ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ
ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
ДАЛЬНЕВОСТОЧНЫЙ ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ

На правах рукописи

Камко Артем Сергеевич

ПРЕДУПРЕЖДЕНИЕ МОШЕННИЧЕСТВА С ИСПОЛЬЗОВАНИЕМ ТЕЛЕКОММУНИКАЦИОННЫХ И КОМПЬЮТЕРНЫХ СЕТЕЙ

Специальность 12.00.08 – уголовное право и криминология;
уголовно-исполнительное право

ДИССЕРТАЦИЯ
на соискание ученой степени кандидата юридических наук

Научный руководитель:
доктор юридических наук, профессор
Номоконов Виталий Анатольевич

Владивосток – 2020

СОДЕРЖАНИЕ

Введение……. 3

1 Криминологическая характеристика мошенничества, совершаемого с использованием телекоммуникационного и компьютерного оборудования: отечественный и зарубежный опыт……..…… 16

1.1 Особенности мошенничества, совершаемого с использованием телекоммуникационного и компьютерного оборудования…….. 16

1.2 Законодательство и опыт зарубежных стран по предупреждению мошенничества, совершаемого с использованием телекоммуникационного и компьютерного оборудования……. 42

2 Характеристика личности преступника и личности потерпевшего в рамках мошенничества, совершаемого с использованием телекоммуникационного и компьютерного оборудования……..….. 63

2.1 «Портрет» личности преступника, совершившего мошенничество с использованием телекоммуникационного и компьютерного оборудования... 63

2.2 Виктимологическая характеристика мошенничества, совершаемого с использованием телекоммуникационного и компьютерного оборудования в России…….……. 89

3 Развитие системы противодействия мошенничеству, совершаемому с использованием телекоммуникационного и компьютерного оборудования…… 118

3.1 Виктимологическая профилактика мошенничества, совершаемого с использованием телекоммуникационного и компьютерного оборудования как основа системы предупреждения данной категории преступлений… 118

3.2 Формирование межведомственных структурных связей в среде предупреждения мошенничества, совершаемого с использованием телекоммуникационного и компьютерного оборудования…… 141

Заключение…… 161

Библиографический список……... 165

Приложения…….. 188

ВВЕДЕНИЕ

Актуальность исследования. В современном мире постоянно происходят процессы генерации и интеграции информации (общего и личного пользования), и преступность, используя впечатляющие результаты технологического прогресса, также претерпевает качественную трансформацию. Техническая и технологическая доступность дистанционного (удаленного) распоряжения капиталом предоставляет преступникам, владеющим определенной информацией, возможность путем мошенничества похитить денежные средства у граждан, проживающих в другом городе, регионе или стране.

При этом преступления, совершаемые с использованием современных компьютерных технологий и средств связи, имеют существенную специфику, которая порождает сложности как в обнаружении фактических действий злоумышленника, так и в определении потенциальной возможности совершения преступного деяния.

В последние годы для повышения эффективности борьбы с преступлениями, совершаемыми с использованием телекоммуникационных и компьютерных сетей, значительные изменения претерпели отдельные положения в Уголовном кодексе Российской Федерации. Так, введен квалифицирующий признак совершения преступления «с использованием средств массовой информации, в том числе информационно–телекоммуникационных сетей (включая сеть Интернет)» в составы отдельных статей УК РФ (например, ч. 1 ст. 171^2, ч. 1 ст. 185^3, п. «б» ч. 2 ст. 228^1, п. «б» ч. 3 ст. 242, п. «г» ч. 2 ст. 242^1 УК РФ) и квалифицирующий признак совершения преступления «с использованием информационно–телекоммуникационных сетей (включая сеть «Интернет»)» – в п. «г» ч. 2 ст. 242^2 УК РФ. Отдельное правовое закрепление также получили составы «высокотехнологичных» видов мошенничества (ст. 159^3, ст. 159^6 УК РФ).

Между тем, как показывает практика деятельности правоохранительных органов, данные меры, являясь необходимыми, не являются исчерпыва-

ющими в вопросах предупреждения как в целом преступлений, совершаемых в сфере информационно–телекоммуникационного пространства, так и мошенничества, совершаемогос использованием телекоммуникационного и компьютерного оборудования в частности.

Следует также отметить, что особую актуальность выбранной теме исследования придает рост числа зарегистрированных преступлений в данной сфере. Так, в 2019 году зарегистрировано 19 518 преступления, совершенного с использованием телекоммуникационного и компьютерного оборудования, из них 17 852 преступлений – с использованием данных расчетных (пластиковых) карт. В динамике за период 2016–2018 годов данный показатель вырос на 38,68%[1].

Степень разработанности темы. Вопросы предупреждения преступлений корыстной направленности, включая и мошенничество, достаточно хорошо освещены в отечественной и зарубежной науке. Между тем основные фундаментальные исследования, посвященные вопросам совершения преступлений с использованием компьютерного и телекоммуникационного оборудования, в настоящее время требуют развития изложенных в них научных положений. Как отмечает А.А. Комаров, «глубоких всесторонних исследований, посвященных компьютерной преступности как явлению – следствию социальной трансформации общества, пока мало»[2].

Рассматривая конкретные направления отечественной юриспруденции в целом и криминологической мысли в частности, можно отметить значительное внимание некоторых исследователей к вопросам «виктимологической профилактики» и «виктимологического предупреждения», обоснованным и активно разрабатываемым такими известными учеными, как К.В. Вишневецкий, Т.В. Варчук, А.А. Гаджиева, В.И. Задорожный, Д.В. Ривман, Л.В. Франк и др. В работах названных авторов предприняты попытки разра-

[1] См.: Портал правовой статистики Генеральной Прокуратуры РФ [электронный ресурс] // режим доступа: http://crimestat.ru/offenses_table

[2] Комаров А.А. Интернет–мошенничество: проблемы детерминации и предупреждения : монография. М. : Юрлитинформ, 2013. 179 с.

ботки как отдельных элементов теоретической модели виктимологического воздействия на преступность, так и системы мер виктимологической профилактики преступлений. Однако, отсутствие законодательного закрепления и четко сформулированной государственной политики виктимологического воздействия до настоящего времени не позволяет в полной мере раскрыть потенциал указанных научных разработок.

Вопросам взаимодействия при расследовании преступлений в финансовой сфере уделяли внимание в своих исследованиях И.Г. Иванова, Д.Н. Иконников, Е.Ю. Карнаухова, Г.А. Шаламов, П.С. Яни и др. Между тем многие вопросы, связанные с совместной деятельностью и оказанием содействия со стороны организаций коммерческого сектора сотрудникам правоохранительных органов, также не получили должного разрешения.

Уголовно–правовые аспекты противодействия преступлениям, совершаемым с помощью телекоммуникационного и компьютерного оборудования, в значительной степени освещены в работах В.Г. Степанова–Егиянца и З.И. Хисамовой. Так, в рамках диссертационного исследования В.Г. Степанова–Егиянца основное внимание уделено вопросам уголовно–правового обеспечения безопасности компьютерной информации. В диссертационном исследовании З.И. Хисамовой предметно рассмотрены вопросы «уголовно–правового противодействия преступлениям, совершаемым в финансовой сфере с использованием информационно–телекоммуникационных технологий». Невозможно проигнорировать взаимосвязь указанных исследований, поскольку в своей совокупности они гармонично дополняют друг друга, что позволило им в значительной степени продвинуть теоретические границы познания юридической науки.

В рамках исследуемого явления интерес представляет диссертационная работа М.Д. Фролова, связанное в основная с разрешением ряда актуальных вопросов о применении и понимании ст. 159^6 УК РФ. Между тем, несмотря на наличие определенных смежных аспектов и общности цели совершения деяний, категория мошенничества, совершаемого с помощью телекоммуни-

кационного и компьютерного оборудования, является более широкой, охватывая не только проблемы безопасности информации, но и вопросы применения современных технологий в уже устоявшихся схемах совершения мошенничества, что приводит к эволюции последних.

Отдельные вопросы преступлений корыстной направленности, совершаемых с использованием телекоммуникационных и компьютерных сетей, с точки зрения криминологической науки изложены в работах таких авторов, как И.Р. Бегишев, А.И. Бойцов, А.Г. Волеводз, О.С. Гузеева, Р.И. Дремлюга, И.А. Клепицкий, В.А. Номоконов, В.С. Овчинский, Т.Л. Тропина, А.Ю. Чупрова и многих других.

Следует отдельно выделить тот факт, что в работах А.Ю. Чупровой и И.Р. Бегишева прослеживаются идеи о недостаточно используемом потенциале межведомственного взаимодействия правоохранительных органов, институтов гражданского общества и коммерческих предприятий. Между тем на момент публикации исследований указанных авторов возможность построения четкой отлаженной системы в контексте рассматриваемого вопроса была невозможна.

Целью исследования является развитие современных мер и механизмов предупреждение мошенничества с использованием телекоммуникационного и компьютерного оборудования.

Задачами исследования соответственно стали:

– выявить характерные особенности мошенничества с банковскими картами и АТМ–терминалами в России;

– рассмотреть особенности системы мер предупреждения мошенничества в сфере безналичных расчетов в зарубежных странах;

– дать характеристику личности преступника, совершающего деяния в рассматриваемой сфере;

– охарактеризовать потерпевшего в рамках мошенничества, совершаемого с использованием телекоммуникационного и компьютерного оборудования;

– разработать меры по развитию системы профилактики и предупреждения высокотехнологического мошенничества.

Объектом исследования выступают общественные отношения, возникающие в связи с совершением, предупреждением и обеспечением профилактики современных видов мошенничества.

Предметом исследования определены:

– материалы, описывающие статистику, динамику, специфические черты мошенничества с использованием телекоммуникационных и компьютерных устройств;

– практика применения норм уголовного законодательства Российской Федерации в части защиты экономических отношений и интересов граждан;

– зарубежные концепции законодательной, правоприменительной и профилактической деятельности в сфере рассматриваемого вида мошенничества;

– характеристики личности преступника и личности потерпевшего в рамках рассматриваемых общественных отношений.

Методологическую основу исследования составили диалектический метод познания и системный подход. В ходе исследования также применялись отдельные элементы методов научной индукции и дедукции, такие как объединенный метод сходства и различия, метод остатков, статистическое обобщение и др.; метод ретроспективного и статистического анализа, вторичный анализ данных работ отечественных авторов, а также сравнительно–сопоставительный метод исследования.

Теоретическую базу составили работы А.И. Бойцова, Т.В. Варчук, К.В. Вишневецкого, А.Г. Волеводза, А.А. Гаджиевой, О.С. Гузеевой, В.И. Задорожного, И.А. Клепицкого, В.С. Овчинского, Д.В. Ривман, В.Г. Степанова–Егиянца и др.

Нормативную основу составили отечественное и зарубежное уголовное законодательство, международные правовые акты об ответственности за

преступления в сфере экономики (преступления против собственности, преступления в сфере экономической деятельности), в сфере компьютерной информации, а также иные нормативные правовые акты, регулирующие отношения в сфере связи, информации и ее защиты, а также имущественных интересов граждан.

Эмпирическую базу исследования составили статистические данные за 2012–2018 годы Главного информационно–аналитического центра МВД РФ, статистические и аналитические материалы по заявленной теме исследования. Кроме того, были проанализированы материалы 250 уголовных дел, касающихся различных видов и отдельных этапов совершения мошенничества, связанного с использованием телекоммуникационного и компьютерного оборудования, приговоры по которым были вынесены в период 2014–2016 годов, в числе которых материалы уголовных дел на стадии предварительного следствия[3] за период 2012–2015 годов.

Кроме того, использованы материалы опроса 200 человек, задержанных в связи с совершением целевой категории преступлений (применялся тест Айзенка, определяющий коэффициент интеллекта личности). Опрос проводился как среди подследственных лиц, так и среди лиц, содержащихся в местах лишения свободы. Проведение теста, определяющего интеллектуальный уровень преступников по рассматриваемому виду корыстных преступлений, позволило определить специфические черты их личности,что стало основанием для формирования авторской классификации таких лиц.

Научная новизна. В рамках настоящего исследования были определены основные особенности мошенничества, совершаемого с использованием телекоммуникационного и компьютерного оборудования, жертвами которого становятся граждане Российской Федерации: определены причины, и отдельные особенности личности самих преступников (социально–демографические, нравственно–психологические признаки).

---

[3] Материалы получены в ходе осуществления профессиональной деятельности автора в качестве заместителя начальника УМВД России по г. Хабаровску – начальника следственного управления.

На основе последнего предложена система критериев классификации лиц, совершивших деяния рассматриваемого вида. Целью классификации является определение соответствующих отдельных и (или) комплексных мероприятий по снижению формирования преступности как на основе виктимности «случайных» участников совершения преступления, так и с учетом фактических критериев личности, совершающей противоправное деяние.

Проведен анализ зарубежного опыта предупреждения мошенничества с применением телекоммуникационного и компьютерного оборудования, а также рассмотрены отдельные аспекты нивелирования последствий данного вида деяний, применяемого в зарубежных странах.

На основании проведенного анализа предложены основные концептуальные положения системы виктимологической профилактики рассматриваемого вида противоправных деяний. Сформулирована и обоснована необходимость формирования системы межведомственных связей, целью чего должны являться информационное взаимодействие и координация усилий по предупреждению случаев мошенничества с использованием телекоммуникационного и компьютерного оборудования (включая, но не ограничиваясь системами ДБО; оплаты услуг путем отправки смс–сообщений на «короткие номера»; оформление незаконных «телефонных подписок»; мошенничество с применением банковских карт и т. д.) и иным правонарушениям в сфере обеспечения имущественных прав и законных интересов граждан.

Основные положения, выносимые на защиту.

1. Обоснована необходимость обеспечения повышенной безопасности систем безналичных расчетов. В условиях современной динамики социально–экономического развития и сопутствующего роста доступности технологических инноваций, связанных с системами безналичных расчетов, вопросы безопасности подобных операций недостаточно проработаны.

Выявлены детерминанты, способствующие мошенничеству, совершаемому с использованием телекоммуникационного и компьютерного оборудования. К ним относятся: комплекс «технических» факторов; наличие

определенных сложностей при выявлении факта совершения деяния; многоэтапность процесса совершения деяния; высокая организованность преступных групп; высокий уровень технической подготовки злоумышленников; международный характер деяния и т. д.

2. Обобщение зарубежного опыта в сфере профилактики и противодействия рассматриваемому виду противоправных деяний позволило определить, что значительная часть применяемых зарубежными странами мер данной направленности обосновывается положениями законодательства этих государств, некоторые из которых в рамках актуальной российской действительности имеют значительные возможности рецепции.

На основании определения такой возможности сделан вывод о необходимости развития системы противодействия мошенничеству, совершаемому с использованием телекоммуникационного и компьютерного оборудования, с учетом принципов виктимологической профилактики.

Определены наиболее перспективные для целей рецепции в процессе совершенствования отечественного законодательства положения зарубежных Уголовных кодексов, в числе которых: обособление норм о так называемом «компьютерном мошенничестве»; дифференциация ответственности за мошенничество, совершаемое «под прикрытием» легальных судебных процедур, и др.

3. Предложена классификация лиц, совершающих мошенничество с использованием телекоммуникационных и компьютерных сетей, основанная на авторском подходе, сформированном в ходе осуществления анализа социально–демографических и нравственно–психологических характеристик личности преступников и практической деятельности органов внутренних дел, которая состоит из четырех групп лиц:

«Случайные». К данной группе относятся лица, оказавшиеся втянутыми в незаконную деятельность без осознания факта правонарушения в своих действиях либо заведомо введенные в заблуждение. Следует отметить, что в зависимости от конкретного эпизода относящиеся к данной

группе лица могут быть отнесены либо не отнесены к категории преступников исходя из наличия либо отсутствия умысла.

«Начинающие». Данная группа состоит, по аналогии с предыдущей классификацией, из лиц, однозначно понимающих, что их действия являются противоправными.

«Специалисты». В рамках настоящей классификации в данной категории предполагаются лица, на «профессиональном» уровне реализующие как отдельно взятый этап мошенничества с применением компьютерного и телекоммуникационного оборудования, так и совокупность таковых действий.

«Организаторы». Представители данной категории заняты формированием эффективного взаимодействия всей преступной цепочки, начиная от формирования схемы получения первичных данных (данные банковских карт, номера телефонов) и заканчивая процессом распределения средств от преступной деятельности.

Предлагаемая классификация позволяет, в первую очередь, установить истинный «уровень значимости» каждого из участников преступной группы, что, в свою очередь, позволит определить необходимые методы и механизмы работы как с отдельно взятой личностью в составе преступной группы, так и со всей группой в целом. В рамках дальнейшего развития криминологической науки на базе предлагаемой модели можно провести разработку значительного числа «шаблонных» механизмов профилактики и противодействия преступлениям рассматриваемого вида.

4. Проведены исследования личности преступников, в различной степени участвующих в совершении рассматриваемого вида мошенничества, связанные с определением их интеллектуального уровня.

Установлено, что значительная часть преступников обладает интеллектуальным потенциалом высокого и выше среднего уровней. Именно благодаря значительным интеллектуальным способностям основной массы

преступников появляются все новые способы совершения мошенничества с использованием телекоммуникационного и компьютерного оборудования.

Данный вывод и полученные результаты должны в дальнейшем послужить основанием для разработки особой системы пенитенциарного и постпенитенциарного сопровождения рассматриваемой категории лиц для перенаправления их способностей в полезное социуму русло.

5. Проведенный в ходе работы анализ позволил определить значительные перспективы развития системы виктимологической профилактики рассматриваемого вида деяний. Предполагаемая система должна быть построена на применении уже имеющихся информационно–аналитических ресурсов органов внутренних дел с определенным объемом дополнений.

В настоящее время в деятельности МВД используется система баз данных, содержащих информацию по различным преступлениям. Достаточно простым решением вопроса анализа этих данных, включая и цели виктимологического учета, представляется внедрение программной надстройки, позволяющей группировать зарегистрированные преступления по соответствующим статьям УК РФ; выводить данные о численности потерпевших; разграничивать их по территории проживания, а также персонифицировать их.

6. Обоснована необходимость формирования структурных межведомственных связей в среде профилактики и противодействия рассматриваемому виду мошенничества.

В настоящее время все более актуальной становится потребность в единой концепции взаимодействия субъектов – участников системы предупреждения мошенничеств, совершаемых с использованием телекоммуникационного и компьютерного оборудования. Для достижения этой цели был разработан механизм привлечения и участия субъектов коммерческого сектора с органами внутренних дел, основанный на действующей системе взаимодействия между отдельными представителями крупного бизнеса и государственными структурами.

Теоретическая значимость полученных результатов. Полученные теоретические результаты исследования развивают существующие научные представления о мошенничестве с использованием телекоммуникационных и компьютерных сетей, равно как и о системе профилактики и пресечения данного вида противоправных деяний.

Отдельные положения настоящей работы являются логическим и обоснованным продолжением актуальных криминологических исследований различных авторов и имеют потенциал дальнейшего развития для целей расширения границ научного познания отечественной криминологии.

Практическая значимость полученных результатов. Полученные в ходе исследования материалы стали основой для проведения практических мероприятий виктимологического характера. Кроме того, отдельные теоретические положения о потребности в развитии межведомственного взаимодействия нашли свое применение в практической деятельности автора.

Значительный охват вопросов, связанных с мошенничеством, совершаемым с использованием телекоммуникационного и компьютерного оборудования, позволил провести комплексный междисциплинарный анализ рассматриваемого явления, что может послужить основой для последующих научных исследований.

Степень достоверности результатов исследования подтверждается:

– использованием в материалах работы фундаментальных исследований отечественных ученых–криминологов, а также правоведов в области уголовного права;

– применением комплекса общенаучных и частно–научных методов познания, соответствующих объекту и предмету исследования, а также его целям и задачам;

– проведением анализа материалов уголовных дел на стадии предварительного следствия, а также материалов судебной и иной правоприменительной практики;

– применением материалов официальной статистики органов внутренних дел и Прокуратуры РФ.

Апробация и внедрение результатов. Основные положения и выводы, сформулированные в диссертации, отражены в семи публикациях, в том числе пять – в научных журналах, входящих в перечень рецензируемых научных изданий, в которых должны быть опубликованы научные результаты диссертации.

Кроме того, в настоящее время на базе УМВД по г. Хабаровску подготавливается система практической реализации мероприятий, основанных на отдельных положениях настоящего исследования. Ряд вопросов практической реализации авторского подхода рассматривались в статье «Практика межведомственного взаимодействия правоохранительных органов и коммерческих структур в системе противодействия преступлениям корыстной направленности, совершаемым с использованием телекоммуникационного и компьютерного оборудования», опубликованной в научно–практическом журнале «Вестник Всероссийского института повышения квалификации сотрудников Министерства внутренних дел Российской Федерации»[4].

Структура работы обусловлена сформулированной целью и обозначенными задачами. Диссертация состоит из введения, трех глав, объединяющих шесть параграфов, заключения и библиографического списка.

[4] См. также: Камко, А. С. Портрет современной преступности Хабаровского края // Молодёжь Востока России: история и современность : материалы VI Всероссийской научно-практической конференции 1 ноября 2019 г. – Хабаровск : Дальневосточный институт управления – филиал РАНХиГС, 2019. – С. 120-123.; Камко, А. С. Уголовно–правовые вопросы противодействия преступности в сфере безналичных расчетов // Сборник материалов научно–практической конференции «Актуальные вопросы обеспечения прав и свобод человека и гражданина: региональное измерение», Хабаровск, 2017. – С. 187–193.

1 КРИМИНОЛОГИЧЕСКАЯ ХАРАКТЕРИСТИКА МОШЕННИЧЕСТВА, СОВЕРШАЕМОГО С ИСПОЛЬЗОВАНИЕМ ТЕЛЕКОММУНИКАЦИОННОГО И КОМПЬЮТЕРНОГО ОБОРУДОВАНИЯ: ОТЕЧЕСТВЕННЫЙ И ЗАРУБЕЖНЫЙ ОПЫТ

1.1 Особенности мошенничества, совершаемого с использованием телекоммуникационного и компьютерного оборудования

Преступность стала одной из главных угроз современности, в первую очередь национальной безопасности государства. Интенсивный рост преступности опережает темпы прироста населения, постоянно приобретая все новые формы и проникая в различные сферы человеческой жизни. Качественные изменения происходят в сторону большей изощренности преступлений, происходит увеличение их общественной опасности и причиняемого ущерба. В условиях активизации борьбы с ней преступность организуется, становится более интеллектуально развитой, эффективно использует все достижения современных технологий. За прошедшее столетие количество преступлений в среднем увеличилось на порядок. Постоянная эволюция преступности приводит к тому, что наряду с фактическим ее ростом происходит непрерывный процесс криминализации новых видов общественно опасного поведения[5].

Между тем основные цели совершения преступлений остаются неизменными. Одним из наиболее ярких явлений преступной среды, совмещающих в себе новые методы совершения и ставшие уже привычными цели, яв-

[5] См. например: Лунеев В.В. Курс мировой криминологии. М., 2011. С. 334.

ляется мошенничество, совершаемое с использованием телекоммуникационного и компьютерного оборудования.

Данный вид мошенничества характеризуется тем, что совершается путем применения в процессе средств мобильной (чаще всего – сотовой) связи; возможностей сети Интернет; компьютерного и иного программируемого оборудования.

Следует отметить, что «согласно последнему исследованию Всероссийского центра изучения общественного мнения (далее – ВЦИОМ), «сталкиваться с противоправными действиями, связанными с сотовой связью и интернет–сервисами» довелось 31% жителей России, то есть трети россиян»[6].

Наиболее частой целью мошенников, совершающих преступления рассматриваемой категории, становятся банковские пластиковые карты.

Такая пластиковая карта представляет собой выпущенную банком платежную карту, привязанную к одному или нескольким банковским счетам, использующуюся для безналичных расчетов, в том числе и через сеть Интернет, а также для снятия наличных или пополнения счета через банкомат или пункт выдачи наличных[7].

По данным статистики, с 2008 года по 2018 год количество банковских карт, эмитированных кредитными организациями в России, увеличилось на 148 677 тысяч единиц[8] (рисунок 1).

Каждая банковская пластиковая карта относится к той или иной международной платежной системе (далее – МПС). Четверка основных международных платежных систем, которые используются во всем мире, в том числе и в России – это VISA, MasterCard, AmericanExpress и DinersClub.

---

[6] Треть россиян стали жертвами интернет–мошенников [Электронный ресурс] // Режим доступа: https://news.rambler.ru/articles/35808456/?utm_content=rnews&utm_medium=read_more&utm_source=copylink

[7] Лукьянов С.О. мошенничество с использованием банковских карт в России: современное состояние и виды защиты // Вестник ТГЭУ. 2012. № 2.

