no. 1 (42), pp. 133-138.

Статья поступила в редакцию 06.02.2023; одобрена после рецензирования 11.05.2023; принята к публикации 13.09.2023

Received on 06.02.2023; approved on 11.05.2023; accepted for publication on 13.09.2023

Сидорова Екатерина Закариевна – кандидат юридических наук, доцент кафедры уголовного права и криминологии, Восточно-Сибирский институт МВД России (Россия, 664071, г. Иркутск, ул. Лермонтова, 110), ORCID: 0000-0003-3216-7107, e-mail: ketrik6@mail.ru

Sidorova Ekaterina Zakarievna – Candidate of Juridical Sciences, Associate Professor of the Department of Criminal Law and Criminology, East Siberian Institute of the Ministry of Internal Affairs of Russia (110, Lermontov st., Irkutsk, 664071, Russian Federation), ORCID: 0000-0003-3216-7107, e-mail: ketrik6@mail.ru