[8] Центральный банк Российской Федерации [Электронный ресурс] // Режим доступа: http://www.cbr.ru/statistics/p_sys/print.aspx?file=sheet013.htm

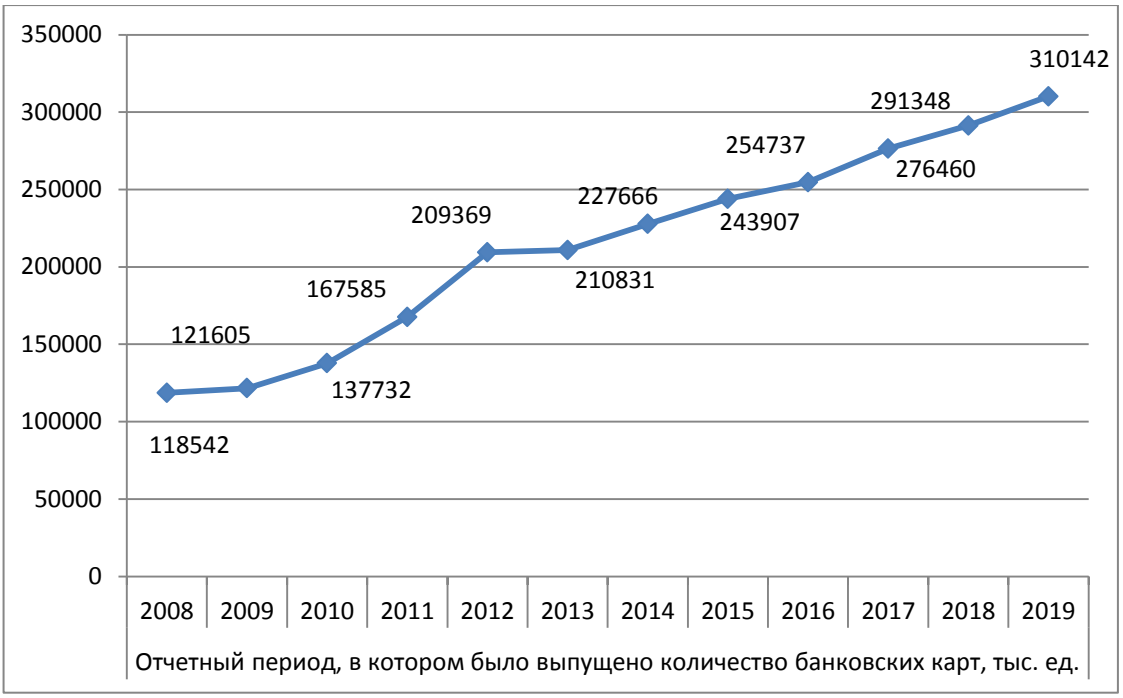


Рисунок 1 – Динамика изменений количества банковских карт, выпущенных кредитными организациями в Российской Федерации за период 2008–2019 годов[9]

Лидером среди них является международная платежная система VISA, примерно 57% всех выпущенных банковских карт принадлежат именно этой платежной системе. Банковские карты VISA принимают более чем в двухстах странах мира. На втором месте по популярности находится платежная система MasterCard, на долю которой приходится около 26% всех банковских карт, выпущенных в мире. Платежная система MasterCard проигрывает платежной системе VISA по количеству выпущенных в мире банковских карт, но по количеству торговых точек и стран, где принимают такие банковские карты, не уступает ей[10].

Эти две платежные системы являются абсолютными лидерами в мире, а также удерживают большую часть рынка России, что делает статисти-

[9] Составлено автором на основе статистических данных ЦБ РФ [Электронный ресурс] // Режим доступа: https://www.cbr.ru/statistics

[10] Лукьянов С.О. Мошенничество с использованием банковских карт в России: современное состояние и виды защиты // Вестник ТГЭУ. 2012. № 2. С. 201.

ческую информацию данных платежных систем достаточно актуальной для применения в целях настоящего исследования.

Анализ судебно–следственной практики показывает, что вместе с процессом постоянного роста эмиссии банковских карт с каждым годом все более актуализируется проблема их компрометации, наиболее сложными сторонами которой до сих пор остаются два вида преступлений: изготовление поддельных банковских карт и АТМ–мошенничество (от англ. Automated teller machire – банкомат) как виды преступных посягательств в сфере экономики. Последние характеризуются высокой изобретательностью злоумышленников и вариативностью способов при совершении преступных посягательств (фишинг–атаки, кардинг и т. п.)[11].

По оценке компании FICO, специализирующейся на защите банковских пластиковых карт (74% банковских пластиковых карт во всем мире защищены по технологиям, запатентованным данной организацией), Россия является лидером среди европейских стран по темпам роста убытков от мошеннических операций с банковскими картами. Согласно оценкам аналитиков FICO пиковым по объему мошеннических операций с банковскими картами для России стал 2013 год, когда наша страна достигла уровня Германии. Рассматривая хронологию развития и распространения мошенничества в банковском секторе и, в частности, преступлений, связанных с банковскими картами, следует отметить, что в 2011 году убытки от мошенничества в данной сфере были в России на одном уровне с Нидерландами, а в 2012 году Россия обогнала Нидерланды и сравнялась по данному показателю с Испанией. Согласно статистике компании «Euromonitor International», которая является одним из мировых лидеров среди независимых компаний, специализирующихся в области международных стратегических исследований потребительских рынков, на Россию приходится 6% от кардинга. Со-

[11]Нагорный В. А. Криминологические особенности некоторых преступлений, совершаемых в сфере оборота платежных карт // Права и свободы человека и эффективные механизмы их реализации в мире, России и Татарстане: материалы Международной научно–практической конференции, 28–29 ноября 2013 г. Казань: Познание, 2014. С. 493–498.

вокупные убытки от противоправных действий с банковскими картами в Европе в 2012 году выросли на 6% по сравнению с 2011 годом. Франция, Россия и Великобритания обеспечили 80% этого роста. При этом около 40% из них приходятся на долю Франции, однако в России наблюдается максимальный абсолютный и относительный рост данного показателя по сравнению со странами Европы. В 2013 году Россия сохранила за собой статус лидера среди европейских стран по темпам роста убытков от мошеннических операций с банковскими картами. Объем потерь вырос на 27,6% по сравнению с 2012 годом (официально – до 104,1 млн евро) и в 10 раз по сравнению с 2006 годом. С этим показателем Россия находится на четвертом месте среди девятнадцати европейских стран, представленных в карте «Эволюция карточного мошенничества в Европе 2013» компании FICO. Во главе данного списка находятся Великобритания (534,9 млн евро), Франция (428,9 млн евро) и Германия (116,3 млн евро)[12].

В 2014 году значительный рост рассматриваемого вида преступлений вызвал ответную реакцию со стороны представителей правоохранительных структур и специалистов отечественного рынка программного обеспечения. Так, в частности, проведя анализ статистических показателей, правоохранительные органы определили, что в структуре мошеннических операций с банковскими картами операции с использованием мобильных устройств и интернета стали резко превалировать по сравнению с объемом операций с использованием банкоматов и платежных терминалов. Вслед за этим эксперты «Лаборатории Касперского» в 2014 году обнаружили свыше 12 тысяч мобильных банковских «троянцев» – это в 9 раз больше, чем годом ранее[13].

В дальнейшем проводимый специалистами FICO мониторинг показал, что темпы роста «карточного мошенничества» в России несколько сни-

---

[12] Носкова Е. Убытки от мошенничества выросли в 10 раз // Российская газета, 2014. [Электронный ресурс] // Режим доступа: http://www.rg.ru/2014/08/19/moshennichestvo.html

[13] Карточные фокусы мошенников [Электронный ресурс] // Режим доступа: http://www.banki.ru/news/bankpress/?id=7950837

зились (до +4% в год) и, несмотря на нахождение нашей страны в списке лидеров по данному показателю среди европейских стран, проблемная ситуация несколько стабилизировалась. Лидером же в 2015 году, как по сумме потерь владельцев карт, так и по темпам роста, стала Великобритания. Здесь в руки мошенников перешло 580,2 млн фунтов, что на 18% больше, чем годом ранее. Эта величина составляет 43% от потерь всех стран.

Авторы исследования назвали главным «виновником» значительного увеличения числа мошеннических операций в Соединенном Королевстве в 2015 году растущий объем интернет–торговли. Преступники использовали украденные платежные данные, которые пользователи оставляют на сайтах ненадежных интернет–магазинов и сервисов. Логично, что среди мошеннических транзакций с большим отрывом в 2015 году лидируют операции без присутствия карты (392,8 млн фунтов). На втором месте операции по украденным и потерянным картам (74,1 млн фунтов), далее – подделка карт (45,3 млн фунтов). Остальные виды воровства денег с карт принесли преступникам в 2015 году лишь 68 млн фунтов[14]. Россия же сравнялась в этом рейтинге с такими странами как Греция, Дания, Франция, Украина и Турция. Следует отметить, что показатели таких стран, как Испания, Германия и Австрия, не изменились – относительный прирост в них остался на прежнем уровне.

Рассматривая феномен мошенничества с банковскими картами, необходимо отметить, что реальной статистики убытков в РФ в настоящее время не существует, так как, во–первых, банки не стремятся обнародовать информацию о своих потерях от деятельности мошенников (поскольку не хотят портить репутацию), а во–вторых, граждане, пострадавшие от преступных действий, крайне редко обращаются в полицию. Это объясняется либо «незначительными» финансовыми убытками от противоправных дей-

[14] Британия лидирует по карточному фроду в Европе [Электронный ресурс] // Режим доступа: http://futurebanking.ru/post/3165

ствий, либо особенностями менталитета населения[15]. Подобная ситуация приводит к повышению латентности данного рода преступлений, что, в свою очередь, приводит к отсутствию достаточной статистической базы для разработки адекватных и актуальных мер противодействия мошенникам.

Кроме того, проблема сбора и анализа достоверных статистических данных отчасти обусловлена также разницей в квалификации деяний в соответствии с различными статьями УК РФ.

Таким образом, статистика по данному вопросу может быть разделена на официальную, т. е. основанную на данных МВД, и неофициальную – т. е. собранную по информации в интервью с различными должностными лицами, либо на материалах внутреннего документооборота банков и т. п.

Таблица 1 – Статистика ущерба от случаев мошенничества с банковскими картами

Год		2011	2012	2013	2014	2015	2016	2017	2018	2019
Ущерб, млн руб.	Офиц. данные МВД	32,21	140	150	172	195	236	257	281	297
	Неофиц. данные банков	5360	11000	12000	12800	13450	14200	15100	17200	19400

Составлено автором на основе материалов официальной статистики органов внутренних дел и статистических данных ФинЦЕРТ.

В рамках официальной статистики следует выделить показатели количества возбужденных и расследованных уголовных дел. Поскольку, как было указано выше, получить полную статистически верную картину не-

[15] О Стратегии развития банковского сектора Российской Федерации на период до 2015 года: Заявление Правительства Российской Федерации № 1472 п–П13: Центральный Банк Российской Федерации № 01–001/1280 от 05.04.2011 // Вестник Банка России. 2011. 20 апреля. № 21.

возможно, автор пришел к выводу о необходимости использования материалов управления «К» БСТМ МВД России как наиболее достоверных.

Основываясь на статистических данных компании FICO (рисунок 2), можно увидеть относительный объем каждого из видов мошенничества с банковскими картами в общем объеме убытков финансовых учреждений и физических лиц. Следует отметить, что компания FICO разграничивает мошенничество с банковскими картами по следующим видам:

– кража/потеря банковской карты;
– подделка карты;
– получение карты по поддельным/украденным документам;
– кража/потеря карты на почте;
– мошенничество с картой в интернете.

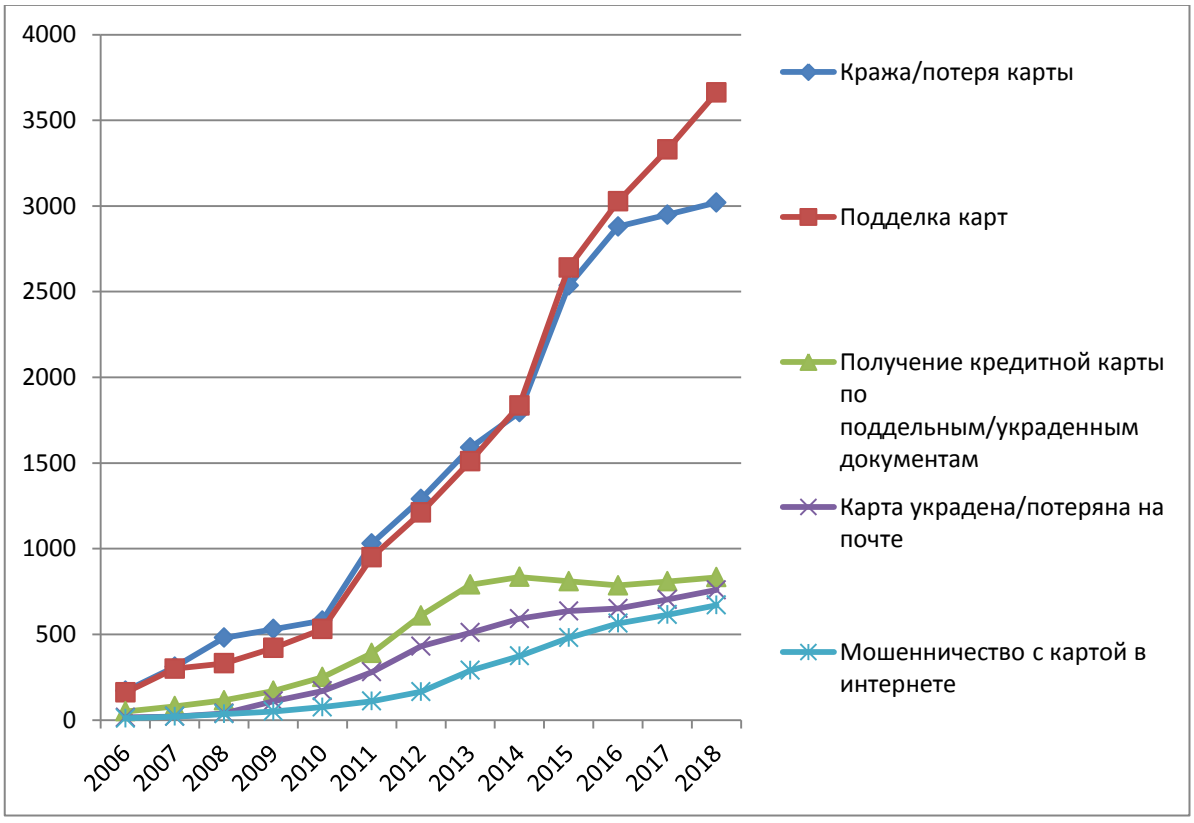


Рисунок 2 – Размер ущерба от различных видов мошенничества с банковскими картами в России по данным компании FICO[16].

[16] Составлено автором на основе статистических показателей, представленных компанией FICO [Электронный ресурс] // Режим доступа: https://www.fico.com/blogs/tag/score–distributions/

В свою очередь, международные платежные системы классифицируют мошенничество с банковскими картами по семи категориям:[17]

1) мошенничество с утерянными картами;
2) мошенничество с украденными картами;
3) мошенничество с неполученными картами;
4) мошенничество с фальсификацией заявления;
5) мошенничество с поддельной картой;
6) прочие виды карточного мошенничества;
7) «завладение» счетом, мошенническое использование карточного счета.

Как можно увидеть, различие в количестве категорий фиктивно, поскольку две «дополнительные» категории по классификации международных платежных систем (далее – МПС) представляют собой разделение на частные случаи по системе компании FICO.

Следует отметить, что постоянный рост технической оснащенности мошенников приводит к тому, что их действия в ряде случаев приобретают характеристики сразу нескольких выше обозначенных категорий одновременно. Так, например, после расходования всех доступных средств по утерянной или украденной карте, ее могут продать преступникам, специализирующимся на подделке платежных карт, которые, в свою очередь, используют карту как материал для повторного эмбоссирования. Также мошенники могут перезаписать информацию, содержащуюся на магнитной полосе карты.

По данным МПС, основным является мошенничество с утерянными и украденными картами – на него приходится около 50% всех случаев мошенничества с банковскими картами (так, например, в Росбанке на данный вид преступлений приходится около 30% от общего числа случаев мошенниче-

[17] Международная практика по организации эмиссии и борьбе с мошенничеством [Электронный ресурс] // Режим доступа: http://visa.com.ru/ru/ru–ru/personal/security/visacardsecurity.shtml

ства за год)[18]. В данном случае рассмотрение статистических данных всех задействованных в операциях с банковскими картами учреждений позволяет сделать вывод о том, что данный вид мошенничества является не только самым распространенным, но и, как показывают данные компании FICO, самым вредоносным с точки зрения финансового ущерба.

Банковские карты зачастую используются для получения денежных средств через пункты выдачи наличных и банкоматы (особенно при наличии ПИН–кода, хранящегося владельцем в нарушение правил вместе с картой) либо в торговых точках для приобретения ликвидного товара, когда кассир вследствие некоторых причин (загруженности или халатности), нарушая множественные запреты (в том числе и правила МПС), продает товар человеку, не являющемуся владельцем карты.

При этом, согласно УК РФ, квалификация данных деяний должна производиться по ст. 158 УК РФ и ст. 159^3 УК РФ при снятии денег с банкоматов либо получении товара в магазине, соответственно.

Еще одним распространенным типом мошенничества является использование поддельной карты с содержащимися на магнитной полосе данными другой (чужой) карты. Существует целый ряд способов получения данных чужой карты:

- сетевое проникновение в крупные процессинговые центры, компрометация данных карт;
- «социальная инженерия»;
- организация фиктивных пунктов выдачи наличных (ПВН);
- подключение к POS–терминалам техники в торговых точках или использование переносных устройств в ресторанах;
- установка накладок на приемные устройства и клавиатуру банкоматов, перехватывающей спецтехники внутри них (также «скимминг» –

[18] Международная практика по организации эмиссии и борьбе с мошенничеством [Электронный ресурс] // Режим доступа: http://visa.com.ru/ru/ru–ru/personal/security/visacardsecurity.shtml

копирование данных магнитной полосы карты) [19].

Несмотря на общность цели, каждый из методов имеет свои отличительные особенности, которые также влияют и на состав преступления. *Сетевое проникновение в крупные процессинговые центры и компрометация данных карт* в последнее время становятся все менее актуальными, поскольку способы и механизмы защиты данных постоянно совершенствуются. Так, например, использование вредоносного программного обеспечения, передающего данные с компьютерных сетей банковских учреждений третьим лицам, в настоящее время является технически сложной задачей ввиду постоянно обновляющихся антивирусных и прочих программ, направленных на защиту персональных данных. Следует при этом отметить, что высокий уровень сложности данного деяния не означает его невозможности. В данном случае успех преступления зависит от уровня и объема знаний преступника.

Так, в конце 2014 года преступниками были украдены данные 100 000 клиентов с серверов одного из небольших банков Европы. В другом случае в 2015 году у одного из американских банков были украдены данные 1 500 тыс. клиентов. В обоих случаях преступники использовали так называемый «ботнет», с помощью которого получали данные с серверов банка непосредственно на свой сервер, относящийся к сети Даркнет («Darknet»). Данная сеть – это частная сеть, соединения которой устанавливаются только между доверенными пользователями, иногда именующимися как «друзья»[20], с использованием нестандартных протоколов и портов передачи данных. Даркнет отличается от других распределенных одноранговых сетей, так как обмен файлами происходит анонимно (IP–адреса пользователей недоступны публично)[21]. Анонимность в данной сети достигается путем использования второго поколения так называемой »луковой маршрутизации», что приводит

[19] Лукьянов С.О. Мошенничество с использованием банковских карт в России: современное состояние и виды защиты // Вестник ТГЭУ. 2012. № 2. С. 201.
[20] Mansfield–Devine S. «Darknets» // Computer Fraud & Security. 2009 (12). P. 4–6 [Электронный ресурс] // Режим доступа: doi:10.1016/S1361–3723(09)70150–2.
[21] Wood J. «The Darknet: A Digital Copyright Revolution» / J. Wood // Richmond Journal of Law and Technology. 2011. № 16(4).

к невозможности отследить пакеты данных от отправителя к получателю.

Однако использование данной технологии лишь обеспечивает анонимность преступника, для получения данных необходимо использовать такое программное обеспечение, которое не будет обнаружено антивирусными программами. В данном случае преступник внедрил подпроцесс исполнения своей программы в системный процесс (в частности, использовался процесс svhost.exe, относящийся к основным системным процессам и не сканируемый антивирусными программами). Таким образом, факт возможности совершения данного рода деяний неоспорим, однако особенности профиля личности преступника позволяют формировать соответствующие методы и механизмы профилактики преступлений.

Методы так называемой «социальной инженерии» – это методы получения несанкционированного доступа к информационным ресурсам, основанные на особенностях психологии человека[22]. Основной целью правонарушителей, применяющих данный метод, как и других хакеров и взломщиков, является получение доступа к защищенным системам и последующая кража информации, паролей, данных о кредитных картах и т. п. Главное отличие от стандартной кибер–атаки состоит в том, что в данном случае в роли атакуемого объекта выступает не компьютер, а человек. Именно поэтому все методы и техники социальных инженеров основаны на использовании человеческих слабостей, «человеческого фактора», что считается крайне разрушительным, поскольку злоумышленник получает информацию, например, с помощью обычного телефонного разговора или путем проникновения в организацию под видом ее служащего. Для защиты от подобного рода атак необходимо не только знать о наиболее распространенных видах мошенничества, но и понимать, какую цель преследуют взломщики и постоянно актуализировать политику безопасности.

Организация фиктивных пунктов выдачи наличных (ПВН); подключение к POS–терминалам техники в торговых точках или использование пере-

[22] Goodchild J. Social Engineering: The Basics. / J. Goodchild // CSOonline. 2010. № 1.

носных устройств в ресторанах и установка накладок на приемные устройства и клавиатуру банкоматов, перехватывающей спецтехники внутри них относятся к так называемому скимингу. Скимминг (от англ. *Skim* – снимать сливки) является методом получения данных платежной карты, при котором используется специальный инструмент – скиммер, позволяющий считывать, например, данные магнитной полосы банковской карты. В процессе реализации мошеннических мероприятий применяется комплекс специализированных устройств:

– комплект инструментов для считывания магнитной дорожки платежной карты – специальное устройство, монтаж которого производится в картоприемник, и устройство для чтения данных с магнитной полосы пластиковой карты (картридер), устанавливаемый на магнитный контроллер замка входной двери в зону обслуживания клиентов в помещении банка. Последнее представляет собой устройство со считывающей магнитной головкой, усилителем – преобразователем, памятью и переходником для подключения к компьютеру. Скиммеры могут быть портативными, миниатюрными. Основной целью и задачей скимминга является получение (считывание) данных (содержимое дорожки/трека) магнитной полосы банковской карты для последующего переноса этих данных на поддельную карту. Таким образом, в процессе оформления операций по поддельной карте запрос авторизации и последующее списание денежных средств по мошеннической транзакции будут осуществлены со счета оригинальной, «скиммированной» карты;

– миниатюрная видеокамера, используемая для получения ПИН–кода держателя карты. Камера устанавливается на банкомат и направлена на клавиатуру ввода (выполняется камера обычно в виде козырька банкомата либо посторонних накладок, например, рекламных материалов).

Данные устройства подключены к автономным источникам энергоснабжения – миниатюрным батареям электропитания, и для затруднения обнаружения зачастую они изготовлены и замаскированы под цветовую гамму и форму банкомата.

В основном скиммеры работают в двух направлениях: накапливают украденную информацию о пластиковых картах, либо дистанционно передают ее злоумышленникам, находящимся поблизости, по радиоканалу. После получения информации с оригинальной банковской карты мошенники изготавливают ее дубликат и, зная ПИН, снимают все доступные в пределах лимита выдачи деньги, как в России, так и за рубежом. Кроме того, текущий уровень технологий позволяет мошенникам использовать незаконно полученную информацию для совершения покупок в торговых точках.

О динамике распространения скимминга как явления говорят и результаты исследований различных авторов, изучающих данное направление преступной деятельности. Значительный вклад в исследование данного вопроса был внесен сотрудниками Экспертной АТМ–группы АРЧЕ (Ассоциации Российских членов ЕВРОПЕЙ), результаты деятельности которой освещались в рамках конференции «Банкоматы в России и СНГ 2012». Большая часть материалов и разработок экспертной группы посвящена проблемам обеспечения безопасности в процессе использования платежных карт.

Так, согласно статистическим данным, в 2011 году в РФ было зафиксировано 397 фактов скимминга, то есть 3 случая на 1000 банкоматов. Для сравнения, в странах Европы данный показатель находился на отметке 19 случаев на 1000 банкоматов[23]. По данным же за 2012 год, было зафиксировано уже 1286 случаев. В последующие 2013 и 2014 годы значительный прирост данного вида преступлений продолжился и составил 1754 и 2395 случаев соответственно. Определенный перечень мер, повсеместно принятых банковскими учреждениями, позволил несколько снизить эту негативную динамику, и в 2015–2016 годах количество случаев скимминга «упало» до примерно равных отметок в 1986 и 1941 случай соответственно. В 2017 году тенденция сохранилась – 1891 случай, однако в 2018-2019 годах ситуация снова приняла негативную динамику – 1962 и 2013 случаев соответственно

[23] Наличные деньги и электронные средства платежа: проблемы, тенденции // Деньги и кредит. 2012. № 7. С. 3–23.

(рисунок 3). За первые три месяца 2020 года в сравнении с аналогичным периодом 2019 года относительный прирост по рассматриваемому виду явлений составил 1,76%.

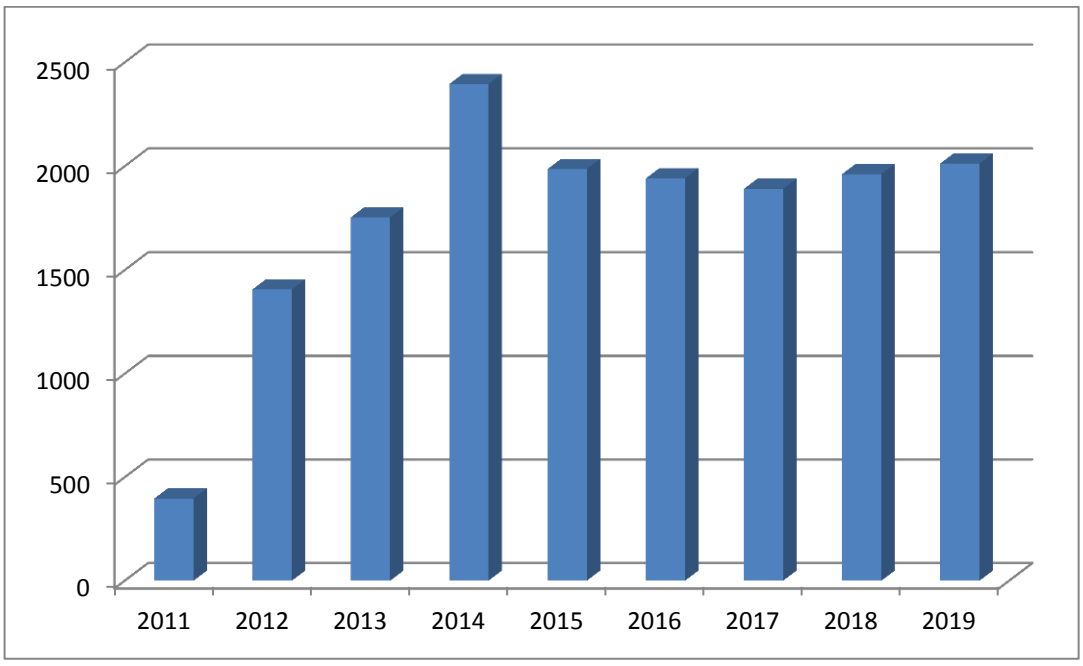


Рисунок 3 – Количество случаев скимминга, официально зарегистрированных в РФ[24]

Учитывая высокую латентность преступлений данной направленности, стоит отметить, что приведенные данные отражают лишь зарегистрированные факты скимминга, реальный объем похищенных средств назвать не представляется возможным. На актуальность данной проблемы обратил внимание и правоприменитель. Так, ЦБ РФ в Письме от 1 марта 2013 года № 34–Т «О рекомендациях по повышению уровня безопасности при использовании банкоматов и платежных терминалов» указал на необходимость классификации мест установки банкоматов, платежных терминалов

[24] Составлено автором на основе статистических данных ФинЦЕРТ [Электронный ресурс] // Режим доступа: https://www.cbr.ru/fincert/

по степени риска подвергнуться в том числе попыткам установки скимминг-гового оборудования[25].

Исследуемые преступные деяния препятствуют как нормальному функционированию, так и распространению современных форм безналичных расчетов. Кроме того, они наносят значительный вред репутации банков, отвечающих за безопасность данного вида расчетов и обслуживающих клиентов. Поэтому, определяя актуальные тенденции рынка банковских карт, необходимо выделить характерные особенности мошенничества, совершаемого с использованием банковских карт, как явления в целом.

1. В качестве одной из детерминант значительного роста скимминг–атак на ПВН и банкоматы следует выделить *комплекс «технических» причин*, к которым следует отнести: сравнительно слабый уровень защищенности платежных карт, оснащенных магнитной полосой (по оценкам экспертов, их количество на рынке пластиковых карт составляет порядка 80% от общего количества)[26], в связи с чем в настоящее время большее предпочтение стали отдавать эмиссии карт со встроенными чипами, обеспечивающими более высокий уровень защиты. Знаковым в этом вопросе стало решение Сбербанка России о переходе с 1 июля 2013 года к эмиссии банковских карт, оснащенных исключительно чипами, что существенно повышает уровень безопасности электронных средств платежа, однако до настоящего времени эффект от данного нововведения не проявился[27].

2. *Наличие определенных сложностей при выявлении факта совершения деяния*. Данная проблема обусловлена значительным хронологическим разрывом между действиями, связанными с обнаружением владельцем факта совершенного посягательства, последующим проведением про-

---

[25] Письмо Банка России от 01.03.2013 № 34–Т «О рекомендациях по повышению уровня безопасности при использовании банкоматов и платежных терминалов» [Электронный ресурс] // Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_143007/

[26] Статистика рынка безналичных расчетов в РФ [Электронный ресурс] // Режим доступа: http://www.cbr.ru/statistics/?PrtId=pdko

[27] Сбербанк с 1 июля откажется от выпуска карт с магнитной полосой [Электронный ресурс] // Режим доступа: http://wwwinterfax.ru/ifx.asp?id=8f938919–675e–f24b–9e51–62f1e702b73a

верочных мероприятий по обстоятельствам, изложенным в заявлении потерпевшего, принятием решения о возбуждении уголовного дела и дальнейшим его расследованием, с одной стороны, и относительно быстрыми действиями преступников, которые, получив информацию, содержащуюся на карте, и используя эти сведения, изготовив поддельную банковскую карту, максимально оперативно (зачастую в течение суток) снимают денежные средства со счета жертвы.

3. В рамках исследования необходимо также отметить, что *скимминг является первичным этапом в последовательной цепи противоправных действий*, направленных на получение денежных средств со счетов потерпевших при помощи банковской карты. Ввиду данного факта в действиях преступников зачастую можно обнаружить признаки составов преступлений, предусмотренных ст. 183 УК РФ (сбор информации, составляющей коммерческую, налоговую или банковскую тайну) и ст. 187 УК РФ (изготовление или сбыт поддельных кредитных либо расчетных карт и иных платежных документов). Преступную схему возможно представить в виде трех взаимосвязанных деяний: сбор информации о банковской карте – изготовление поддельной карты, содержащей собранную информацию – хищение денежных средств с банковского счета потерпевшего.

Таким образом, причиной количественного роста случаев скимминга является наличие множества способов дальнейшего использования полученных данных. Соответственно, значительный рост различного числа связных деяний влечет за собой рост и случаев скимминга.

4. С.П. Кушниренко, Н.А. Данилова и А.Н. Саржин в своем исследовании отмечают, что большая часть хищений с использованием поддельных банковских карт *совершается высокоорганизованными преступными группами*, отдельными членами которых являются лица с соответствующим техническим образованием, полученным как самостоятельно, так и в высших учебных заведениях, но всегда отличающиеся высоким уровнем тех-

нической подготовки[28]. Представляется, что таким образом проявляется своего рода «разделение труда», при котором в рамках преступной группы одни ее члены занимаются изготовлением, либо приобретением необходимого оборудования, вторые – устанавливают считывающие устройства на банкоматы (или иные устройства аналогичного назначения), третьи – изготавливают поддельные пластиковые карты, четвертые – наносят полученные данные на фальшивые инструменты платежа, а пятые – обналичивают денежные средства.

5. *Высокий уровень технической подготовки злоумышленников*. В рамках рассмотрения практического аспекта данного вопроса интерес представляет исследование Д.А. Кузнецова, в ходе которого было установлено, что для подделки банковской карты и получения ее ПИН–кода злоумышленники используют такие устройства, как: эмбоссер – механизм, позволяющий наносить надписи на пластиковую основу, из которой изготавливается поддельная банковская карта; тайпер, служащий для «впаивания» магнитной пленки на пластиковую основу будущей карты; скиммер – устройство, считывающее информацию, в дальнейшем переносимую в память ЭВМ для последующей обработки; энкодер, с помощью которого происходит запись полученной информации на пластиковую карту[29].

6. *Международный характер* исследуемого направления преступной деятельности проявляется в том, что участниками схемы незаконной деятельности могут быть граждане нескольких государств, а также участники международных преступных организаций, кроме того, процесс получения данных и изготовления поддельной банковской карты может быть реализован на территории одной страны, а получение денежных средств с нее произведено в другой стране.

Так, в апреле 2012 года сотрудниками Управления «К» МВД России

---

[28] Цитируется по: Данилова Н.А., Кушниренко С.П., Саржин А.Н. Преступления в сфере банковской деятельности как высокотехнологичные преступные посягательства международного характера // Вестник Санкт–Петербургского университета МВД России. 2006. № 2. С. 329–333.

[29] Там же.

была пресечена деятельность организованной преступной группы, входившей в состав международного «кардерного» сообщества, центр которого располагался в Республике Молдова. Двое граждан Молдовы, используя скимминговое оборудование, получали реквизиты и ПИН–коды платежных карт, относящихся к МПС «Visa» и «MasterCard», в дальнейшем используя их для изготовления поддельных банковских карт и последующего хищения денежных средств с банковских счетов действительных держателей карт как на территории РФ, так и за ее пределами. В результате действий правоохранительных органов было предотвращено хищение средств на сумму свыше 4 млн рублей[30].

Далее кратко рассмотрим оставшиеся виды мошенничества с банковскими картами.

Следует указать мошенничество с использованием реквизитов карты (в том числе в сети Интернет), к которым относятся: номер карты, срок ее действия, CVC или CVV–код (три последних цифры на обороте карты).

Ситуация осложняется тем, что в условиях жесткой конкуренции кредитные организации прибегают к всевозможным способам предложения кредитных карт. На практике подобное поведение кредитных организаций оказывается малоэффективным, а зачастую еще и сопряжено со значительными рисками, как для организаций, так и для клиентов. Многие банки в последние годы стали использовать экспресс–метод кредитования, основанный на рассылке кредитных карт через почтовые и курьерские службы. Наиболее характерна подобная система для банков, стратегия которых основана на потребительском кредитовании.

Почтовая рассылка платежных карт является, с одной стороны, маркетинговым ходом, с другой – попыткой кредитных организаций использовать недостаточный уровень финансовой и юридической грамотности населения. При использовании данного метода кредитование граждан произво-

[30] Пресс–служба Управления «К» МВД РФ [Электронный ресурс] // Режим доступа: http://www.mvd.ru/news/show_104337/

дится при помощи неперсонифицированных карт с кредитным лимитом Instante Issue. При этом оценка заемщика происходит на основе применения скоринговых систем, что изначально сопряжено с высокой степенью риска невозврата займа. Соответственно, по подобным кредитам устанавливается сравнительно небольшой лимит доступных средств и достаточно высокий уровень процентной ставки (чаще всего 40–60%)[31].

Высокая вероятность мошенничества – один из факторов, который определяет высокую степень риска по кредитам такого рода и, как следствие, влияет на его высокую стоимость для получателя. Путем применения высокой процентной ставки банк компенсирует бреши в риск–менеджменте по авторизации кредита за счет клиента. Также при почтовой пересылке такого рода карт высока вероятность копирования данных, содержащихся на магнитной полосе. Вторым фактором, значительно повышающим уровень риска такого метода кредитования, является невозможность получения банком полной информации о клиенте и, соответственно, невозможность оценить его платежеспособность. Однако основным риском является возможность потери карты в нераспечатанном конверте, поскольку та может быть украдена из почтового ящика либо на другом этапе доставки. Несмотря на то, что карта и ПИН–код обычно доставляются отдельными письмами, их все равно приносит тот же почтальон и кладет в тот же ящик. Таким образом, разделение писем, содержащих ПИН–код и саму кредитную карту – условный способ защиты, не несущий действительного эффекта.

Рассматривая статистические данные компании FICO, можно сделать вывод о том, что, несмотря на уязвимость, возникающую при вышеописанной системе выдачи кредитных карт гражданам, по ущербу в нашей стране данный вид мошенничества также находится на третьем месте.

Кроме того, в 2011 году Высший арбитражный суд (ВАС) предложил установить прямой запрет на рассылку этих банковских продуктов, за ис-

---

[31] Пластик свободной конвертации [Электронный ресурс] // Режим доступа: http://www.prostobank.ua/layout/set/print/plastikovye_karty/stati/plastik_svobodnoy_konvertatsii.

ключением случаев, когда заемщик сам выразил намерение получить пластиковую карту именно таким образом[32]. Данная мера в нынешних условиях абсолютно оправдана.

В отдельную категорию выделяется *мошенничество с банковскими картами в сети Интернет*. Более точно данный вид мошенничества следует обозначить как мошенничество в системе дистанционного банковского обслуживания (ДБО).

Согласно статистике, переломными на рынке мошенничества в системе ДБО являлись 2008–2009 годы. На это повлияло одновременно два фактора: вызванное экономическим кризисом сокращение инвестиций в информационную безопасность на 7% со стороны банков РФ и широкое распространение средств совершения киберпреступления. За 2008–2009 годы объем мошенничества в ДБО вырос в 2,8 раза[33] (рисунок 4).

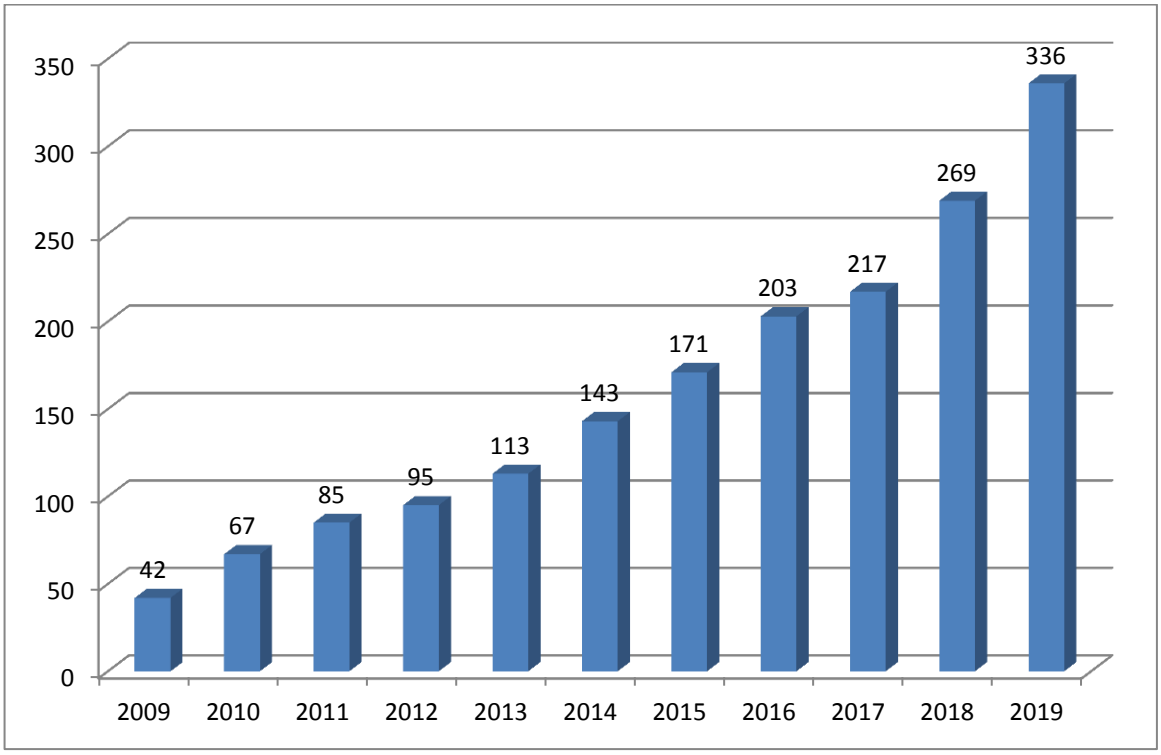


Рисунок 4 – Прямой ущерб от мошенничества в ДБО в России, млн долл.[34]

[32] Репин М.Е., Афанасьев А.Ю. Преступления в сфере компьютерной информации: проблемы выявления и раскрытия // Молодой ученый. 2015. № 15. С. 460–463.

[33] Статистика работы банковского сектора. ЦБ РФ [Электронный ресурс] // Режим доступа: http://www.cbr.ru/statistics/?PrtId=pdko

[34] Составлено автором на основе статистики Центра мониторинга и реагирования на компьютерные атаки в кредитно–финансовой сфере – ФинЦЕРТ [Электронный ресурс] // Режим доступа: http://www.cbr.ru/statichtml/file/14435/fincert_survey.pdf

Широкое освещение дел по задержанию злоумышленников в 2011–2012 годах, а также повышенное внимание служб безопасности банков к угрозам в ДБО повлияло на снижение ущерба от действий преступных группировок, промышляющих на территории РФ. Темпы роста убытков приостановились с 60% в 2010 году до 12% в 2012 году.

Однако технологии совершения киберпреступлений не стоят на месте, потому в 2013–2016 годах темпы роста убытков восстановились и, более того, увеличились за счет роста объемов транзакций и пользователей ДБО в целом, составив около 30 млн долл. ежегодно. Следует отметить некоторое снижение темпов роста ущерба в 2017 году – прирост составил всего 7,1%, но в 2018-2019 годах темпы прироста снова выросли – 24,2% и 25,1% соответственно.

Кроме того, российский рынок интернет–мошенничества становится все более привлекательным для злоумышленников не из стран СНГ.

Следует отметить, что детерминанты рассматриваемого вида мошенничества, равно как и всей экономической киберпреступности, по уровню субординации условно можно разделить на общие и специальные. Общие детерминанты в данном случае – это совокупность причин и условий, характерных как для рассматриваемого вида мошенничества, так и для всей экономической преступности в целом.

Следует согласиться с позицией М.А. Простосердова, что «общими детерминантами для всех экономических преступлений являются: экономический кризис, резкое снижение стоимости денежной массы, резкое повышение розничных цен на предметы первой необходимости (еду, одежду, коммунальные услуги), снижение уровня жизни, повышение уровня безработицы»[35] и т. д.

Специальные детерминанты мошенничества, совершаемого с использованием телекоммуникационного и компьютерного оборудования – это

[35]Простосердов М.А. Экономические преступления, совершаемые в киберпространстве, и меры противодействия им: дис. … канд. юрид. наук. – М., 2016. С. 54.

совокупность причин и условий, характерных лишь для рассматриваемого вида преступлений.

При рассмотрении мошенничества, совершаемого с использованием телекоммуникационного и компьютерного оборудования, следует отметить такие стабильно сохраняющиеся детерминанты, как:[36]

- небрежность и неосведомленность держателей карт;
- соучастие в преступлениях инсайдеров;
- трансграничность преступлений;
- появление новых угроз в связи изменениями, как в технологии карточной индустрии так и с развитием общества в целом;
- развитие высокотехнологичных форм преступления, требующих специальных знаний;
- повышение уровня угроз со стороны традиционной преступности.

По мнению автора, справедливым является подход, в соответствии с которым к особенностям преступлений в отношении банкоматов и АТМ–терминалов следует, в первую очередь, отнести:[37]

- закрытость информации относительно преступлений против АТМ;
- отсутствие систематизации по данному виду преступлений;
- преступления против АТМ квалифицируются как грабеж, кража, мошенничество или совсем не попадают под понятие уголовного преступления;
- отсутствие полных и достоверных данных о преступлениях против АТМ;
- отсутствие криминологических исследований в данной области;

[36] Березуцкая А. Г., Яблонская А. Е. Современные проблемы безопасности пластиковых карт в платежной системе России // ЭПП. 2016. № 3. – С.195–202.
[37] Там же.

– отсутствие согласованных действий в данной области со стороны правоохранительных органов, производителей, кредитных организаций, процессинговых центров.

Еще одним источником незаконного обогащения преступников, относящимся к сфере «высокотехнологичных», являются преступления, связанные с платежными терминалами.

Появившиеся в начале 2000–х годов платежные терминалы решили многие проблемы населения в области наличных платежей и произвели настоящую революцию на этом рынке. По данным Национальной ассоциации участников электронной торговли, оборот платежных терминалов в 2009 году составил 630 млрд рублей, количество установленных терминалов перевалило за 350 тысяч, а количество совершенных транзакций – за 5 миллиардов, однако в 2013 году данные показатели не имели значительного роста по отношению к предыдущим периодам, однако с 2015 по 2017 год оборот платежных терминалов снова отмечен стабильным приростом на 6–7% ежегодно, показав к середине 2017 года прирост в 19,3%[38].

Приведенная статистика отражает значимость платежных терминалов на рынке электронных финансовых услуг. Представители Банка России отмечали, что участники рынка мобильных платежей, использующие терминалы, фактически создали параллельную банковскую систему. Однако и банки, и банковский регулятор обратили внимание на бурно растущую отрасль лишь с 1 апреля 2010 года, когда полностью вступил в силу Федеральный закон Российской Федерации от 3 июня 2009 года № 103–ФЗ «О деятельности по приему платежей физических лиц, осуществляемой платежными агентами».

Аналогично ситуации в сфере банковских платежных карт платежные терминалы кроме очевидных удобств принесли сопутствующие риски мошенничества. Виды мошенничества с платежными терминалами можно условно разделить на две категории, по сути обозначающие типы угроз:

[38] http://www.cbr.ru/statistics/pdko/lic/

(1) мошенничество, совершенное посредством применения информационных технологий, и (2) мошенничество, основанное на механических способах обмана платежного терминала. Дополнительным, «инновационным» риск–фактором является появление на рынке киберпреступности такого явления, как FaaS (Fraud–As–A–Service), или «мошенничество, как услуга». Суть этого явления в том, что если еще несколько лет назад хакеры взламывали компьютерные системы ради прямой личной выгоды (и, косвенно, демонстрации своих возможностей), то сегодня они предлагают мошеннические услуги другим нечистоплотным пользователям, работая за «комиссию» от мошеннической сделки.

Самой примитивной и часто реализуемой «физической» атакой на терминал является его кража. Компьютерные средства защиты включают в себя активный и пассивный мониторинг терминала, включая систему оповещения в реальном времени, видеонаблюдение (реальное или мнимое) и мониторинг на открывание и удар («сторожевой таймер», или «watchdog»). Установка кассет с защитными несмываемыми чернилами, часто используемая в банкоматах, обычно непопулярна.

Любопытной вариацией на тему физической кражи терминала является так называемый «балаковский» сценарий, или, как его назвали журналисты, «размножатель денег»: в пригороде Саратова мошенники похитили и увезли терминал, подключили его к сети в своем гараже и многократно «прокатывали» через него однотысячную купюру, проводя платежи в свою пользу.

Методы защиты от такого рода атаки включали бы следующее: энергонезависимое питание купюроприемника, мониторинг оповещений о его открытии (или частоте выключений терминала), географический мониторинг модемов и настройки на серверном программном обеспечении, которые позволили бы обнаружить нетипичный случай многократного, частого платежа купюрой одного и того же номинала.

Известны также случаи установки неавторизованного, или «черного», терминала с внешним видом и интерфейсом, имитирующими терминалы известных компаний, что несет репутационные риски для владельцев. Методов защиты от такого рода мошенничества, в общем, немного, но сам по себе риск снижен высокими накладными расходами для злоумышленников (сравнимыми с денежной емкостью кассеты купюроприемника).

Рассматривая вопрос компьютерных атак на платежные терминалы, важно помнить, что, как и банкоматы, терминалы включают в себя обычный, хоть и специальным образом защищенный и настроенный компьютер. Как и для обычного компьютера, для терминалов актуальна угроза применения вредоносного ПО, что, в случае получения злоумышленником контроля над терминалом, может позволить ему проводить незаконные платежи, создавать новых получателей платежей, подменять кнопки на сенсорном экране терминала, удалять или добавлять записи, накапливающиеся в файле терминала для «офлайн–платежей», а так же подменять логи валидатора и чекового принтера (или, с недавнего времени, контрольно–кассовой техники).

Внедрение вредоносного программного обеспечения на терминал происходит также традиционными методами: через ручное обновление программного обеспечения, через внешнюю память, через заражение базы обновлений на сервере и через локальную сеть в случае «проводного» подключения терминала. Средства защиты также традиционны: регулярные обновления, своевременная установка обновлений программного обеспечения (так называемых «патчей»), управление конфигурациями, отключение ненужных и неиспользуемых сервисов.

Еще одной целью для хакеров являются программы удаленного администрирования терминалов. Обычно низкоскоростные GPRS–каналы для удаленного управления терминалом не используются, однако в случаях, когда выезд ИТ–специалиста для настройки терминала обходится слишком

дорого или сопряжен с организационными сложностями, могут применяться программы типа «remote desktop»[39].

Само программное обеспечение терминала также подвержено атакам, в частности, на саму архитектуру приложения (на последовательность и связность формирования платежа, электронно–цифровую подпись (ЭЦП), на методы хранения ключей и т. д.). От атак такого рода владельцы терминалов могут защититься либо анализом текущей архитектуры программного обеспечения (ПО) на предмет уязвимостей, либо разработкой нового ПО с учетом методологий безопасной разработки, таких как, например, SDL (Security Development Lifecycle).

Существуют также атаки на трафик GPRS–модема, поскольку многие терминалы не используют VPN и ограничиваются шифрованием на уровне программного обеспечения (симметричным и асимметричным), фильтрацией динамического диапазона IP на уровне сервера и IP–сервера на уровне терминалов. К счастью, подобные атаки упираются в сложность метода перехвата GPRS–трафика и сравнительную дороговизну необходимого для этого оборудования.

Атаки на трафик при подключении через локальную сеть включают в себя все традиционные атаки на канал: «session hijacking», «session replay», «man–in–the–middle», и т. д. Методы защиты столь же традиционны – это защита как на уровне протоколов (SSL/VPN), так и на уровне инфраструктуры – использование коммутаторов, логическое разделение локальной сети на VLAN, фильтрация трафика внутри сети – «списки доступа»[40].

Таким образом, можно сказать, что платежные терминалы, в принципе, подвержены всем традиционным компьютерным уязвимостям. Сети платежных терминалов, разрабатываемые банками (или для банков) «с нуля», скорее всего, будут защищены на привычном для банков уровне, но

---

[39] Пресс–служба Управления «К» МВД РФ [Электронный ресурс] // Режим доступа: http://www.mvd.ru/news/show_104337/

[40] Письмо Банка России от 01.03.2013 № 34–Т «О рекомендациях по повышению уровня безопасности при использовании банкоматов и платежных терминалов» [Электронный ресурс] // Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_143007/

уже существующие сети, приобретаемые банками, будут нуждаться в совершенствовании методов защиты от мошенников.

Следует также отметить, что проблемы в вопросе защиты от АТМ–мошенничества возникают, кроме прочего, и ввиду высокого уровня образования самих мошенников. В дальнейшей части исследования автором будет проведен анализ характерных черт личности данной категории преступников, который более подробно раскроет данную проблематику.

В целом, в защите от мошенничества постоянно появляющиеся новые виды противоправных действий ведут за собой и эволюцию методов защиты. Приходится признать при этом, что в настоящее время система профилактики и предупреждения преступлений в анализируемой сфере практически отсутствует, а механизмы привлечения правонарушителей к уголовной ответственности недостаточно отработаны и, как следствие, малоэффективны. Все это приводит к выводу о необходимости разработки методологической основы как профилактики, так и противодействия преступлениям корыстной направленности в сфере систем безналичных расчетов.

1.2 Законодательство и опыт зарубежных стран по предупреждению мошенничества, совершаемого с использованием телекоммуникационного и компьютерного оборудования

Существенное изменение условий общественной жизни и стремление россиян следовать принципам, принятым народами развитых стран, требует изучения иностранного опыта, включая возможность заимствования из зарубежного права.

В последние годы отечественные авторы все больше внимания уделяют сравнительно-правовым исследования законодательства, касающегося как имущественных правоотношений в целом, так и соответствующих

преступлений[41]. При этом, однако, недостаточное внимание уделяется мошенничеству, совершаемому с использованием телекоммуникационного и компьютерного оборудования, что обусловлено достаточно «узкой» спецификой рассматриваемого вида противоправных деяний.

Ввиду вышеобозначенной тенденции, в рамках настоящего раздела автором будет проведен анализ наиболее значимых особенностей как зарубежного законодательства, так и отдельных аспектов системы профилактики/пресечения/предотвращения мошенничества, которые функционируют в этих странах.

К перечню рассматриваемых нами стран были отнесены:

Китайская народная республика (далее также – КНР, Китай), занимающая третье место в мире по территории, второе – по номинальному ВВП и первое – по численности населения. Страна является социалистическим государством и одной из старейших цивилизаций в мире. Все это обусловливает интерес автора как к законодательству, так и к системе профилактики и противодействия мошенничеству, совершаемому с использованием телекоммуникационных и компьютерных сетей;

Германия, представляющая особый интерес с точки зрения анализа норм права и опыта профилактики и противодействия мошенничеству, совершаемому с использованием телекоммуникационного и компьютерного оборудования, обусловленный тем фактом, что до недавнего времени темпы роста, равно как и объем ущерба от преступлений рассматриваемого вида в России и Германии были примерно равны;

Великобритания (далее также – Англия) или Соединенное Королевство, полная официальная форма – Соединенное Королевство Великобритании и Северной Ирландии) – островное государство на северо–западе от континентальной Европы. Как было обозначено в предыдущей части настоящего исследования, данная страна – лидер по показателю темпов роста рассматриваемого нами вида мошенничества, что обуславливает объективную необхо-

[41] Малиновский А.А. Сравнительное правоведение в сфере уголовного права. М.: Юристъ, 2002. С. 4.

димость анализа как законодательства этой страны, так и системы профилактики и противодействия мошенничеству, сформированной на ее территории;

Азербайджанская Республика (далее также – Азербайджан) – многонациональная и многоконфессиональная страна. Большинство населения республики исповедует ислам (преимущественно шиитского толка), меньшинство христианство и иудаизм. По показателям населения (более 9 млн чел. на январь 2013 года) и территории (86 600 км²) Азербайджан является крупнейшей страной Закавказья. Все это делает указанную страну интересной для настоящего исследования как с точки зрения государства, совмещающего в себе традиции исламского законодательства с более классической системой права, так и с позиции рассмотрения опыта крупнейшей страны Южного Кавказа;

Республика Казахстан (далее также – Казахстан) – государство в центре Евразии, большая часть которого относится к Азии, меньшая – к Европе. Население – 18 117 641 человек. Данная страна выбрана автором ввиду ее значительной социально–экономической схожести с Российской Федерацией. Взаимозависимость экономик Казахстана и России проявляется как в периоды спада, так при росте экономик наших стран. Так после апреля 1999 года экономический рост в обрабатывающих отраслях промышленности Казахстана в определенной, и немалой, степени был связан с экономическим подъемом в России и увеличением объемов казахстанского экспорта в эту страну. Социально–экономические преобразования, происходящие в нашей стране до сих пор, находят свое отражение и в социально–экономической жизни Казахстана.

Выбор стран определен их географической природой, разницей в уровне социально–экономического развития и характерными особенностями менталитета, находящими свое отражение как в нормативно–правовом аспекте, так и в рамках реализации инициатив гражданского общества.

В первую очередь необходимо выделить тот факт, что зачастую зару-

бежным законодательством устанавливаются единые стандарты в вопросе охраны государственной и частной собственности от мошенничества. Исключение составляют лишь небольшое количество стран с «социалистическим» подходом[42]. Необходимо отметить, что нормы права выступают в данном случае как отражение менталитета населения страны. В некоторой степени данная особенность права позволяет сказать о высоком уровне личной ответственности граждан и нетерпимости к преступной деятельности.

Детализация мошенничества, проведенная законодателем в уголовном праве КНР представляется необычной в контексте отечественной уголовно-правовой науки, поскольку мошенничество как раз подразделяется на преступления «против собственности» и «против экономического порядка». В первом случае это ст.ст. 266,269 УК КНР – «мошенничество с общественными, частными ценностями на значительную сумму», во втором – ст.ст. 192-197 УК КНР в соответствии с которыми нет конкретного пострадавшего, а ущерб наносится именно экономическим отношениям внутри государства (подделка банкнот и т.п.)

Так, рассмотрим мошенничество с банковскими картами и АТМ-терминалами.

Согласно данным статистики международных организаций, за период 2006–2011 годов жертвами мошенников с кредитными картами стали 43% жителей Китая[43], с активным ростом в период 2009–2010 годов. За период 2011–2014 годов рост данного направления преступных посягательств прекратился, однако, можно говорить лишь о стабилизации проблемы, но не о ее решении (рисунок 5).

---

[42] Сунчалиева, Л. Э. Мошенничество (Уголовно-правовой и криминологический аспект) : дис. ... канд. юрид. наук. – Ставрополь, 2004. – 187 с.

[43] Кредитно–карточное мошенничество растет и процветает // Бизнес&Балтия. 2011. [Электронный ресурс] // Режим доступа: http://bb.lv/bb/all/2857/

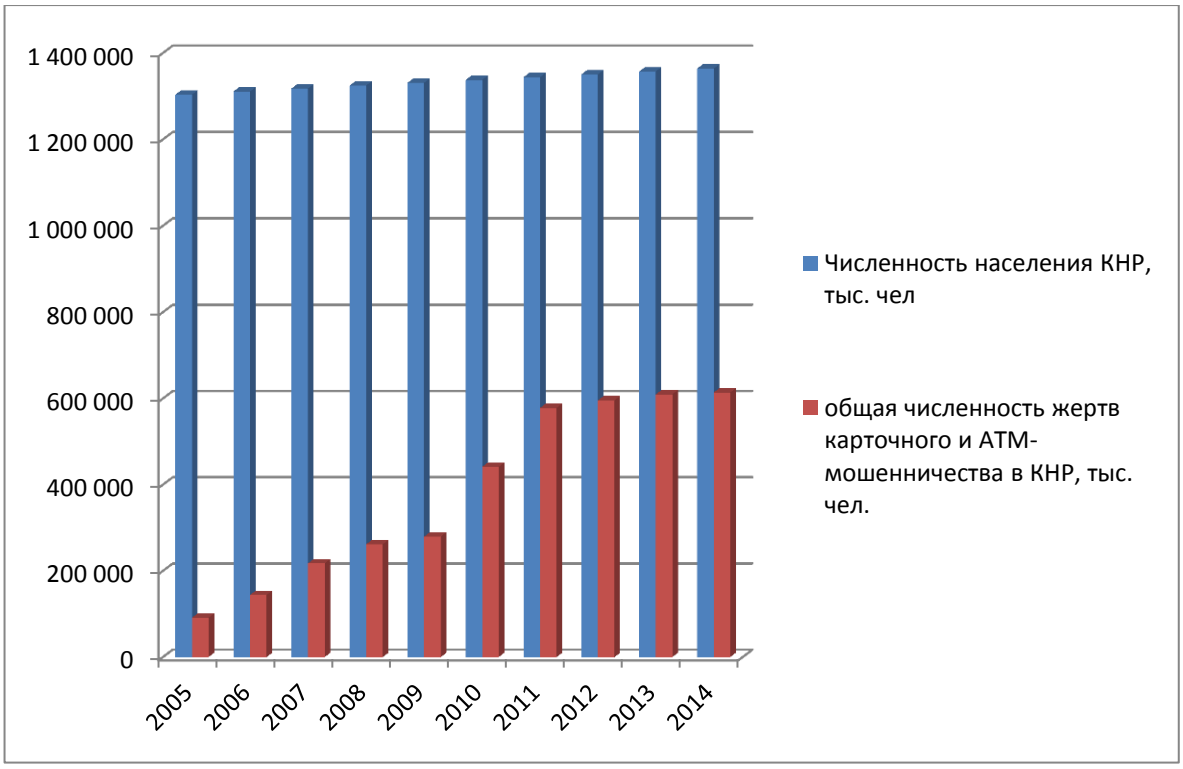


Рисунок 5 – Темпы роста карточного и АТМ–мошенничества в КНР в 2005–2014 годах[44]

Учитывая, что в период 2012–2015 годов в КНР был зафиксирован рост числа банкоматов с возможностью работы по чиповой технологии, то стабилизация роста карточного и АТМ–мошенничества объясняется технологическим совершенствованием АТМ. В данном случае наиболее примечательно, что чипы, используемые совместно с ПИН–кодами, могут генерировать динамичные данные, позволяющие осуществлять уникальную одноразовую аутентификацию отдельной трансакции (EMV–стандарт).

Применение новой (для рынка КНР) технологии создало продукт, который контрастирует с картами, имеющими только магнитную полосу, которые используют статические данные, используемые только для верификации самой карты. Чип имеет существенно более высокую степень защиты по сравнению с магнитной полосой. Секретный ключ чипа, идентифицирующий карту в банковских операциях, хранится в защищенной па-

[44] Составлено автором на основе статистических показателей, представленных компанией FICO [Электронный ресурс] // Режим доступа: https://www.fico.com/blogs/tag/score–distributions/

мяти, он записывается в память чипа на стадии изготовления, и его невозможно оттуда извлечь с помощью внешних устройств, не нарушая целостности самого чипа.

Вывод о столь благоприятном влиянии внедрения технологии EMV подтверждается и отсутствием существенных изменений в соответствующем разделе законодательства страны, а также отсутствием изменений в пенитенциарной системе и принципах постпенитенциарной работы.

Уголовное законодательство Германии представляется, по мнению ряда авторов, наиболее всеобъемлющим в отношении определения мошенничества. Так, в соответствии с параграфом 263 УК Германии мошенником признается лицо, которое «с намерением доставить себе или третьему лицу противоправную имущественную выгоду причинит ущерб имуществу другого путем введения его в заблуждение или поддержания в нем заблуждения, выдавая ложные факты за истинные, или искажая, или скрывая истинные факты».[45]

Таким образом, в качестве мошенничества законодательством Германии определяется причинение имущественного ущерба с корыстной целью путем обмана.

Квалифицированные виды мошенничества, предусмотренного уголовным законодательством Германии, определяются через субъект преступления. Так, квалифицированным видом признается мошенничество, совершаемое лицом на постоянной основе («в виде промысла») «единолично», либо в составе организованной преступной группы, совершающей деяния на постоянной основе.

Еще один квалифицированный состав определяется через количественные характеристики деяния: причинение имущественного вреда в крупном размере, либо постановкой в опасность причинения имущественного вреда значительного (неопределенного) круга лиц.

---

[45] Уголовный кодекс Германии с изменениями от 28 декабря 2003 года [Электронный ресурс] // Режим доступа: http://lexetius.com/StGB/263a

Среди квалифицированных составов мошенничества в уголовном праве Германии выделяется и такой относительный признак, как постановка потерпевшего в состояние экономической нужды. Отметим, что источники права германии не конкретизируют объем материальных благ, который необходимо считать пороговым значением, оставляя данный аспект на усмотрение суда (сообразно образу и уровню жизни потерпевшего).

Злоупотребление служебным положением и полномочиями также образуем квалифицированный состав мошенничества по рассматриваемому уголовному законодательству.

И последний квалифицированный состав образует страховое мошенничество, при котором происходит фальсификация страхового случая. При этом, законодателем уточнено, что квалифицированный состав образует только поджог (или разрушение, причиненное через поджог), либо потопление (посадка на мель) корабля[46].

Ряд авторов отмечает также[47], что в качестве обмана в уголовном праве Германии понимаются намерения, убеждения, мотивы поведения и иные психические факты мошенника или другого лица.

При этом, согласно § 263 УК Германии, «оценка» фактом не является, так как «оценка имеет свое основание в субъективном и не является объективным познаваемым обстоятельством»[48].

Таким образом, основными особенностями мошенничества германского типа являются:

а) широкое понимание обмана;

б) широкое понимание ущерба;

в) широкое понимание корыстной цели.

В разделе «Мошенничество и преступное злоупотребление довери-

---

[46] Сунчалиева Л. Э. Мошенничество (Уголовно-правовой и криминологический аспект) : дис. ... канд. юрид. наук. – Ставрополь, 2004. – С. 50.
[47] Там же.
[48] Клепицкий И.А. Собственность и имущество в уголовном праве // Государство и право. 1997. № 5. С. 78.

ем» УК Германии содержит еще два состава: утаивание и растрата заработной платы (§ 266a) и злоупотребления с чеками и кредитными картами (§ 266b). Последний состав преступления охватывает частный случай, когда лицо злоупотребляет переданной ему чековой или кредитной картой и этим вынуждает владельца карты произвести оплату.

Следует отметить, что столь подробное изложение в уголовном законе видов мошеннических действий встречается не во всех зарубежных УК.

Рассматривая же практический аспект эффективности уголовного законодательства Германии в вопросах предотвращения и профилактики карточного и АТМ–мошенничества, следует отметить его низкую эффективность.

По данным исследования компании FICO, в 2014 году в Германии значительно увеличилось количество мошенничества с кредитными картами.

Эксперты проанализировали 7,5 млн активных платежных карт, выпущенных в Германии, и пришли к выводу, что в период с сентября 2013 года по сентябрь 2014 года количество случаев мошенничества увеличилось на 17%.

При этом объем покупок с помощью платежных карт за данный период времени увеличился только на 5%, количество попыток мошенничества по картам увеличилось на 30%, а общий объем авторизированных транзакций поднялся на 8%.[49]

Как видно из статистических данных, в настоящее время каждый четвертый гражданин Германии стал жертвой карточных мошенников (рисунок 6).

Исследование специалистов FICO показало, что чаще всего мошенничество происходит с операциями без присутствия карты

[49] Годовой отчет компании FICO – 2016 [Электронный ресурс] // Режим доступа: https://www.fico.com/blogs/fraud–security/what–is–a–cybersecurity–posture/

(cardnotpresenttransaction – CNP). К ним относятся онлайн–платежи и трансграничные платежи.

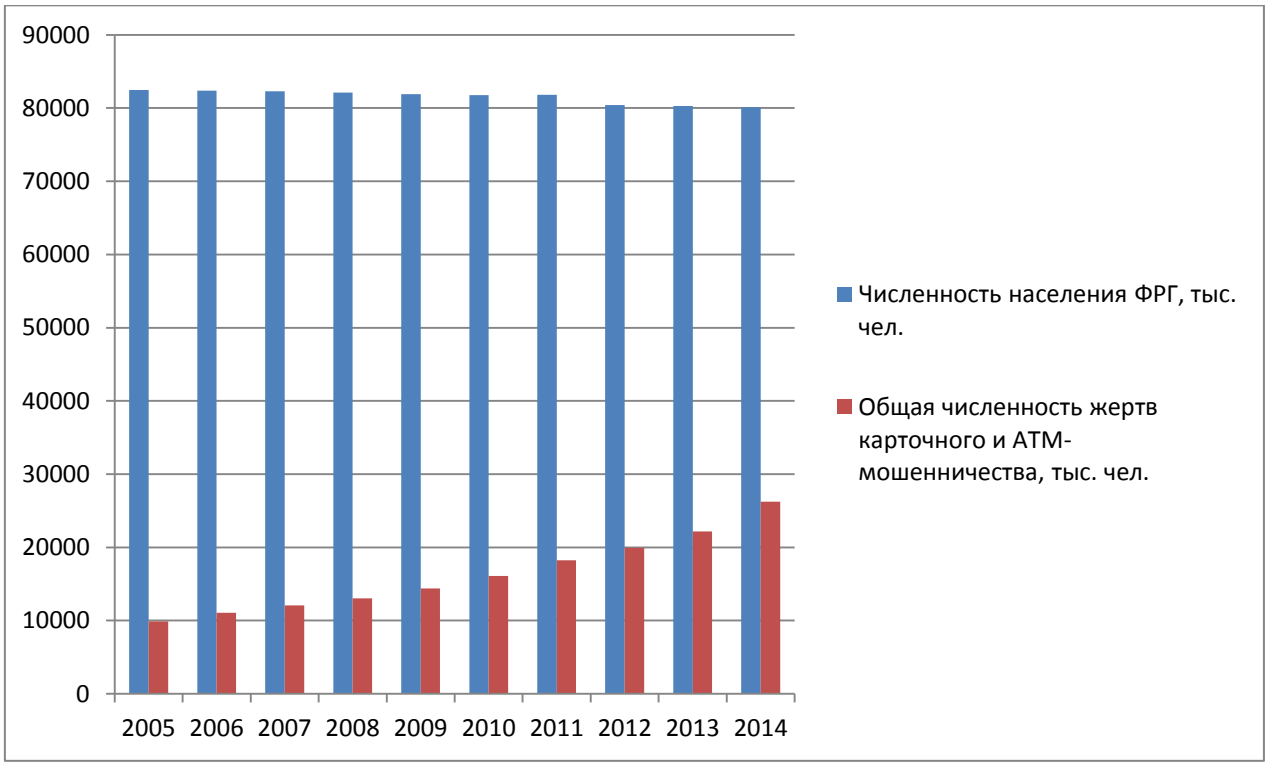


Рисунок 6 – Темпы роста карточного и АТМ–мошенничества в Германии в 2005–2014 годах[50]

Уровень CNP–мошенничества составляет около 70% от всего карточного мошенничества. При этом на трансграничное мошенничество приходится 80%. Стоит отметить, что большинство платежных карт в Германии имеют чип и мошенничество по этим картам составляет всего 10% от общего количества фрода.

По данным исследования, заполучив данные платежных карт, мошенники чаще всего пользовались услугами туроператоров (16,1%), авиакомпаний (4,5%), а также оплачивали номера в гостиницах (3,1%).

Согласно данным компании FICO, около 32% всех платежей с использованием как контактных, так и бесконтактных карт соответствуют

[50] Составлено автором на основе статистических показателей, представленных компанией FICO [Электронный ресурс] // Режим доступа: https://www.fico.com/blogs/tag/score–distributions/

стандарту безопасности EMV, разработанному международными платежными системами[51].

Пример Германии показывает, что внедрение платежных карт с чипом и проведение операций в соответствии со стандартом EMV не решает проблему карточного и АТМ–мошенничества. Аналогично КНР законодательство Германии не претерпело значительных изменений в последние несколько лет. Изменений не было также ни в пенитенциарной системе, ни в принципах постпенитенциарной работы. Следует также отметить высокий уровень социализации граждан в постпенитенциарный период. Однако, как уже было отмечено выше, социальная активность и значительное количество социальных контактов является одной из характерных особенностей преступлений в данной области.

Рассматривая опыт виктимологической работы в Германии, следует отметить, что более 60 лет назад там стала широко практиковаться целенаправленная работа с общественностью, ориентирующая граждан на самозащиту – спецкурсы по виктимологии, консультированию населения и т.д. Кроме того, реализуются как государственные, так и частные инициативы.

Однако, несмотря на достаточно длительный опыт реализации и сформированную систему профилактики виктимологического направления полицейской работы, лишь каждый 18-й житель Германии посещал соответствующие курсы и мероприятия. Подобная статистика говорит о низком уровне личной ответственности со стороны граждан. У населения за длительный период сформировался соответствующий менталитет, в рамках которого личная ответственность индивида, направленная на заботу о безопасности своего имущества и финансов, находится на достаточно низком уровне.

Таким образом, значительный объем социальных гарантий является,

---

[51] Годовой отчет компании FICO – 2016 [Электронный ресурс] // Режим доступа: https://www.fico.com/blogs/fraud–security/what–is–a–cybersecurity–posture/

с одной стороны, показателем высокого уровня социального развития общества и государства, с другой же – фактором формирования у населения низкого уровня личностной ответственности, что, в свою очередь, на практике приводит к постоянному и значительному росту преступлений рассматриваемого вида.

Широкий перечень мошеннических действий предусмотрен и в законодательстве Англии. Мошенничество (fraud) в английском праве представлено в виде единого преступления. Это название объединило несколько самостоятельных преступлений (deceptionoffences). Закон о краже 1968 года предусматривает ответственность за приобретение имущества путем обмана и получение денежной выгоды путем обмана. Закон о краже 1996 года установил ответственность за обман, повлекший совершение финансовых операций на счетах в кредитных организациях.[52]

Великобритания, осуществившая практически полную миграцию на технологию чиповых карт, поддерживающих офлайновую проверку ПИН–кода, стала ярким примером резкого роста мошенничества по транзакциям ЭК, который прогнозировали эксперты, в странах, мигрировавших на чип. По данным за 2005 год, совокупный годовой объем потерь от карточного мошенничества в стране снизился на 13% по сравнению с 2004 годом, а если принимать во внимание все категории фрода, кроме CNP–операций, то потери английских банков от действий преступников уменьшились на 28%. В частности, объем мошенничества по поддельным картам уменьшился на четверть, а по украденным (потерянным) картам – на 22%[53].

Однако в связи с миграцией банковской эмиссии на микропроцессорные карты CNP–фрод становится объектом повышенного интереса со стороны криминальных структур. Рассматривая статистику по данному направлению преступной деятельности, следует отметить, что в Великобритании в 2005 году скорость годового роста CNP–фрода составила 21%,

---

[52] Клепицкий И.А. Собственность и имущество в уголовном праве // Государство и право. 1997. № 5. С. 78.

[53] Годовой отчет компании FICO – 2016 [Электронный ресурс] // Режим доступа: https://www.fico.com/blogs/fraud–security/what–is–a–cybersecurity–posture/

а в абсолютном выражении на этот вид мошенничества пришлось 183,2 млн фунтов стерлингов, что почти в 2 раза превысило потери банков от поддельных карт и более чем в 2 раза – потери от использования украденных (потерянных) карт. В 2006 году тенденция продолжилась, и CNP–фрод вырос на 16% по сравнению с 2005 годом. На него в 2006 году уже приходилась половина всех потерь английских банков по карточным операциям.

По данным APACS, за первую половину 2007 года рост CNP–фрода составил 44% в сравнении с аналогичным периодом 2006 года, достигнув размера 137 млн фунтов стерлингов за шесть месяцев, в общем же 2007 год показал относительный рост общего числа преступлений данной направленности на 69,7%.

Опыт Великобритании примечателен тем, что, в отличие от прочих рассматриваемых нами, позволяет судить о динамике мошенничества в сфере высоких технологий в более длительном хронологическом периоде.

В 2014 году киберпреступность нанесла держателям банковских карт этой страны самый большой ущерб в мире – 534,9 млн евро, такая статистика должна говорить о том, что внедрение новых технологических решений не позволяет в должной мере избежать преступных посягательств. Однако эта цифра на 94,2% состоит из CNP–фрода, то есть практически все потери держателей банковских карт произошли из–за неосмотрительности самих жертв[54].

О низком уровне личной ответственности граждан говорят и другие исследования. Ученые из Университета Кента проанализировали результаты интервью Офиса национальной статистики и пришли к выводу, что количество преступлений в Англии и Уэльсе растет на 50 процентов в год.

---

[54] Годовой отчет компании FICO – 2016 [Электронный ресурс] // Режим доступа: https://www.fico.com/blogs/fraud–security/what–is–a–cybersecurity–posture/

Социологи ONS провели 40 тысяч интервью в различных регионах страны для того, чтобы выяснить опыт людей, которые столкнулись с преступностью. Они выяснили, что 3,8 миллиона случаев мошенничества с банковскими карточками вообще не были учтены. Остались за рамками статистики и карточные мошенники, которые в 2013 году обошлись государству в 450 миллионов фунтов. Таким образом, если включить их в статистику, количество ежегодных преступлений вырастет с 7,3 миллиона до 11 миллионов в год, что является 50–процентным ростом преступлений[55].

Авторы расследования обвинили полицейских в том, что они не включают в статистику, а значит, не ведут борьбу с онлайн–мошенничеством, фиктивными интернет–аукционами, мошенничествами на сайтах онлайн–знакомств.

Если преступники и задерживаются, то несут мягкие наказания, чтобы не портить статистику. Как подчеркнул криминолог из Университета Кента – профессор Марион Фитцджеральд, «министров легко убедить в том, что нынешняя статистика преступности являет собой «золотой стандарт», это происходит с тех пор, как лейбористы стали показывать статистику непрерывного падения преступности начиная с их прихода к власти в 1997 году, однако мы приводим свои собственные результаты, свидетельствующие о том, что преступления на 50 процентов выше, чем утверждает официальная статистика». По словам Питера Кутбертсона из Центра по предупреждению преступности, «общественное доверие к статистике преступлений является жизненно важным и требует подсчета полного спектра преступлений. Это издевательство, когда авторитетный опрос выявил, что каждое третье преступление остается за рамками статистики»[56].

В Великобритании разработаны программы виктимологической

---

[55] Исследование Офиса национальной статистики [Электронный ресурс] // Режим доступа: https://www.kent.ac.uk/news/tags/comment/

[56] Интервью Питера Кутбертсона [Электронный ресурс] // Режим доступа: achievementsnews.co.uk/archives/2999

профилактики основаны на привлечении граждан в гражданские патрули, добровольнические отряды и иные организационные структуры, деятельность которых направлена на включение населения в обеспечение собственной безопасности.

Значимым отличием от Германии является наличие во всех учебных заведениях – от начальной школы до вузов – занятий по прикладной виктимологии, которые являются обязательными. Следует отметить, что кроме лекционных занятий желающие могут пройти специальный практический курс, позволяющий освоить приемы самозащиты и выработать навыки эффективного поведения в экстремальных ситуациях.

Таким образом, примеры европейских государств показывают, что одно лишь внедрение технологических решений является недостаточным. Требуется также проведение виктимологической профилактики, что означает плотную работу с населением.

Основополагающими принципами международного права в части виктимологической ориентации являются, во–первых, ответственность государства перед потерпевшими, создание всех условий для защиты их прав и интересов, не нарушая при этом права правонарушителя, а также создание системы и механизмов, направленных на снижение уровня виктимности общества в целом и отдельных социальных групп и граждан.

Рассматривая систему виктимологической профилактики в зарубежных странах, К. В. Вишневецкий справедливо предложил разделить ее составные элементы на три группы: [57]

– нейтрализация объективных условий виктимизации личности или социальной группы;

– разъяснительная работа среди отдельных категорий населения, виктимологическая пропаганда;

[57] Вишневецкий К.В. Зарубежный опыт виктимологической профилактики преступлений и перспективы ее развития в России // Современное право. 2008. № 2. С. 117.

– оказание помощи жертвам, включая систему государственных компенсаций и возмещения ущерба.

В большинстве высокоразвитых стран виктимологическая профилактика выступает в качестве специфической составной части деятельности государства и институтов гражданского общества, направленной на предотвращение преступной деятельности, что обосновывается фактом того, что поведение жертвы в современных криминологических концепциях трактуется как важный элемент в системе детерминации преступления.

Государство и органы государственного и муниципального управления выступают основным субъектом предупредительной деятельности в рамках первой выше обозначенной группы.

По мнению западных виктимологов, общество в лице органов самоуправления обладает мощным потенциалом социального регулирования, способным нейтрализовать виктимизирующее воздействие со стороны процессов урбанизации. Именно общественное самоуправление может выступить выражением принципиальной культурной разнородности, существующей как в мировом масштабе, так и на региональном и локальном уровнях. Оно представляется наиболее демократичным ответом на вызовы глобализации, заявляющим о необходимости уважения к частному. Кроме того, общественное самоуправление способно смягчить негативные последствия радикализации стратификационных процессов, и прежде всего те, которые связаны с локальным сосредоточением и концентрацией в неблагополучных районах городов представителей маргинальных слоев населения[58].

Кроме того, рассматривая зарубежный опыт, следует также отметить некоторые особенности стран ближнего зарубежья. Так, например, в УК

[58] Там же.

Азербайджанской Республики содержится глава 13 «Киберпреступления», в соответствии с нормами которой криминализированы следующие деяния:[59]

– Неправомерный доступ к компьютерной системе (ст. 271), то есть преднамеренный вход в компьютерную систему без права доступа либо с нарушением мер защиты. К данной статье отнесено и использование так называемых «Личных кабинетов» пользователей, данные от которых нередко стараются получить мошенники для последующего свободного распоряжения денежными средствами потерпевших.

– Неправомерное завладение компьютерной информацией (ст. 272). В соответствии с указанной статьей криминализировано завладение компьютерной информацией, не предназначенной для публичного пользования. Сюда же возможно отнести и неправомерное получение данных платежных карт (при использовании скиммингового оборудования).

– Неправомерное вмешательство в компьютерную систему или компьютерную информацию (ст. 273). Статья закрепляет ответственность за неправомерное повреждение, уничтожение, порчу или изменение компьютерной информации.

– Оборот средств, изготовленных для совершения киберпреступлений (ст. 273–1). Статья устанавливает ответственность за производство устройств или компьютерных программ, с целью совершения предусмотренных статьями 271–273 преступлений. Сюда также относится использование вредоносного ПО и специальных устройств. Примером также может служить скимминговое оборудование и ПО, включая так называемые «кейшарки», служащие для «запоминания» нажатых клавиш на клавиатуре.

Фальсификация компьютерных данных (ст. 273–2), то есть несанкционированное преднамеренное введение, изменение, уничтожение или блокирование компьютерных данных с целью выдачи фальсифицированных дан-

[59] Харламов Д. Д. Критерии криминализации новых видов мошенничества в УК РФ // АВБсП. 2016. № 1. – С. 44–46.

ных за аутентичные. К данной категории в большей степени относятся «фишинговые» сайты.

Таким образом, выделяя данные статьи в отдельную главу, законодатель охватил значительное количество преступлений, включая как взломы компьютерных сетей и незаконное использование данных «изнутри», так и мошенничество с применением высоких технологий.

Отдельно следует отметить правовые системы Республики Казахстан. Уголовный кодекс Республики Казахстан содержит две статьи, регламентирующие ответственность за совершение преступлений с использованием компьютерных технологий:

– Неправомерный доступ к информации, в информационную систему или сеть телекоммуникаций (ст. 205).

– Нарушение работы информационной системы или сетей телекоммуникаций (ст. 207).

При этом указанные статьи не выделены в отдельную главу, а размещаются в главе 7 кодекса «Уголовные правонарушения в сфере информатизации и связи».

Рассмотрим более подробно положения указанных статей.

«Статья 205. Неправомерный доступ к информации, в информационную систему или сеть телекоммуникаций

1. Умышленный неправомерный доступ к охраняемой законом информации, содержащейся на электронном носителе, в информационную систему или сеть телекоммуникаций, повлекший существенное нарушение прав и законных интересов граждан или организаций либо охраняемых законом интересов общества или государства, –

наказывается штрафом в размере до ста шестидесяти месячных расчетных показателей либо исправительными работами в том же размере, либо привлечением к общественным работам на срок до ста шестидесяти часов, либо арестом на срок до сорока суток, с лишением права занимать опреде-

ленные должности или заниматься определенной деятельностью на срок до двух лет или без такового.

2. То же деяние, совершенное в отношении критически важных объектов информационно–коммуникационной инфраструктуры, –

наказывается штрафом в размере до двухсот месячных расчетных показателей либо исправительными работами в том же размере, либо привлечением к общественным работам на срок до двухсот часов, либо арестом на срок до пятидесяти суток, с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до двух лет или без такового.

3. Деяния, предусмотренные частями первой или второй настоящей статьи, повлекшие по неосторожности тяжкие последствия, –

наказываются штрафом в размере до двух тысяч месячных расчетных показателей либо исправительными работами в том же размере, либо привлечением к общественным работам на срок до шестисот часов, либо ограничением свободы на срок до двух лет, либо лишением свободы на тот же срок, с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до трех лет или без такового.»

Следует выделить положение о лишении права занимать определенные должности или заниматься определенной деятельностью, поскольку в настоящее время для практики Российской Федерации подобный подход является необходимым, хоть и отсутствующим в правоприменительной практике.

Анализ отдельных примеров зарубежного опыта в части построения систем виктимологической профилактики преступлений и соответствующих мер (мероприятий) показывает, что основным элементом подобных систем выступают, в первую очередь, общественные организации. Разумеется, цель деятельности таких организаций достаточно специфична и формулируется, чаще всего, как «защита интересов жертв преступлений». Деятельность же сводится непосредственно к снижению рецидивной виктимизации, оказанию психологической помощи, проведению юридических

консультаций по соответствующим вопросам и т.д. Как справедливо утверждает Н.В. Ревина «именно участие общественности в предупреждении преступлений составляет одну из главных виктимологических идей».[60]

Отметим, что эффективность таких структур зависит в значительной степени от сложившейся в стране системы правосознания и правопонимания.

Так, в Германии законодательно закреплено право представителей общественных организаций на участие в заседаниях соответствующих комитетов и комиссий органов государственной власти и местного самоуправления, отраслевых ведомств; определены права и обязанности по вопросам взаимодействия со средствами массовой информации; и тому подобное.

Ряд отечественных криминологов[61] в ходе анализа деятельности организаций, целью которых является виктимологическая профилактика, обращает внимание на четыре структурных элемента, которые предопределяют эффективность рассматриваемой деятельности:

– особенности организационной структуры;

– взаимодействие и взаимоотношения со смежными организациями;

– объект предоставляемой помощи (поддержки);

– приоритетные направления деятельности организации (условная «специализация» организации на помощи жертвам того или иного вида преступлений).

Характеризуя особенности организационной структуры, подразумевается непосредственно подчиненность организации (добровольная неправительственная/созданная с участием и (или) по инициативе предста-

[60] Ревина Н.В., Ростокинский А.В. Опыт зарубежных стран в развитии виктимологической профилактики мошенничества // Бизнес в законе. 2010. № 1. С. 164.

[61] См., например: Вишневецкий К.В. Место виктимологической теории в криминологии // Наука и практика. 2011. № 3(48).; Зыков Д.А. Виктимологические аспекты предупреждения компьютерного мошенничества: дис. ... канд. юрид. наук. – Владимир, 2002.

вителей властных структур). Следует отметить, что подавляющее большинство организаций и соответствующих программ виктимологической профилактики и помощи жертвам преступлений различного вида в западных странах создано и финансируется неправительственными организациями и агентствами, которые в свою очередь являются операторами грантовых средств. Однако, существуют и исключения.

Так, в Бельгии, Германии и Испании преобладают организации, напрямую финансируемые из средств государственного бюджета, а также созданные государством[62]. На примере опыта Германии нами уже был сделан вывод о негативных аспектах данной особенности системы виктимологической профилактики.

Отметим, что конструктивные отношения с полицией во всех странах трактуются как ключевое условие оказания эффективной помощи жертве преступления.

Подводя итог сравнительно–правовому анализу норм об ответственности за мошенничество по законодательству зарубежных стран, необходимо отметить следующие основные выводы:

1. Мошенничество относится к числу достаточно распространенных посягательств на имущественные отношения, о чем свидетельствует детальная регламентация ответственности за данное преступление в законодательстве практически всех зарубежных стран.

2. В законодательстве многих зарубежных стран присутствует развернутая система специальных предписаний, касающихся не только лишь мошенничества в его общей форме, но и отдельно квалифицирующая мошенничество в таких сферах, как страхование; финансовые рынки; кредитование; обращение товаров и услуг, а также фальсификация предметов, представляющих историческую и иную ценность.

3. В значительной степени перспективной представляется рецеп-

[62] Вишневецкий К.В. Криминогенная виктимизация социальных групп в современном обществе: монография. М.: ЮНИТИ–ДАНА, 2010. 295 с.

ция отдельных положений зарубежного законодательства, среди которых, в частности, уголовно–правовые нормы и положения:

– о необходимости возбуждения уголовного преследования за так называемое «мелкое мошенничество» по первичной жалобе потерпевшего;

– касающиеся вопросов обособления норм, связанных с «компьютерным мошенничеством» в системе уголовного права;

– о дифференциации ответственности за мошенничество, совершая которое преступник использует легальные процедуры в качестве фактора, ослабляющего бдительность жертвы, подрывая при этом авторитет и доверие к соответствующим органам, службам и организациям у граждан.

Кроме того, проведенный анализ позволяет говорить о наличии признаков рецепции отдельных положений зарубежного законодательства в условиях современной социально-экономической действительности нашей страны, а также показывает необходимость создания эффективной системы виктимологической профилактики.

2 ХАРАКТЕРИСТИКА ЛИЧНОСТИ ПРЕСТУПНИКА И ЛИЧНОСТИ ПОТЕРПЕВШЕГО В РАМКАХ МОШЕННИЧЕСТВА, СОВЕРШАЕМОГО С ИСПОЛЬЗОВАНИЕМ ТЕЛЕКОММУНИКАЦИОННОГО И КОМПЬЮТЕРНОГО ОБОРУДОВАНИЯ

2.1 «Портрет» личности преступника, совершившего мошенничество с использованием телекоммуникационного и компьютерного оборудования

Изучение личности преступника считается одним из самых сложных аспектов криминологии. Достижение целей предупреждения отдельных видов преступлений, и в частности хищений с использованием служебного положения, возможно только при внимательном, тщательном изучении личности преступника учеными и правоприменителями. Личность занимает ведущую позицию в механизме противоправного поведения, именно она признается первопричиной совершения преступления, подталкивающей на него. Обладая определенными особенностями, она формирует предрасположенность к нарушению уголовного закона. «Именно на корректировку особенностей личности должен быть направлен основной и сконцентрированный удар предупредительного воздействия»[63].

В рамках криминологии личность исследуется через ее преступное поведение с целью выяснения ее социально–психологических свойств, определения причин, сформировавших антиобщественные установки в сознании обвиняемого. Эти характеристики многочисленны и разнообразны по своему содержанию (физические, психические, моральные, социальные и т. д.), поскольку «любое преступление определяется в итоге всей предшествующей жизнью преступника, теми его личностными чертами и каче-

[63] Кравцов И.А. К вопросу о социально–демографических признаках личности преступника, совершающего хищение чужого имущества с использованием служебного положения, на территории Центрально–Черноземного региона // Вестник ВИ МВД России. 2011. № 3. С. 99.

ствами, которые сформированы в процессе воспитания и которые в конкретной, порой весьма сложной или конфликтной ситуации и предопределяют выбор общественно опасного варианта поведения»[64]. Само это поведение есть «не что иное, как реализация вовне (объективизация) определенных сторон, свойств внутреннего мира данной личности»[65].

Таким образом, личность как сложное социальное явление предполагает многоаспектный анализ своей сущности. Проблема личности преступника всегда имела существенное научное и практическое значение, поскольку без изучения личности тех, кто совершает преступления, невозможно эффективно бороться с преступностью.

Успешное предупреждение преступлений возможно лишь в том случае, если внимание будет сконцентрировано на личности преступника, поскольку именно личность - носитель причин их совершения. Личность преступника - основное и важнейшее звено всего механизма преступного поведения. Те её особенности, которые порождают такое поведение, должны быть непосредственным объектом предупредительного воздействия. Поэтому проблема личности преступника относится к числу ведущих и вместе с тем наиболее сложных проблем криминологии.

Ученые вкладывают разное содержание в понятие личности преступника. К примеру, Г. А. Аванесов считает, что «личность преступника определяется как личность человека, виновно совершившего общественно опасное деяние, запрещенное законом под угрозой уголовной ответственности».

П.С. Дагель, раскрывает личность преступника в уголовно-правовом смысле, указывал, что «это совокупность социально политических, психических и физических признаков лица, совершившего преступление, имеющая уголовно-правовое значение»[66].

---

[64] Орлова Ю.Р., Гусева О.Н. Криминологические особенности личности несовершеннолетних женского пола, совершивших корыстно–насильственные преступления // Юридическая психология. 2008. № 4. С. 19–23.

[65] Мерзлов Ю.А. Криминологический портрет лиц, совершающих преступления в сфере компьютерной информации // Правопорядок: история, теория, практика. 2015. № 4(7). С. 56–61.

[66] Дагель П.С. Учение о личности преступника в советском уголовном праве. – Владивосток: Изд-во Дальневост. ун-та, 1970. – 132 с.

Ю.М. Антонян определяет личность преступника как «совокупность психологических социально значимых негативных свойств психики человека, развившихся в процессе многообразных и систематических взаимодействий с другими людьми»[67].

Авторы проявляют различные подходы к определению сути понятия «личность преступника», наделяя её различными признаками и свойствами, с целью отличия от законопослушной личности.

В работах ряда отечественных ученых сделан вывод, что характер и нравственное формирование личности играют главную роль в генезисе преступного поведения. Не биологические свойства человека, не кратковременное, в том числе и случайное, воздействие внешней ситуации, а весь жизненный путь индивидуума в конечном счете определяет содержание подавляющего большинства его поступков[68].

Традиционный криминологический анализ личности преступника предполагает условное выделение в ее структуре трех подсистем:[69]

1. Социальный статус личности, определяющийся принадлежностью лица к тому или иному классу (социальному слою) и группе с социально–демографической характеристикой (пол, возраст, образование, семейное и должностное положение, национальная и профессиональная принадлежность, уровень материальной обеспеченности и т. д.);

2. Социальные функции (роли) личности, включающие совокупность видов деятельности лица как гражданина в системе общественных отношений (степень умственного развития, культурно–образовательный уровень, знания, навыки, умения);

3. Нравственно–психологические свойства (нравственные качества, ценностные ориентации и стремления личности, ее социальные позиции и интересы, потребности, наклонности, привычки).

---

[67] Антонян Ю.М. Личность преступника. Криминология: учебник / под ред. В.Н. Кудрявцева, В.Е. Эминова. 4-е изд., перераб. и доп. М.: Норма, 2009.

[68] Кудрявцев В.Н. Причинность в криминологии (О структуре индивидуального преступного поведения). М.: Изд–во «Юрид. лит.», 1968. С. 22–23.

[69] Алексеев А.И. Криминология: Курс лекций. М.: Щит–М, 1999. С. 123.

Компоненты этой системы находятся в тесных взаимоотношениях и взаимозависимостях, благодаря чему мы имеем дело «со сложной совокупностью элементов, образующих структуру личности преступника»[70].

Криминологический портрет лиц, совершивших мошеннические действия, как в общем, так и в частности, может быть составлен на основе четырех групп признаков: [71]

– социально–демографические, к числу которых относятся: пол, возраст, уровень образования, занятость и др.;

– социально–ролевые: гражданство, профессия, семейное положение;

– уголовно–правовые, к ним относятся: особый служебный статус, обусловливающий совершение мошенничества, наличие судимости;

– нравственно–психологические качества, характеризующие мотивационный фон преступного поведения.

Рассмотрим данные признаки в динамике за период 2001–2016 годов. Для этого автор использует вторичный анализ данных исследований 2001 и 2006 годов[72], а также данные, полученные в результате собственных исследований[73] в начале 2016 года.

При этом необходимо отметить тот факт, что столь значительный разрыв в хронологическом ряду объясняется недостаточностью проводимых отечественными авторами исследований личности преступника в рассматриваемом направлении незаконной деятельности. Наиболее близкими к настоящему исследованию личности преступников являются материалы исследований[74], проводимых именно в 2001 и

---

[70] Частная криминология: учебник / отв. ред. Д.А. Шестаков. СПб.: Юрид. центр Пресс, 2007. 771 с.

[71] Игошев К.Е. О некоторых чертах личности преступника молодежного возраста и возможностях их использования при разработке типологий // Типология личности преступника и индивидуальное предупреждение преступлений. 1979. С. 80.

[72] Дремлюга Р.И. Интернет–преступность. – Владивосток: изд–во Дальневосточного университета, 2008. 240 с.

[73] Материалы получены в ходе осуществления профессиональной деятельности автора в качестве заместителя начальника УМВД России по г. Хабаровску – начальника следственного управления.

[74] Дремлюга Р.И. Интернет–преступность. – Владивосток: изд–во Дальневосточного университета, 2008. 240 с.

2006 годах, что и стало причиной анализа личности мошенника, совершающего преступление с использованием телекоммуникационного и компьютерного оборудования в столь значительном хронологическом разрыве.

Следует при этом отметить также, что в рамках отдельных исследований рассматривались схожие типы личности преступников[75], однако применить эти материалы в рамках настоящего исследования невозможно ввиду значительных различий между рассматриваемым типом преступления и иными видами мошенничества.

В основе социально–демографической характеристики личности мошенника лежат его пол, возраст, социальное положение и др. Взятые в совокупности, они указывают на наличие определенных отклонений в системе социализации мошенников и служат информационной основой для общесоциальной и специально–криминологической профилактики хищений[76].

Пол. По данным изученных автором материалов[77], большинство преступлений против собственности, в том числе и мошенничество, совершается мужчинами (рисунок 7). Однако, рассматривая статистические данные в динамике, следует отметить повышение (хоть и незначительное) относительной доли женщин.

Результаты статистических исследований 2001 и 2006 годов были практически неизменны (мужчины – 98,2% и 97,2%, женщины – 1,8% и 2,8% соответственно)[78], однако соотношение мужчин и женщин в 2016 году составило 91,1% и 8,9% соответственно. Несмотря на то, что относительная численность женщин выросла втрое, разница на 6,1% (прирост в диапазоне 2006–2016 годов) за 10 лет может считаться незначительной.

---

[75] См. например: Теплова Д.О. Криминологические основы противодействия организованному мошенничеству: монография. М.: РГУП, 2017. 220 с.

[76] Дагель, П.С. Учение о личности преступника в советском уголовном праве. Учебное пособие. Владивосток: Изд-во Дальневост. ун-та, 1970. – 132 с.

[77] См. например: Дремлюга Р.И. Интернет–преступность. – Владивосток: изд–во Дальневосточного университета, 2008. 240 с.

[78] Кесареева Т.П. Криминологическая характеристика и предупреждение преступности в Российском сегменте сети Интернет: дис. ... канд. юрид. наук. М., 2002. С. 103; Дремлюга Р.И. Интернет–преступность. – Владивосток: изд–во Дальневосточного университета, 2008. 240 с.

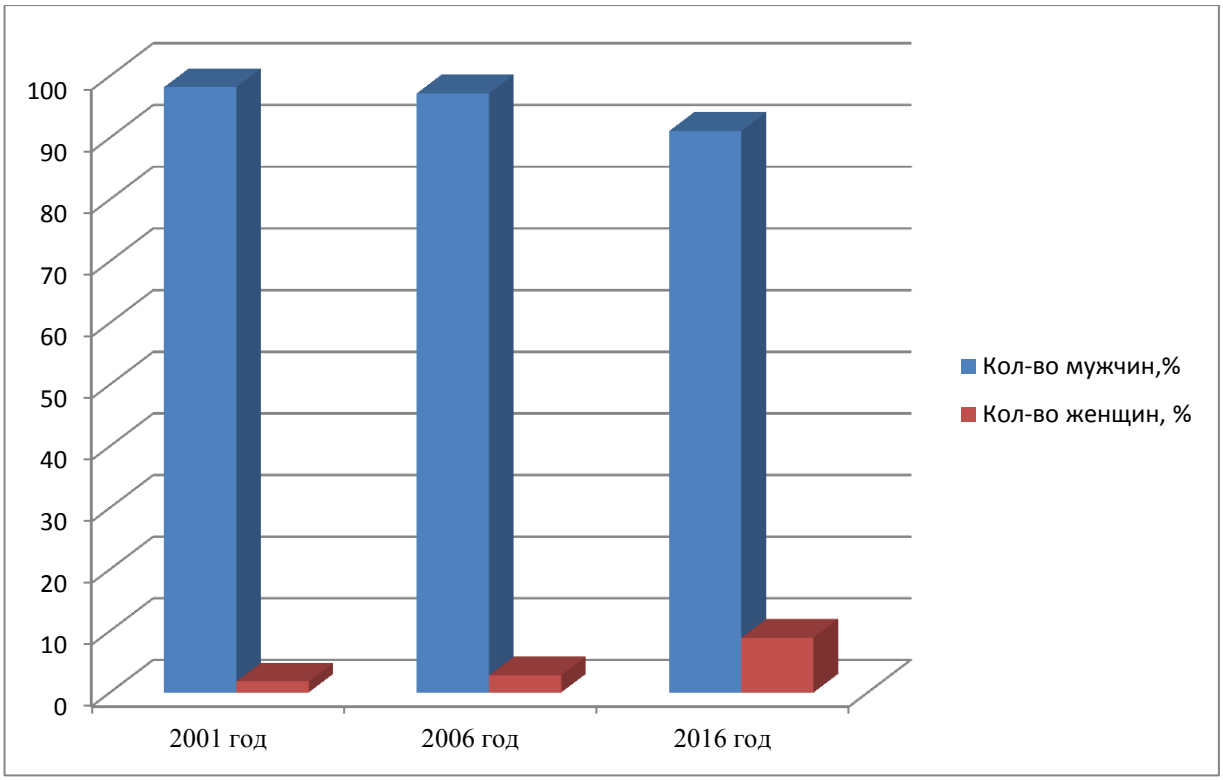


Рисунок 7 – Гендерная динамика лиц, совершивших преступления с использованием телекоммуникационных и компьютерных сетей[79]

Кроме того, анализируя изменение соотношения численности мужчин и женщин в сфере IT (как на соответствующих должностях, так и на соответствующих направлениях подготовки специалистов), следует отметить, что в 2016 году доля женщин составляет около 10%[80], в то время как в 2005 году этот показатель был на отметке 4,1%. Таким образом, можно говорить об определенном уровне корреляции между данными показателями.

Возраст. По данным исследования, проведенного в 2006 году, распределение преступников по возрасту выглядело следующим образом: до 18 лет – 29,9%; от 18 до 24 лет – 60,4%; старше 24 лет – 9,7%. При этом самому младшему было 12 лет, самому старшему – 45. Средний возраст преступника составлял около 20–ти лет.

[79] Составлено автором на основании сравнительного анализа собственных исследований и материалов более ранних работ других авторов (Дремлюга Р.И. Интернет–преступность. – Владивосток: изд–во Дальневосточного университета, 2008. 240 с.)

[80] На основании статьи «Исследование рынка труда и обзора заработных плат. Россия. 2017» (Исследование проведено компанией Антал). [Электронный ресурс] // Режим доступа: https://antalrussia.ru/upload/medialibrary/d54/antal_issledovanie–rynka–truda–i–obzor–zarplat–2018_rus_2.pdf

По сравнению с исследованиями 2001 года доля преступников группы от 18 до 24 практически не изменилась (65,8%), зато процент преступников, не достигших 18 лет, заметно вырос (12,8% в 2001 году)[81].

Динамика преступников по возрастному признаку представлена на рисунке 8.

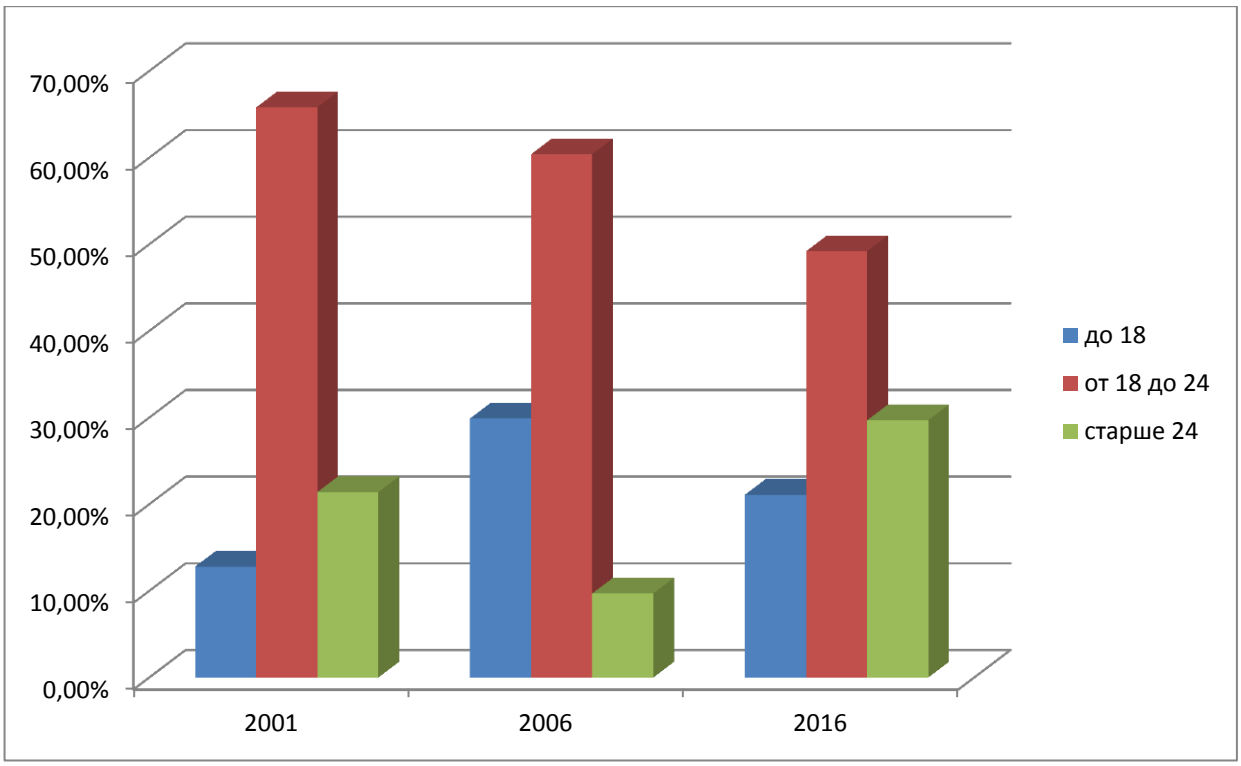


Рисунок 8 – Динамика возраста преступников в период 2001–2016 годов[82].

Рассматривая актуальные данные, следует отметить, что возрастная группа от 18 до 24 лет по–прежнему остается самой многочисленной. Численность же двух оставшихся групп можно условно считать равными. Подобное изменение (в сравнении с данными более ранних исследований), по мнению автора, можно считать закономерным, поскольку минимальный разрыв между исследованиями составляет 10 лет. Сравнивая данные, полученные в 2016 году, с данными 2006 года, можно отметить, что категории «до 18 лет» и «старше 24 лет» различаются на 0,2%. Снижение же относительной

[81] Дремлюга Р. И. Международно–правовое регулирование сотрудничества в сфере борьбы с интернет–преступностью // Библиотека криминалиста. 2013. № 5(10). С. 339–346.

[82] Составлено автором на основании сравнительного анализа собственных исследований и материалов более ранних работ других авторов (Дремлюга Р. И. Интернет–преступность. – Владивосток: изд–во Дальневосточного университета, 2008. 240 с.)

доли лиц от 18 до 24 лет не говорит о сокращении абсолютного значения данной категории. В рамках статистических данных всех периодов следует сделать вывод о том, что данная категория была и остается самой многочисленной.

Объяснение данного факта в действительности весьма простое – в этот возрастной диапазон входят лица, только вступающие в сознательную взрослую жизнь. Это студенты высших и средних специальных учебных заведений и не поступившие на дальнейшее обучение выпускники школ. С точки зрения психологии в современном мире у данной возрастной группы порог социальной ответственности достаточно низок, а понятие «преступление» носит в большей степени романтическую окраску. К тому же уровень собственных доходов у лиц данной возрастной группы зачастую минимален, и если лица, не достигшие 18–летнего возраста и фактически, и психологически находятся в зависимости от уровня доходов своих родителей, то рассматриваемая категория лиц зачастую испытывает психологический дискомфорт, обусловленный как сравнением себя с более успешными сверстниками в рамках внутреннего диалога, так и ввиду фактического отсутствия возможности повышения своего социального статуса за счет улучшения материального благосостояния законными методами.

В исследовании 2006 года был сделан логичный вывод о возможном последующем численном росте категории «до 18 лет» ввиду «увеличения доли подростков в аудитории российского интернета» [83]. Однако, в настоящее время численность данной категории даже несколько ниже показателей 2006 года. Подобное расхождение обусловлено постоянной коммерциализацией российского сегмента сети Интернет. Значительная часть подростков является пользователями различных развлекательных ресурсов (MMORPG, соц. сети и др.), что привело ни к росту уровня знаний молодежи о «технической стороне вопроса», а, напротив, к его снижению. Таким образом, большая часть подростков попросту не обладает достаточным уровнем знаний для со-

[83]Дремлюга Р.И. Интернет–преступность. Владивосток: изд–во Дальневосточного университета, 2008. 240 с.

вершения преступлений в рассматриваемой сфере. Кроме того, зависимость данной категории лиц от дохода родителей позволяет говорить о снижении мотивации к противоправным действиям ввиду целого ряда факторов, таких как: рост доходов населения, снижение уровня социальной напряженности (по сравнению с 2001 и 2006 годами) и т. п.

Отсутствие роста доли несовершеннолетних объясняется также сложностью мошеннического способа хищения. Также, при определенных способах совершения преступления злоумышленник «может достигнуть «успеха» лишь при наличии определенного доверия к нему со стороны потерпевшего»[84]. Подростку труднее завоевать такое доверие, когда речь идет об имущественных интересах.

Образование. Совершающий деяние данного вида преступник всегда технически подготовлен и обладает комплексом программно–аппаратных методов и навыков, позволяющих не просто облегчить, но и обеспечить сам факт совершения преступления.

Также необходимо отметить, что лица, совершающие преступления в сфере мошенничества с использованием современных технологий, обладают более высоким интеллектуальным уровнем, чем преступники в других сферах. В данном случае речь идет не только об образовании в классическом его понимании, но и о стремлении к саморазвитию, которое предопределяет, по сути, процесс выявления в существующих системах (как компьютерных, так и социальных) брешей, позволяющих злоумышленникам улучшить свое материальное положение незаконным путем.

К сожалению, ранее проводимые исследования содержат недостаточно сведений для проведения полноценного анализа изменений данной тенденции, однако, можно утверждать, что данный вид преступлений всегда являлся и является самым «требовательным» к уровню образованности преступника.

---

[84] Теплова Д.О. Криминологическая характеристика и предупреждение организованного мошенничества: дис. ... канд. юрид. наук. М., 2014. С. 248.

В исследовании В.Б. Вехова, проводимом в 2005 году, была представлена следующая градация преступников: «по уровню образования – 40% преступников имели среднее специальное образование, 40% – высшее и 20% – среднее. По уровню интеллектуального развития компьютерных преступников можно охарактеризовать следующим образом: 77% имеют средний уровень интеллектуального развития, 21% – выше среднего и только 2% – ниже среднего»[85].

Полученная нами в ходе статистического анализа, проведенного автором в период 2014–2017 годов,[86] общая картина распределения преступников по уровню образования имела следующий вид: 34% – среднее образование, 27% – среднее специальное образование (из них 72% – образование в сфере информатики и инфокоммуникаций), 39% – высшее образование (из них высшее техническое образование – 37%, экономические специальности – 52%).

Такое статистическое распределение убедительно опровергает распространенное мнение о том, что совершить преступление с использованием компьютерной техники могут только лица, имеющие фундаментальное образование и глубокие знания особенностей функционирования средств компьютерной техники. Как показывает статистика, значительная доля лиц, совершивших рассматриваемые преступления, не имели профильного образования по специальностям технической направленности. Представляется, что данное обстоятельство связано с тем, что нередко для реализации того или иного способа совершения преступления достаточно навыков владения персональным компьютером на уровне пользователя, что в наше время весьма распространено. Навыки работы с компьютером на уровне пользователя приобретаются еще в средней школе, к тому же многим доступны различные

[85] Вехов В.Б. Хакеры, крэкеры, фрикеры, кардеры – кто они? // Информационно–методический журнал «Защита информации. Инсайд». 2005. № 5. С. 67.
[86] Камко А.С. Проблемы и перспективы системы противодействия мошенничеству с использованием телекоммуникационного и компьютерного оборудования // Власть и управление на Дальнем Востоке. 2017. № 4. С. 182–187.

самоучители работы на компьютере, курсы компьютерной грамотности и иные источники знаний.

Диапазон различий по специальным знаниям, умениям и навыкам также весьма широк – от высококвалифицированных специалистов до лиц, обладающих минимально необходимыми познаниями для работы в качестве пользователя ЭВМ.

В целом, проведенное исследование подтвердило известный криминологический тезис о том, что «образование и социальный статус преступника предопределяют сложность и изощренность преступного поведения»[87].

Говоря об интеллектуальном уровне преступников, следует отметить, что в большинстве исследований нами не было найдено данных о конкретных методиках, применявшихся при тестировании, однако везде указывалось на высокий интеллектуальный потенциал.

В рамках настоящего исследования автором была предпринята попытка оценки интеллектуального потенциала лиц, осужденных по соответствующим статьям Уголовного кодекса РФ (рисунок 9).

Исследование проводилось с участием осужденных по соответствующим статьям УК РФ лиц, а также подследственных, давших признательные показания в участии в соответствующих профилю исследования эпизодах преступной деятельности.

[87] Кудрявцев В.Н., Эминов В.Е. Причины преступности в России: криминологический анализ. М.: Юристъ, 2006. С. 71.

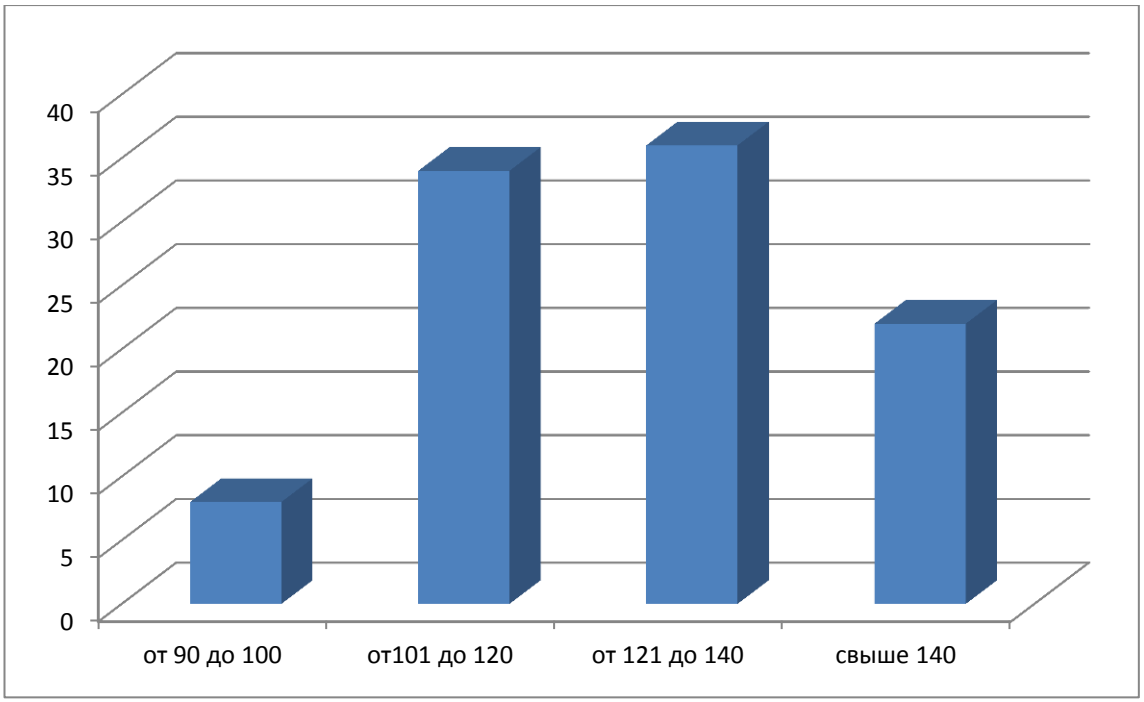


Рисунок 9 – Показатели уровня интеллекта лиц, совершивших мошенничество с использованием телекоммуникационного и компьютерного оборудования, %[88]

В качестве метода тестирования автором применялся тест Айзенка – тест коэффициента интеллекта (IQ), разработанный английским психологом Гансом Айзенком. Тесты интеллекта предназначены для оценки интеллектуальных способностей для людей в возрасте от 18 до 50 лет, имеющих образование не ниже среднего. Коэффициент интеллекта (англ. IQ – intelligence quotient) – количественная оценка уровня интеллекта человека: уровень интеллекта относительно уровня интеллекта среднестатистического человека такого же возраста. Определяется с помощью специальных тестов. Тесты IQ рассчитаны на оценку мыслительных способностей, а не уровня знаний (эрудированности). Коэффициент интеллекта является попыткой оценки фактора общего интеллекта.

[88] Материалы получены в ходе осуществления профессиональной деятельности автора в качестве заместителя начальника УМВД России по г. Хабаровску – начальника следственного управления.

На уровень IQ влияет несколько факторов, в том числе наследственность, окружающая среда (семья, школа, социальный статус человека). Также значительно влияет на результат прохождения теста возраст испытуемого. В 26 лет, как правило, интеллект человека достигает своего пика, а потом только снижается[89].

Тесты IQ разрабатываются так, чтобы результаты описывались нормальным распределением со средним значением IQ, равным 100, и таким разбросом, чтобы 50% людей имели IQ между 90 и 110 и по 25% – ниже 110 и выше 120. Значение IQ менее 70 обычно квалифицируется как умственная отсталость. Представленные результаты тестов подтверждают, что большая часть преступников в рассматриваемой сфере имеет показатели интеллекта выше среднего. Минимальным показателем стали 94 балла. В целом, лишь 8% опрошенных имели показатели ниже 100 баллов, 62% опрошенных относятся к категории со средним показателем (до 135) и 30% показали результаты выше среднего, из них 22% в категории свыше 140.

В данном случае следует отдельно пояснить, что обозначает каждый из представленных диапазонов.

Уровень IQ выше 140. Люди с показателями IQ свыше 140 – это обладатели отличных творческих способностей, которые достигли успехов в разных научных отраслях. Среди известных личностей с результатом теста интеллектуальных способностей от 140 – Билл Гейтс и Стивен Хокинг. Такие гении своей эпохи известны своими выдающимися способностями, они вносят неимоверно высокий вклад в развитие знаний и науки, создают новые изобретения и теории. Таких людей всего 0,2% от всего населения.

Уровень IQ от 131 до 140. Высокие показатели IQ есть только у трех процентов населения. Это успешные люди с высокими умственными способностями, они могут достигать высот в разных сферах деятельности, науке и творчестве.

---

[89] Бельская З.В. Тесты интеллекта в диагностической практике психолога // Актуальные вопросы современной психологии: материалы III Междунар. науч. конф. (г. Челябинск, февраль 2015 г.). Челябинск: Два комсомольца, 2015. С. 77–80.

Уровень IQ от 121 до 130. Интеллектуальный уровень выше среднего показывает всего 6% населения. Таких людей видно в ВУЗах, так как они являются обычно отличниками по всем дисциплинам, успешно заканчивают университеты, реализуют себя в разнообразных профессиях и достигают высоких результатов.

Таким образом, между криминальной специализацией мошенников и уровнем их образования имеется тесная взаимосвязь. Высокий интеллектуальный уровень и хорошая профессиональная подготовка способствуют разработке более сложных и безопасных мошеннических схем. Углубление криминальной специализации обусловливает потребность в привлечении в сферу криминального бизнеса высокообразованных специалистов.

В связи с этим следует особенно выделить тот факт, что значительный уровень интеллектуальных способностей преступников позволяет им не просто находить пробелы в законодательстве для использования в процессе достижения своих противоправных целей, но и формировать значительный объем скрытых от правоохранителей эпизодов преступной деятельности, что фактически является основной причиной высокого уровня латентности данной категории преступлений.

Учитывая высокий уровень социализации данной категории преступников[90], а также способность приспосабливаться к динамично меняющейся системе профилактики и противодействия мошенничеству, совершаемому с использованием телекоммуникационного и компьютерного оборудования, разработанной правоохранительными органами, необходимо сделать вывод о том, что фактическое воздействие на представителей данной категории населения возможно также путем введения определенных мер ограничения их свободы, а при выявлении явной тенденции к противоправному поведению либо совершении преступления в особо крупном размере – путем вынесения запрета на использование определенных технических устройств в

[90]Овчинский В.С. Трамп, ФБР, искусственный интеллект [Электронный ресурс] // Режим доступа: http://zavtra.ru/blogs/tramp_fbr_iskusstvennij_intellekt

определенном хронологическом периоде; запрета заниматься определенными видами деятельности, связанными с настройкой, установкой и эксплуатацией того же перечня технических устройств в том же хронологическом периоде.

Трудовая занятость. Одним из связующих звеньев между отдельной личностью и обществом является трудовая деятельность, в процессе которой человек ощущает на себе воздействие соответствующей социальной среды и сам, в свою очередь, влияет на нее.

Рассматривая данные исследований прошлых лет, мы установили, что постоянное место работы в 2006 году было лишь у 31,3% (33% – по данным исследований 2001 года), лишь у 13,9% из выявленных лиц работа была связана с IT–индустрией. По актуализированным данным, за 2016 год постоянное место работы имели более 60%, случайные заработки имели лишь 8% лиц[91].

Следует отметить, что столь высокий рост показателя трудовой занятости (постоянное место работы) не опровергает идею активной трансформации рассматриваемого вида мошенничества в одну из форм профессиональной преступности. По признанию опрошенных лиц, наличие постоянного места работы предполагает, с их точки зрения, некоторую систему «социальной маскировки»: в понимании мошенника социальная интеграция является показателем отсутствия социальной девиации, что, в свою очередь, должно усыпить бдительность правоохранителей.

Заработная плата на занимаемых должностях не позволяет преступникам вести желаемый образ жизни, что также является одной из причин совершения преступлений.

Преступник из числа сотрудников организации является образцовым служащим, имеющим соответствующее образование, как правило, ранее не совершавшим никаких преступлений. Нередко – это руководители различ-

[91] Дремлюга Р. И. Интернет–преступность. – Владивосток: изд–во Дальневосточного университета, 2008. 240 с.

ного ранга, обладающие распорядительными функциями, но непосредственно не отвечающие за конкретные участки работы с компьютерной информацией.

Семейное положение. Рассматривая статистику семейных отношений, данные о которых были получены автором в ходе самостоятельного исследования в период 2014–2016 годов, следует отметить, что почти треть (32%) лиц, совершавших преступления в рассматриваемой сфере, никогда не имели длительных отношений и не состояли в официальном браке, еще 19% разведены. Из оставшихся 49% большая часть (37%) состоят в официальном браке, остальные имеют постоянных сожителей. Значительная доля лиц (56%) имеют детей.

На рассматриваемый контингент преступников распространяется общий статистический закон: по мере увеличения возраста преступников увеличивается количество лиц, состоящих в браке и имеющих детей. Это говорит о достаточно высоком уровне социализации мошенников и отсутствии таких изолирующих факторов, как жесткие правила воровской субкультуры[92].

Большая часть лиц постоянно проживает в крупных городах, что объясняется, с одной стороны, концентрацией денежных потоков (что приводит к увеличению возможностей для совершения преступлений и одновременно увеличивает их латентность), а с другой – возможностью подбора сообщников и более свободным доступом к техническим средствам, необходимым для совершения такого рода преступлений.

Следует отметить, что в настоящее время отсутствует сколь–нибудь проработанная система классификации лиц, совершающих рассматриваемый вид противоправных деяний.

Одним из наиболее рациональных подходов к данному вопросу является предлагаемая О.М. Сафоновым классификация лиц, совершающих

---

[92] Мерзлов Ю. А. Криминологический портрет лиц, совершающих преступления в сфере компьютерной информации // Правопорядок: история, теория, практика. 2015. № 4(7). С. 56–61.

преступления в сфере компьютерной информации:

а) **«Начинающие».** Возраст данной группы колеблется от 18 до 30 лет. Преобладают лица мужского пола. Образование – техническое: среднее, среднее специальное или высшее (иногда неоконченное). Лица имеют средний достаток, позволяющий им владеть одним или более компьютерными устройствами. Обладают существенными познаниями в области компьютерных технологий, включая языки программирования, а также программно–аппаратных частей компьютерных устройств[93].

Вместе с тем лица, относящиеся к данной группе, не имеют постоянной работы, либо их работа связана с компьютерными технологиями (специалисты компьютерных фирм, администраторы баз данных и т. д.). Их личность характеризует увлечение компьютерными технологиями. Противоправную деятельность они, как правило, начинают, не имея должного понимания о том, что их действия являются преступными.

б) **«Устойчивые».** Средний возраст данной группы – 20–25 лет. Сужение возрастной группы объясняется исключением «начинающих», совершивших несколько эпизодов противоправной деятельности и теряющих дальнейший интерес к данной деятельности.

Преобладает мужской пол, но наблюдается тенденция к проявлению активности женщин: их доля в настоящее время составляет около 5%[94].

Преступники данной категории имеют преимущественно высшее либо неоконченное высшее техническое образование[95]. Обладают средним и выше среднего достатком. Могут себе позволить современные компьютерные устройства, а также дополнительные специальные технические приспособления. Владеют глубокими и системными знаниями в сфере компьютерных технологий, языков программирования, а также программно–

---

[93] Сафонов О. М. Уголовно–правовая оценка использования компьютерных технологий при совершении преступлений: состояние законодательства и правоприменительной практики, перспективы совершенствования : дис. … канд. юрид. наук. М., 2015.
[94] Там же.
[95] Ясенев В.Н. Информационная безопасность в экономических системах. Н. Новгород: Изд–во ННГУ, 2006. С. 58.

аппаратной части компьютерных систем. При совершении преступления осмысленно используют комплексы заранее подготовленных программно–аппаратных инструментов, разработанных самостоятельно или найденных в сети Интернет.

Психологический портрет устойчивого компьютерного преступника представляет лицо уравновешенное, со сформировавшейся системой взглядов и ценностей, но не обладающее высокими амбициями[96].

в) «**Профессиональные».** Лица данной категории относятся к старшей возрастной категории среди прочих – они старше 25 лет. Происходят из семей выше среднего достатка. Имеют высшее техническое образование и обладают высоким уровнем знаний в области компьютерной техники и информационных технологий. Многие из «профессиональных» преступников получают второе высшее образование, преимущественно по юридическим или экономическим специальностям[97]. Лица, относящиеся к данной группе, обладают навыками программирования на нескольких языках, глубокими знаниями в области программных средств и устройства аппаратной части компьютерных систем (как персональных компьютеров, так и профессиональных программно–аппаратных комплексов), обладают профессиональными навыками работы с различными компьютерными платформами, основными операционными системами и большинством пакетов специализированного программного обеспечения (офисные приложения, пакеты разработки приложений, сетевое программное обеспечение), в совершенстве владеют информацией об основных системах электронных коммуникаций (сотовая связь, сетевые протоколы, системы и методы защиты информации, защищенной связи) и используют эти знания в противоправной деятельности.

Данный тип личности характеризуется устоявшимися взглядами и системой ценностей, а также стойкостью к внешним воздействиям. Это лич-

---

[96] Бабаева Ю.Д., Войскунский А.Е., Смыслова О.В. Интернет: воздействие на личность [Электронный ресурс] // Режим доступа: http://www.relarn.ru/human/pers.html

[97] См.: Ясенев В.Н. Указ. соч. С. 57–59.

ности довольно амбициозные, но при этом четко знающие цену своим навыкам[98]. Постоянно совершенствуются в области методик и средств противоправной деятельности, которые часто разрабатывают сами.

Следует отметить, что рассмотрение нами данной классификации в рамках настоящего исследования было проведено с позиции использования ее лишь как одной из наиболее близких к теме мошенничества, совершаемого с использованием телекоммуникационных и компьютерных сетей, поскольку рассматриваемая О.М. Сафоновым тема («Использование компьютерных технологий при совершении преступлений») является достаточно близкой по смыслу к исследуемому нами направлению.

Однако, как нам представляется, ввиду отдельно нами взятой более узкой категории «мошенничество, совершаемое с использованием телекоммуникационных и компьютерных сетей» данная классификация не в полной мере подходит для нашего исследования.

Таким образом, проведенный анализ показывает, что в настоящее время отсутствует общепризнанная классификация лиц, совершающих мошенничества с использованием компьютерных технологий и телекоммуникационных сетей. Подобное положение вещей определяется, в первую очередь, отсутствием выделения в законодательстве преступлений подобного рода в отдельную самостоятельную категорию. Как показал анализ зарубежного опыта, подобный подход вполне оправдан с учетом выделения отдельных составов для соответствующих деяний. Между тем отсутствие подобной классификации либо использование взамен ее иных аналогов приводит к трудностям разработки конкретных мер, направленных на профилактику и пресечение преступных деяний в соответствующей области.

В аспекте мошенничества, совершаемого с использованием компьютерных технологий и телекоммуникационного оборудования, автором предлагается классификация, сформулированная с учетом исследования материалов уголовных дел (приложение Б) и основанная на степени вовле-

[98] См.: Бабаева Ю.Д., Войскунский А.Е., Смыслова О.В. Указ. соч.

ченности и устойчивости преступного поведения лиц:

«Случайные». К данной группе относятся лица, оказавшиеся втянутыми в незаконную деятельность без осознания факта правонарушения в своих действиях либо заведомо введенные в заблуждение. К данной категории, например, могут относиться так называемые «дропы» – лица, которых привлекают при осуществлении «вещевого кардинга», обналичивании незаконно полученных денежных средств и т. п. Зачастую лица, втянутые в процессы «вещевого кардинга», являются промежуточным звеном в процессе получения товарно–материальных ценностей «покупателем» от реального магазина, в котором товар был приобретен при помощи незаконно–полученных данных банковских карт либо при «отмывании» незаконно полученных денежных средств.

Для данной категории отсутствует потребность в определении уровня образования, однако в большинстве своем это лица, оказавшиеся в трудной жизненной ситуации либо просто ищущие дополнительные источники дохода. Чаще всего возможность квалификации их действий как преступных либо невозможна в принципе, либо труднодоказуема.

В данную же категорию следует отнести и лиц, совершающих операции с найденными платежными картами, что обусловлено разовой эпизодичностью деяния.

«Начинающие». Данная группа состоит, по аналогии с предыдущей классификацией, из лиц, однозначно понимающих, что их действия являются противоправными. Между тем пример «успешных» и более опытных «коллег» делает для них идею преступной деятельности достаточно привлекательной. Часть лиц, относящихся к данной категории, приходят из категории «случайных», другая же – «извне». Всех лиц данной категории характеризует высокая потребность в получении материальных ресурсов как основной мотив противоправного поведения.

Следует отметить также, что относящиеся к данной группе преступники, несмотря на наличие умысла и знаний в отдельно взятых конкретных

аспектах совершения деяния, имеют весьма слабое представление о комплексных формах и методах получения как денежных средств, так и товарно–материальных ценностей.

В зависимости от уровня интеллектуальных способностей и знаний «начинающие» мошенники могут либо получить «карьерный рост», либо прекратить противоправную деятельность ввиду внешних обстоятельств, среди которых может быть как попадание в поле зрения правоохранительных органов, так и отказ рассматриваемого преступного сообщества от взаимодействия с менее интеллектуально развитыми индивидами.

Однако именно из данной категории происходит большая часть лиц, относящихся к следующей группе.

«Специалисты». В рамках настоящей классификации в данной категории предполагаются лица, на «профессиональном» уровне реализующие как отдельно взятый этап мошенничества с применением компьютерного и телекоммуникационного оборудования, так и совокупность таковых действий. Преступники данной группы четко осознают нарушаемые ими нормы права как отдельно взятого государства, так и международного свойства. Их действия имеют не только явно выраженное направление сокрытия следов преступления, но и свойство осознанного манипулирования другими участниками процесса (из числа относящихся к группам «случайные» и «начинающие»).

Относящиеся к данной группе лица обладают достаточно незаурядными умственными способностями. Большинство из них либо имеет одно и более высших образований, либо ограничено рамками среднего общего образования. Подобное разграничение объясняется неспособностью представителей последних уживаться в рамках общепринятой системы, ввиду чего они не смогли окончить обучение в ВУЗе, а прохождение обучения в заведениях более низкого статуса является для них морально неприемлемым.

В рамках личностной ориентации представителей данной категории имеется два варианта существования в структуре групп, совершающих мо-

шенничество рассматриваемого вида: они стремятся либо получить некоторый объем денежных средств (зачастую отсутствует конкретная сумма), находясь на уже занимаемом ими месте, либо перейти в следующую категорию, чтобы иметь постоянный источник доходов в виде части незаконно полученных в процессе мошеннических действий денежных средств.

«Организаторы». Данная категория является своего рода «вершиной карьеры» для мошенников, действующих в рамках рассматриваемого вида преступлений. «Организаторы», как следует из названия, заняты формированием эффективного взаимодействия всей преступной цепочки, начиная с разработки схемы получения первичных данных (данные банковских карт, номера телефонов) и заканчивая участием в процессе распределения средств от преступной деятельности. Большая часть лиц из данной категории – материально обеспеченные люди, имеющие стабильный официальный доход, чаще всего служащий также частью структуры по «отмыванию» незаконно полученных денежных средств. К таковым относятся различного рода предприятия малого бизнеса, ориентированные на IT–аутсорсинг.

Нельзя оставить без внимания, что среди группы «организаторов» также можно выделить подгруппу «одиночек», которые характеризуются практически теми же чертами личности, однако из опасения быть раскрытыми другими участниками преступной ячейки осуществляют все операции самостоятельно. Следует также отметить, что выделение подобной подгруппы рационально только для данной группы, поскольку, находясь в любой другой категории, мошенник, по сути, остается частью общей структуры, вне зависимости от его собственного мнения.

Предлагаемая классификация является достаточно унифицированной, поскольку использует критерии «ролевых моделей» для участников преступного сообщества.

Учитывая специфику рассматриваемого вида противоправных деяний, следует отметить, что на практике аспекты распределения ролевых моделей между преступниками не всегда позволяют разграничить их место

в группе. Для формирования более полного представления о таких сложностях подробно рассмотрим один из примеров совершения мошенничества с использованием телекоммуникационного и компьютерного оборудования, расследование которого относится к практическому опыту автора настоящего исследования.

Так, в период с марта 2015 года по октябрь 2015 года на территории г. Хабаровска и г. Владивостока действовала организованная преступная группа, в состав которой вошли ранее знакомые между собой граждане: З., Н., П. и Ф, созданная для совершения преступлений, а именно совершения хищений денежных средств путем обмана, принадлежащих гражданам, проживающим в различных субъектах РФ, с целью личного обогащения[99].

В начале марта 2015 года гражданин З. при встрече с ранее знакомым Н. узнал от последнего о совершении им в октябре 2014 года и январе 2015 года двух мошенничеств, а именно хищений денежных средств путем обмана, принадлежащих лицам, проживающим в других регионах РФ, используя преступную схему, информация о которой была получена Н. из сети Интернет. Н. рассказал о данной преступной схеме З., после чего последний самостоятельно подыскал необходимую информацию в сети Интернет.

З., заведомо зная, что его знакомые Н. и Ф. не имеют постоянного источника дохода, нуждаются в денежных средствах, Н. склонен к совершению преступлений и обладает криминальным опытом и преступными навыками, так как ранее совершал подобные преступления, обладая качествами лидера и организатора, принял решение о создании организованной преступной группы для совершения многократных хищений денежных средств путем обмана, принадлежащих лицам, проживающим в различных субъектах РФ, по следующей преступной схеме: используя ноутбук и модем с сим–картой осуществить рассылку одинаковых смс–сообщений одно-

[99] Камко А. С. Уголовно–правовые вопросы противодействия преступности в сфере безналичных расчетов // Сборник материалов научно–практической конференции «Актуальные вопросы обеспечения прав и свобод человека и гражданина: региональное измерение». Хабаровск, 2017. С. 187–193.

временно на большое количество абонентских номеров путем набора кода любого сотового оператора случайно выбранного субъекта РФ и случайно выбранных последующих цифр и затем последовательного набора последних двух цифр абонентского номера от 00 до 99 с информацией о том, что данный абонентский номер по итогам акции в честь юбилея автокомпании, имеющей заранее придуманное название, выиграл автомобиль марки «Шевроле Авео» и более подробную информацию можно узнать, позвонив по абонентскому номеру, указанному в смс–сообщении, или на сайте автокомпании с одноименным названием.

Так, гр. З. взял на себя ролевую модель лидера преступной группы, а гр–не Н., П. и Ф. в разные временные промежутки соответственно стали непосредственными исполнителями. З. при этом также принимал участие в непосредственном исполнении отдельных этапов мошенничества.

Следует отметить, что в рамках авторской классификации гр. Н. может быть отнесен в большей степени к группе «начинающих», равно как и гр. Ф. Отнесение указанных лиц к данной группе рационально объясняется тем, что оба, несмотря на некоторую разницу в личном опыте, не были способны к самостоятельной разработке вышеуказанной схемы мошеннических действий.

Гр. З. в данном примере также не может быть в полной степени отнесен к категории «организаторы», несмотря на тот факт, что реализация мошенничества была инициирована и проработана его усилиями. Фактически, данное лицо находится на переходной ступени между группами «начинающие» и «специалисты»: полученные им знания и опыт реализации указанной модели однозначно могут быть позднее повторно реализованы, а также модифицированы при должном намерении. Однако, его практические навыки и недостаточное понимание ряда процессов предопределило как неспособность преступной группы как скрыть следы преступной деятельности, так и изначально держать деятельность в той области социаль-

но–экономических процессов, которая позволяет значительному числу деяний оставаться вне поля зрения правоохранителей.

Значительный интерес представляет также гр. П., деятельность которого сводилась к реализации базовых механизмов мошенничества: телефонные разговоры, рассылка и т. п. В данном случае он относится к категории «начинающие», однако, данное лицо не имело собственной инициативы по вхождению в преступную группу, что говорит о возможности осуществления с ним последующей профилактической работы и устранения последующего рецидивного преступного поведения.

Разграничение лиц из вышеописанной группы по соответствующим категориям позволяет, в первую очередь, определить истинный «уровень значимости» каждого из участников, личную роль и характер их действий. Так, например, отнесение гр. З к категории «организаторы» в предлагаемой модели возможно только ввиду некоторой семантики речи, поскольку данное лицо было инициатором создания преступной группы, то есть ее организатором. Однако для практики пресечения и профилактики преступлений данного вида отнесение его к более высшей иерархической ступени, чем в действительности, должно быть, приведет к появлению некоторого «избыточного потенциала» и неоправданно высоких затрат, как человеческих и временных, так и денежных ресурсов.

За период 2015–2018 годов нами был проведен анализ материалов 98 подобных уголовных дел, в расследовании которых автором принималось личное участие. На основании материалов указанных уголовных дел автором был произведен расчет относительной доли той или иной группы преступников от их общего числа (рисунок 10).

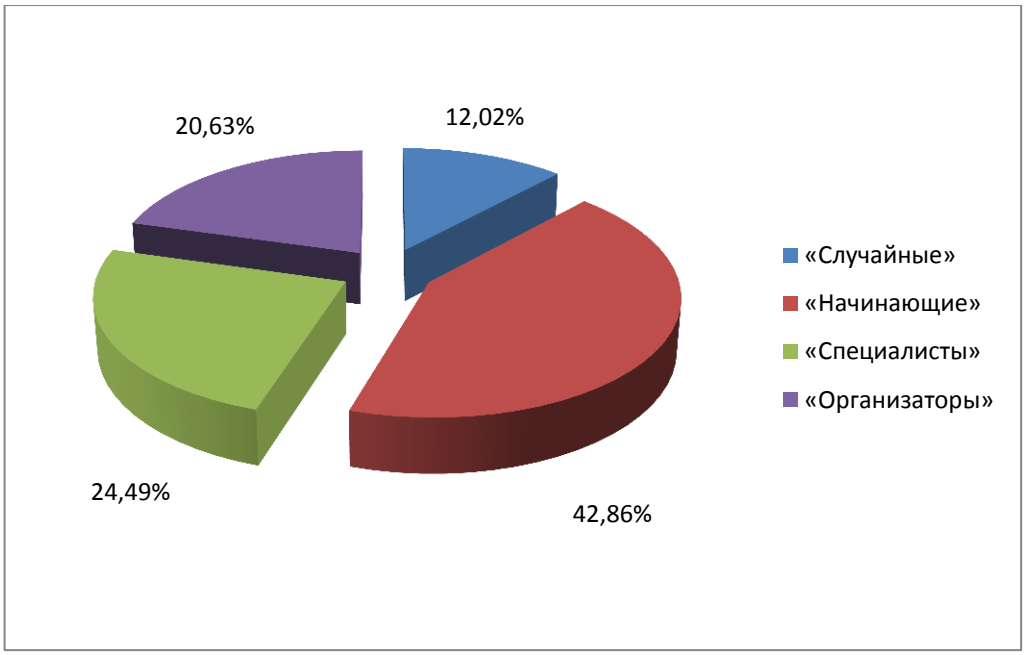


Рисунок 10 – Доля лиц, совершивших мошенничество с использованием телекоммуникационного и компьютерного оборудования, в соответствии с предлагаемой классификацией[100]

Как видно из представленных данных, не во всех случаях факт совершения деяния рассматриваемого вида предполагает наличие в группе лица, относящегося к категории «организаторы». Между тем число групп «специалисты» и «начинающие» в полной мере отражает наличие лиц, соответствующих этим группам при совершении каждого эпизода мошенничества с использованием телекоммуникационного и компьютерного оборудования.

Таким образом, только корректное соотнесение модели поведения, личных качеств и уровня образовательного и интеллектуального развития способно позволить сделать корректный вывод о принадлежности лица к той или иной группе в предлагаемой автором модели. Между тем подобное распределение в должной степени позволит установить необходимые методы и механизмы работы как с отдельно взятой личностью в составе пре-

[100] Расчет произведен автором на основании материалов, полученных в ходе осуществления профессиональной деятельности автора в качестве заместителя начальника УМВД России по г. Хабаровску – начальника следственного управления.

ступной группы, так и со всей группой в целом. В рамках дальнейшего развития криминологической науки на базе предлагаемой модели можно провести разработку значительного числа «шаблонных» механизмов профилактики и противодействия преступлениям рассматриваемого вида.

Кроме того, необходимо отметить и потребность в дальнейшем развитии исследований, связанных с изучением интеллектуального уровня преступников как в рассматриваемом виде деяний, так и в иных видах противоправной деятельности.

Проведенное автором при содействии специалистов правоохранительных органов исследование, связанное с определением интеллектуального уровня, показало, что значительная часть преступников обладает интеллектуальным потенциалом высокого и выше среднего уровней. Именно благодаря значительным интеллектуальным способностям основной массы преступников появляются все новые способы совершения мошенничества с использованием телекоммуникационного и компьютерного оборудования.

Данный вывод и полученные результаты должны в дальнейшем послужить основанием для разработки особой системы пенитенциарного и постпенитенциарного сопровождения рассматриваемой категории лиц для перенаправления их способностей в полезное социуму русло.

2.2 Виктимологическая характеристика мошенничества, совершаемого с использованием телекоммуникационного и компьютерного оборудования в России

Рассматривая вопросы противодействия мошенничеству, совершаемому с использованием телекоммуникационного и компьютерного оборудования в зарубежных странах, нами была выявлена необходимость виктимологической профилактики как один из основных факторов снижения количественного показателя роста преступных деяний рассматриваемого вида.

В рамках современной российской действительности вопросы снижения склонности граждан стать жертвой преступления в значительной степени актуальны. Социально–экономические реформы и сопутствующие им кризисные явления в совокупности создают множественные предпосылки изменения стиля поведения граждан.

С точки зрения отечественной криминологии о виктимологии принято думать с двух различных позиций: «как о науке, изучающей личность жертвы преступления, характер и содержание ее поведения, нравственно–психологический облик потерпевшего, роль жертвы в механизме преступного поведения»[101]; либо же как об одном из направлений (отраслей) криминологии[102]. Следует при этом отметить, что в настоящее время никто из отечественных ученых, какой бы позиции относительно данного вопроса он или она не придерживался, не может отрицать значимости виктимологических исследований.

В пользу криминологической природы виктимологии, кроме прочего, говорят и труды советских исследователей. Так, Л.В. Франк в своей работе «Потерпевшие от преступления и проблемы советской виктимологии»[103] пишет, что фактор жертвы способен как «порождать и ускорять, так и нейтрализовать и замедлять преступные проявления».

Специфическим предметом виктимологии являются «количественные и качественные статистически значимые характеристики виктимизации и индивидуальная способность тех или иных лиц стать потерпевшими, или, иными словами, неспособность избежать преступного посягательства, противостоять ему там, где это было объективно возможно»[104].

«В рамках виктимологии проводится исследование демографических, социально–статусных, культурных, психологических и других особенностей личности и образа жизни жертв преступлений, анализируются факто-

[101]Вишневецкий К.В. Место виктимологической теории в криминологии // Наука и практика. 2011. № 3(48).
[102] Квашис В.Е. Основы виктимологии. М., 1999.
[103] Франк Л.В. Потерпевшие от преступления и проблемы советской виктимологии. Душанбе: Ирфон, 1977. 240 с.
[104] Варчук Т.В., Вишневецкий К.В. Виктимология. М.: Закон и право, 2012. С. 184.

ры и закономерности формирования виктимогенных особенностей их личностей. Изучаются отношения и взаимоотношения между преступником и жертвой в момент возникновения и реализации уголовно наказуемого деяния. Особое внимание уделяется анализу роли и поведения жертв в генезисе преступного поведения, процессу виктимизации, и прежде всего – вызывает ли виктимизация преступность или только поощряет ее»[105].

«Виктимология обращает основное внимание на необходимость всестороннего учета фактора жертвы, на ее межличностные связи и отношения до, во время и после совершения преступления. Особый интерес для виктимологии представляет так называемая «виновная» жертва. Исследование материалов судебной практики, уголовной статистики, выяснение причин и условий, способствующих совершению преступлений, дает возможность сделать вывод, что многие преступления в определенной степени обусловлены поведением самих жертв».[106]

В отечественной криминологии проблемами взаимосвязи криминологических детерминант виктимности и преступного поведения занимались многие ученые: Ю.М Антонян, К.Д. Блувштейн, Б.С. Волков, П.С. Дагель, А.П. Закалюк, Л.В. Кондратюк, В.Н. Кудрявцев, В.В. Лунеев, В.С. Минская, Г.И. Чечель и другие.

В рамках как зарубежной, так и российской виктимологической теории основное развитие получили такие направления, как:

– анализ и разработка оптимальных паттернов поведения в потенциально криминогенных ситуациях;

– снижение общей и частной виктимности через систему постоянной профилактической работы и информирования граждан о виктимогенных ситуациях–ловушках;

– защита и реабилитация потерпевших от преступлений.

---

[105] Бумаженко Н.И. Виктимология. Витебск: ВГУ им. П.М. Машерова, 2010. С. 48

[106] Франк Л.В. Потерпевшие от преступления и проблемы советской виктимологии. Душанбе: Ирфон, 1977. С. 5.

В современной виктимологии существует значительное количество типологий потерпевших.

Так, Б. Мендельсон, резюмируя результаты своих исследований касательно отношений между злоумышленником и жертвой, сформировал первую типологию потерпевших: [107]

1. *Полностью невиновная жертва.* К числу таких жертв были отнесены дети и полностью невменяемые лица.

2. *Жертва с незначительной виной.* К данной категории жертв могут быть отнесены женщины, провоцирующие ошибочное нападение на себя.

3. *Жертва, которая является столь же виновной, как и обидчик.* Лица, относящиеся к третьей категории, целенаправленно провоцировали обидчика на совершение преступления своим поведением.

4. *Жертва, более виновная, чем обидчик.* Это лица, подталкивающие другое лицо к совершению преступления.

5. *Наиболее виновная жертва.* В данном случае жертвой в результате реализации другим лицом мер самозащиты становится сам преступник.

6. *Воображаемая жертва.* В эту категорию входят лица, страдающие от различных расстройств (например, паранойя), ввиду чего они ошибочно приписывают себе качества жертвы.

Подобная классификация, однако, кажется более уместной при рассмотрении жертв насильственных преступлений, поскольку при совершении преступлений рассматриваемого вида у злоумышленника зачастую контакт с жертвой отсутствует. Исключением можно считать телефонное мошенничество, однако в данном случае у мошенника отсутствует возможность предварительной (до телефонного контакта) оценки жертвы, что приводит к невозможности провокации действий мошенника со стороны

[107] Аракелян К.Н. Виктимология как отрасль юридической психологии: экскурс в историю возникновения // PsyJournals. 2011. № 2. С. 4–8.

жертвы.

Проводя свои исследования, Ганс фон Гентиг[108] рассматривал отношения между «деятельной стороной» (от англ. do – делать) и «страдательной стороной» (от англ. suffer – страдать), под которыми подразумевались преступник и жертва соответственно.

Предлагаемая им классификация была основана на психологических, социальных и биологических показателях. Одним из оснований для подобной классификации являлась необходимость идентификации жертв относительно различных факторов риска. В результате произошло распределение всех видов жертв на три основные категории: общий класс жертв, психологические типы жертв и активированное страдательное лицо (англ. – The Activating Sufferer).

В общий класс жертв входят:

1. *Молодежь, дети.* Ввиду своей незащищенности лица, относящиеся к данной категории, считались, по мнению автора, наиболее уязвимой группой.

2. *Женщины.* По мнению Гентига, женщины относятся к категории, наделенной определенной формой слабости, что провоцирует появление преступного намерения. В Германии слабость женщины до сих пор закреплена законодательно.

3. *Старшее поколение.* К данной категории относится большинство владельцев крупных состояний и власти, выступающей эквивалентом богатства в различных ее проявлениях. И в то же самое время лица, относящиеся к этой категории, слабы.

4. *Умственно неполноценные лица.* В данную группу входят психически больные люди, люди с умственной недостаточностью, а также наркоманы и алкоголики.

5. *Иммигранты и различного рода социальные меньшинства.* Иммиграция является причиной устойчивого чувства беспомощности как в

[108] Hentig H. Remarks on the Interaction of perpetrator and Victim // The of Criminal and Criminology. 1941. V. 31.

бытовых, так и в межличностных отношениях. Неопытный, бедный и зачастую депрессивный иммигрант – легкая добыча по всем видам преступления.

Психологические типы жертв состоят из следующих групп:

1. *Депрессивный тип.* Лица, относящиеся к данной категории, могут пострадать из–за подавленного инстинкта самосохранения. Лишенный такого инстинкта индивидуум может быть легко подвержен насилию, обману и т. п.

2. *Жадный.* Этот тип человека представляет собой легкую жертву. Чрезмерное стремление к выгоде затмевает любые доводы разума.

3. *Экстравагантный.* Поведение, выходящее за общепринятые рамки, часто провоцирует преступление.

4. *Одинокие и «убитые горем» жертвы.* Одиночество, по мнению Гентига, приводит к ослаблению умственных способностей индивида, ввиду чего тот становится легкой добычей для преступников. «Убитые горем» жертвы часто бывают настолько ошеломлены своими потерями, что становятся легкой добычей для преступников всякого рода.

5. *Мучитель*. Жертва в данном случае становится преступником по причине длительного насилия над ней.

6. *«Блокированная жертва».* Ситуация, при которой жертва столь запутана в ситуации сложного отношения с преступником, что защитные шаги становятся для нее невозможными.

7. *Активированное страдательное лицо.* Данный раздел включает в себя всего один одноименный элемент. Подобная ситуация имеет место, когда «жертва трансформируется в преступника. Множество факторов может выступать такого рода «активаторами» жертвы: личные предрасположения, возраст, алкоголь, потеря самоконтроля»[109].

[109] Аракелян К.Н. Виктимология как отрасль юридической психологии: экскурс в историю возникновения // PsyJournals. 2011. № 2. С. 4–8.

Следует отметить, что классификация жертв в случае учета «латентной» категории выглядит следующим образом:

1. *Потенциальная жертва*. Лица, способные стать целью при определенных обстоятельствах и в силу своих личностных свойств, либо социальных обстоятельств выступить в качестве жертвы преступления еще до самого факта его совершения.

2. *Случайная жертва*. Более детерминированная ввиду определенной ситуации потенциальная жертва.

3. *Латентная жертва*. Лицо, являющееся фактически пострадавшим от преступления, при этом факт преступления в силу каких–либо причин остался невыявленным, то есть скрытым от официального учета преступлений в условиях, когда такого рода учет обязателен.

«На основании содержания категорий виктимности и особенностей поведения жертв преступлений современная отечественная виктимология выделяет несколько типов жертв: агрессивные, активные, инициативные, пассивные, некритичные, нейтральные, случайные, реальные, потенциальные»[110].

Следует отметить, что, согласно исследованию, проведенному К.В. Вишневецким, «наиболее распространенными, по мнению экспертов, являются случайные (72%), реальные (69%) и потенциальные (56,6%) жертвы. Несколько снижены представления опрошенных о пассивных (40,2%) и некритичных (26%) жертвах. Агрессивные (конфликтные) жертвы преступлений отметили 23,6% экспертов. Вынужденно пассивные, инициативные и активные жертвы преступлений известны 18,5% опрошенных сотрудников. Весьма незначительную часть (11,4%) составляют нейтральные жертвы»[111].

В рамках настоящего исследования автором был проведен анализ таких характеристик жертв рассматриваемого вида мошенничества, как поло-

[110] Ривман Д.В. Криминальная виктимология / Д.В. Ривман. СПб.: Питер, 2002. 304 с.
[111] Варчук Т.В., Вишневецкий К.В. Виктимология. М.: Закон и право, 2012. С. 184.

возростная характеристика, уровень образования, семейное положение и т. п. Рассматривая указанные статистические показатели по материалам более 500 уголовных дел на стадии предварительного следствия[112] за период 2012–2015 годов, нами был составлен виктимологический портрет жертвы мошенничества, совершаемого с использованием телекоммуникационного и компьютерного оборудования.

Пол. Среди проанализированных материалов зарегистрированных преступлений среднее соотношение мужчин и женщин составило 23,95% и 76,05% соответственно (рисунок 11).

Несмотря на некоторую динамику – незначительное снижение числа мужчин среди потерпевших в 2015 году по отношению к 2012 году и увеличение доли женщин за аналогичный период, следует отметить абсолютное преобладание женщин среди потерпевших. Подобная статистика объясняется более высоким уровнем эмоциональной сферы, что подтверждается рядом исследований, проводимых отечественными психологами[113]. Высокий уровень эмоциональной сферы имеет значение при совершении мошенничества посредством телефонных звонков и смс.

[112] Материалы получены в ходе осуществления профессиональной деятельности автора в качестве заместителя начальника УМВД России по г. Хабаровску – начальника следственного управления.

[113] Например: Салихова Н.Р., Клементьева М.В. Соотношение характеристик ценностно–смысловой сферы личности и стратегий совладающего поведения // Известия ТГУ. 2014. № 4. С. 224–235; Минуллина А.Ф., Муртазина Э.И. Исследование характеристик эмоционального интеллекта и показателей толерантности к неопределенности у мужчин и женщин // Гуманитарные исследования в Восточной Сибири и на Дальнем Востоке. 2014. № 4(30). С. 125–130; Хазова С.А. Эмоциональные ресурсы совладающего поведения // Ярославский педагогический вестник. 2014. № 1. С. 293–297.

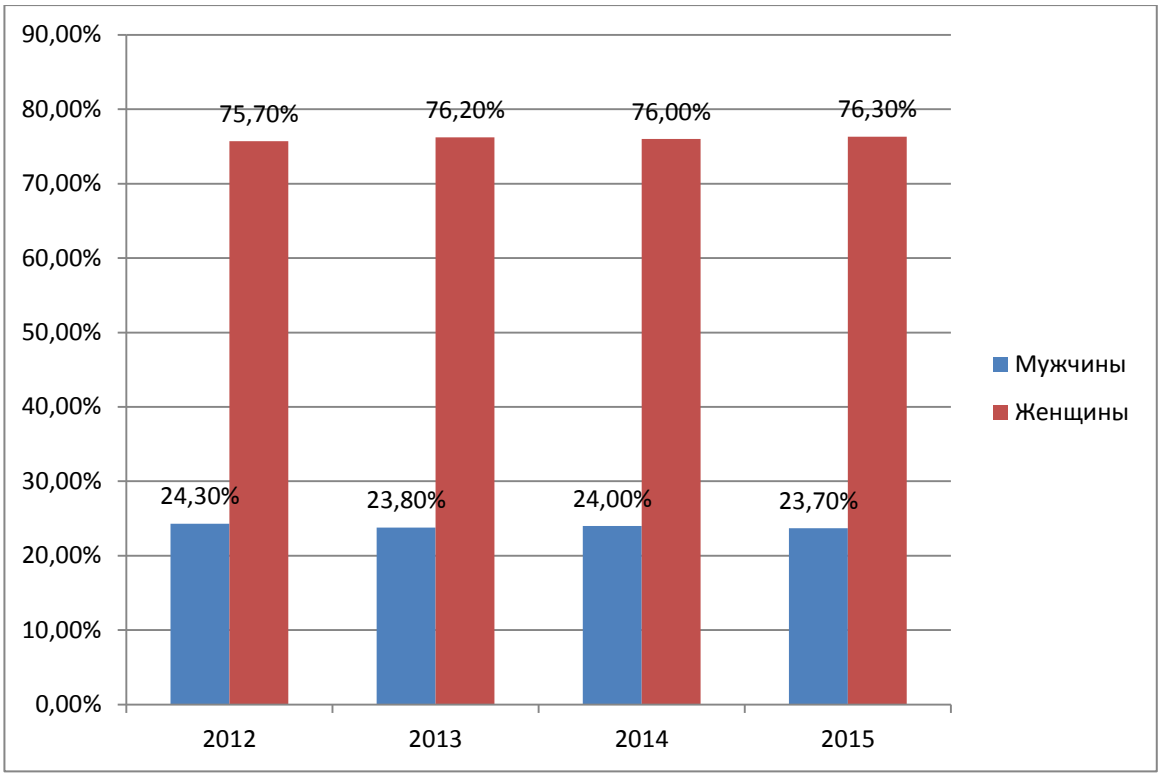


Рисунок 11 – Соотношение мужчин и женщин среди потерпевших в 2012–2015 годах, %

Другой причиной является более высокая активность женщин в качестве покупателей интернет–ресурсов, где оплата товаров или услуг происходит при помощи прямого перевода средств между счетами физических лиц, что подтверждают исследования некоторых маркетинговых компаний[114]. Следует при этом отметить, что к числу таких ресурсов были отнесены как сайты так называемых «совместных покупок» (например, 100sp.ru), так и «доски объявлений» (например, Avito, Youla). Последнее имеет значение при мошенничестве с банковскими картами.

Возраст. Рассматривая данный аспект личности жертв, автором была составлена диаграмма, представленная на рисунке 12.

Как видно из представленных на рисунке 12 данных, основная доля жертв мошенничества, совершаемого с использованием телекоммуникационного и компьютерного оборудования, приходится на возрастные группы

[114] Мужской и женский интернет: кто и как ведет себя в сети [Электронный ресурс] // Режим доступа: https://texterra.ru/blog/muzhskoy–i–zhenskiy–internet–kto–i–kak–vedet–sebya–v–seti.html

23–35 лет и 35–45 лет, суммарное значение которых составляет 63,2 %. Во–первых, это наиболее экономически активная часть населения, оплачивающая товары и услуги банковскими картами как в сети Интернет, так и в повседневной жизни, что приводит к появлению возможности у злоумышленников завладеть данными этих самых карт[115].

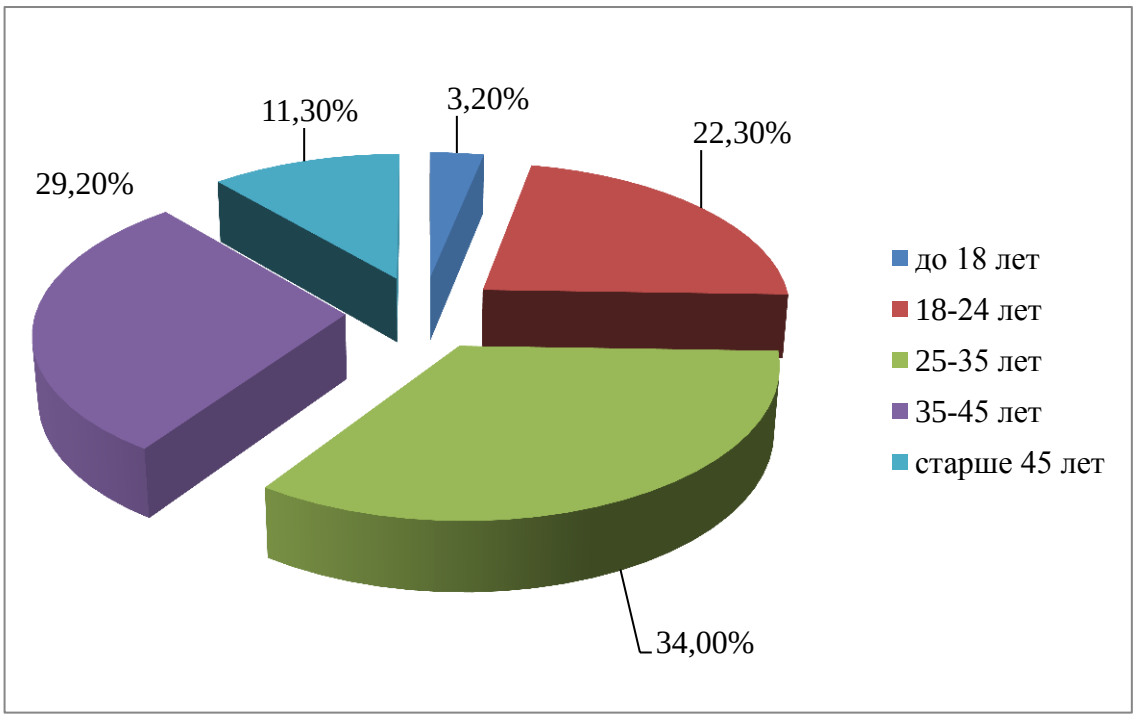


Рисунок 12 – Возрастная градация жертв мошенничества, совершаемого с использованием телекоммуникационного и компьютерного оборудования, %

Во–вторых, ввиду повышенной мобильности и постоянного стресса, связанного со скоростью жизни современного мира, данная категория лиц подвержена телефонному мошенничеству, поскольку одним из наиболее частых требований последних является наискорейшее совершение платежа, либо перевода денежных средств.

Группа лиц «до 18 лет» представляет собой наименьшую категорию

[115] Камко А.С. Виктимологическая профилактика преступлений в сфере безналичного обслуживания в России: состояние и перспективы развития, опыт // Библиотека криминалиста. 2016. № 6.

(3,2%) ввиду аналогичных причин: у большинства из них нет собственных банковских карт и значительных сумм собственных средств, что делает данную категорию малопривлекательной для мошенников подобного толка.

Рассматривая группу «18–24 лет» (22,3%), можно отметить ее как «переходную категорию» в понимании экономической самостоятельности, поскольку, во–первых, самостоятельно зарабатываемые средства уже появляются, однако их объемы зачастую незначительны. Во–вторых, молодые люди данного возраста достаточно сильно проявляют социальную активность, и, несмотря на игнорирование традиционных СМИ, активно пользуются различного рода социальными сетями и подобным, что приводит к их повышенной осведомленности о различных способах мошенничества. Кроме того, многие из них хорошо понимают принципы работы систем электронных платежей в части, касающейся сведений о карте либо клиенте, которые необходимы для проведения тех или иных операций. Таким образом, данная категория имеет относительно низкий уровень виктимности и вместе с группой «до 18 лет» составляет лишь четверть от всех жертв мошеннических операций.

Группа лиц «старше 45 лет» (11,3%) являет собой наименее виктимную категорию из числа экономически активного населения. Это объясняется как, с одной стороны, стремлением сохранить более привычный жизненный уклад (то есть данная категория наименее подвержена принятию сиюминутных, необдуманных решений), так и наличием значительного жизненного опыта. В рамках последнего необходимо учитывать специфику РФ, а именно период распада СССР и последующий период 90–х годов, во время которых уровень криминализации населения в стране значительно возрос, а имена некоторых организаций стали нарицательными. Подобный жизненный опыт соответственно отразился на менталитете населения.

Образование. «В значительной мере социальная ценность личности определяется уровнем его образования. Образование оказывает влияние на формирование жизненных установок, ценностных ориентаций, мотивов и

целей деятельности, привычек, правил поведения, способов реагирования на конкретные жизненные ситуации»[116].

Согласно проведенным автором исследованиям,[117] распределение потерпевших по уровню образования выглядит следующим образом (рисунок 13).

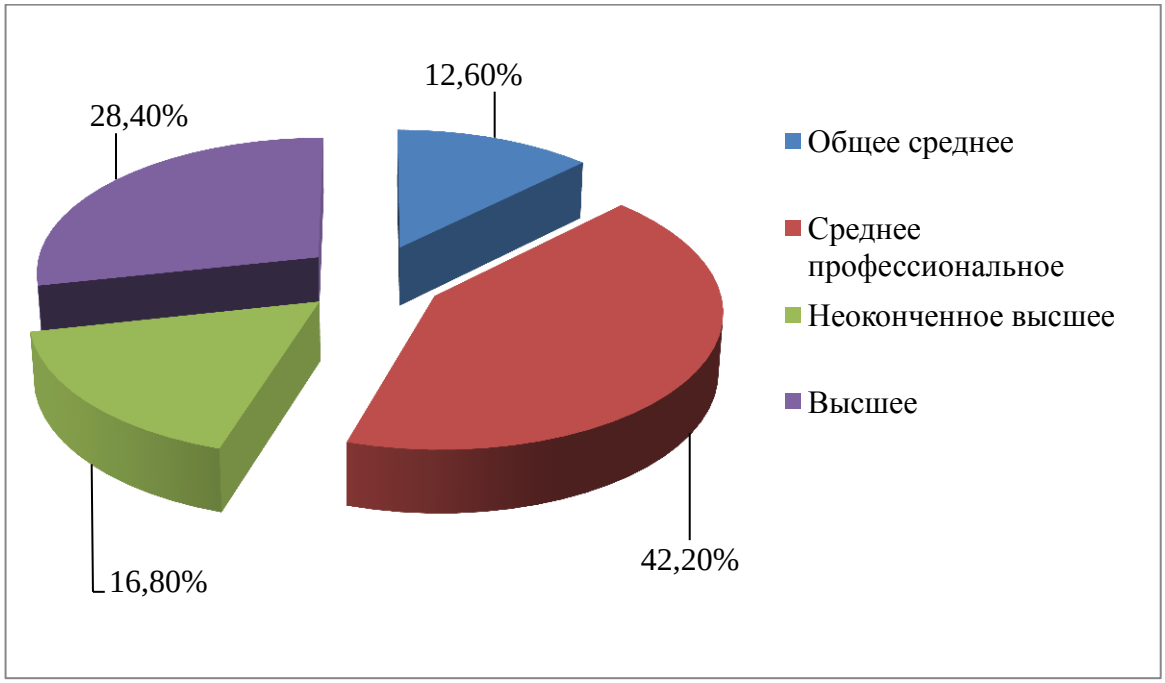


Рисунок 13 – Уровень образования у жертв мошенничества в сфере высоких технологий

Как показывают статистические данные, наименьшими являются группы лиц, имеющих общее среднее и неоконченное высшее образование: 12,6% и 16,8% соответственно. Рассматривая показатели образования и возраста, можно отметить, что общее значение (29,4%) двух минимальных групп в категории образования весьма близко к суммарному значению показателей «до 18 лет» и «18–24 лет», которое составляет 25,5%, что объясняется реализуемым стремлением многих молодых людей после окончания

[116] Ветров Н. И. Криминологическая характеристика правонарушителей молодежного возраста. М.: Наука, 1981. С. 43–44.
[117] Камко А.С. Виктимологическая профилактика преступлений в сфере безналичного обслуживания в России: состояние и перспективы развития опыт // Библиотека криминалиста. 2016. № 6.

школы поступить в высшие учебные заведения.

При этом категория лиц, имеющих высшее образование, составляет почти треть от общего числа жертв мошенничества в сфере высоких технологий, что, в свою очередь, говорит нам о том, что одного только факта получения высшего образования самого по себе не достаточно для снижения виктимности.

Наиболее многочисленной категорией среди жертв рассматриваемого вида мошенничества являются лица, имеющие среднее профессиональное образование. При этом, согласно всероссийской переписи населения, «лишь 31,2% граждан РФ имеют среднее профессиональное образование»[118], что позволяет говорить о наиболее высоком уровне виктимности данной категории населения. Наиболее лаконичным объяснением высокого уровня виктимности двух последних категорий могут стать слова М.А. Светлова: «некоторые идут в университет, чтобы научиться думать, но большинство – чтобы научиться тому, что думают профессора»[119].

Таким образом, основываясь на статистических данных, следует сделать вывод о необходимости включения в систему современного образования на каждом ее уровне профилактических мероприятий, направленных на снижение виктимности населения.

Семейное положение. В рамках настоящего исследования представляет интерес не сам статус семейного положения (рисунок 14), а состав семьи и внутрисемейные отношения.

---

[118] Всероссийская перепись населения [Электронный ресурс] // Режим доступа: http://www.gks.ru/free_doc/new_site/perepis2010/croc/perepis_itogi1612.htm

[119] Огнев В. О грустном юморе М. Светлова // Литературная газета. 2011. № 2.

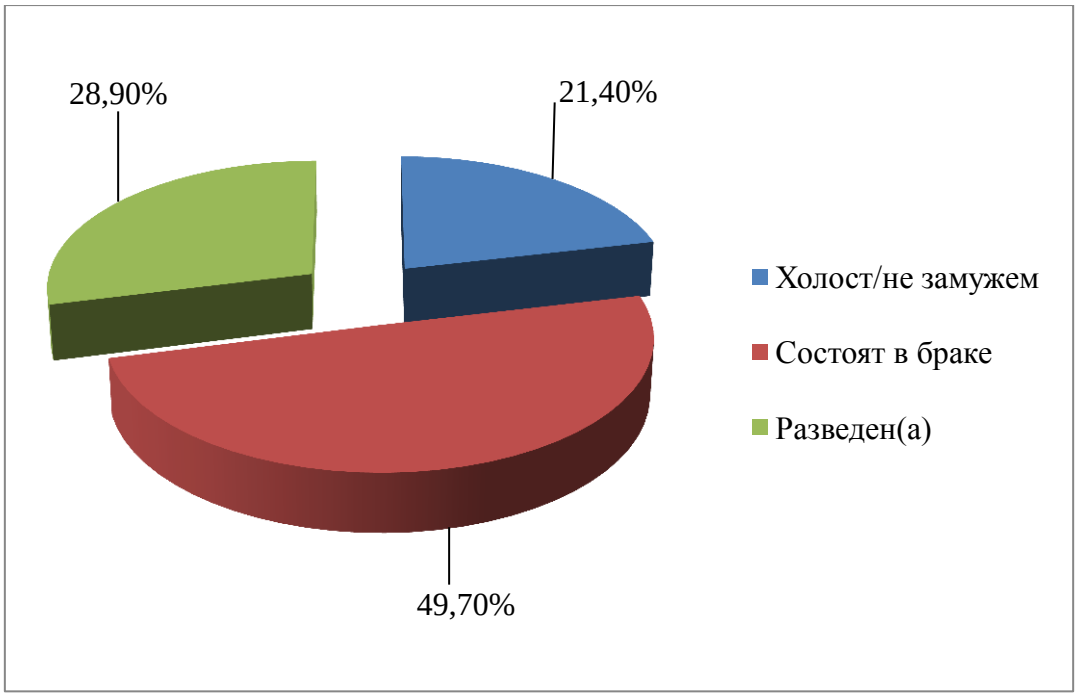


Рисунок 14 – Семейное положение жертв высокотехнологичного мошенничества, %

Как видно из данных рисунка 14, большую часть жертв рассматриваемого вида мошенничества составляют лица, состоящие или ранее состоявшие в браке. Данная тенденция наглядно демонстрирует поведенческие мотивы значительной части жертв, основанные на желании оказать помощь попавшему в беду родственнику или другу, что является одним из наиболее частых сценариев, используемых мошенниками.

Следует отметить, что минимальная относительная доля лиц, не состоящих и не состоявших в браке, среди жертв мошенничества, совершаемого с использованием телекоммуникационного и компьютерного оборудования, объясняется некоторой психологической закрытостью данной категории, появившейся в результате превалирования определенных внутренних мотивов, среди которых: карьерный рост, достижение личного комфорта и т. д. В результате этого у данной категории жертв рассматриваемого вида мошенничества, во–первых, отсутствует ряд социальных условий, на которые часто ссылаются мошенники (например, фактически может отсутствовать категория родственников, якобы попавших в беду). Во–вторых, большинство лиц

указанной категории не оставляют свои контактные данные в сети Интернет без наличия на то фактической причины (например, продажа какого–либо имущества путем размещения объявления на соответствующих интернет–ресурсах), что приводит к ситуации, когда злоумышленник просто не связывается с ними ввиду отсутствия у него таковой возможности.

Значительная часть потерпевших (71,2%) имеет одного и более детей (рисунок 15), оставшимся 28,8% в основном соответствует молодежь до 24 лет.

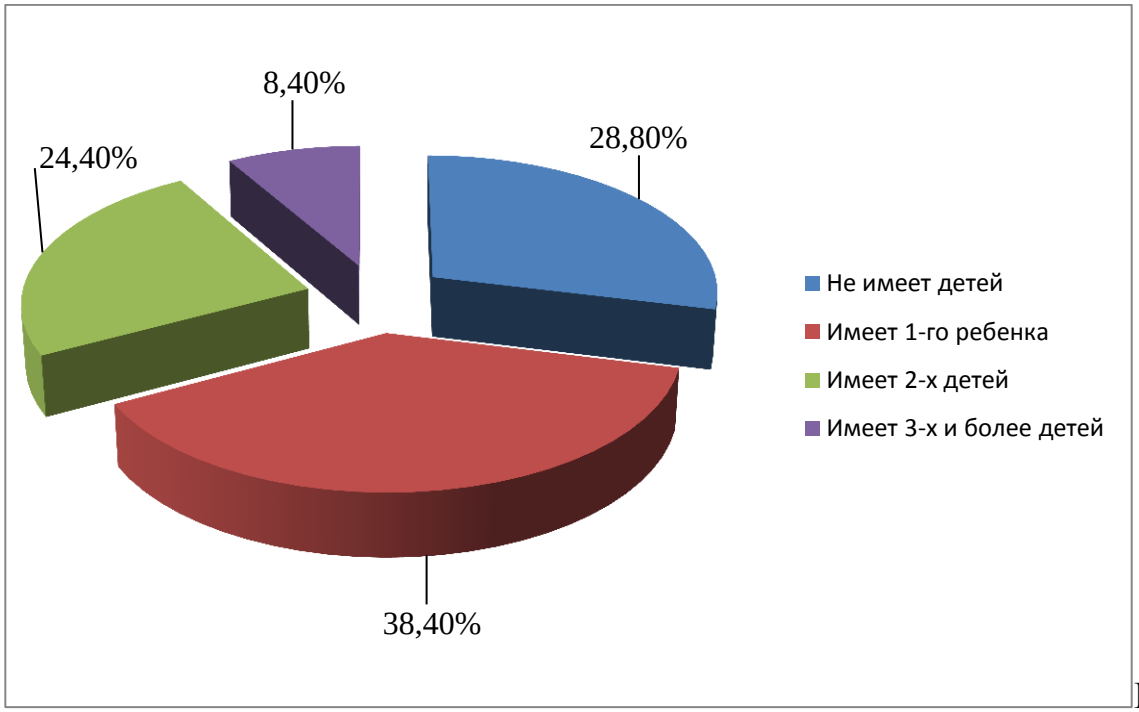


Рисунок 15 – Наличие детей у рассматриваемой категории жертв, %

Мошенники, прибегающие к психологическому манипулированию на семейных отношениях и чувствах жертв, чаще всего звонят абонентам с предложением откупиться за якобы задержанного правоохранительными органами родственника. При этом мошенники либо называют правильные имена, либо узнают имена напрямую у жертв. Суммы выкупа различны: от нескольких тысяч до полумиллиона рублей.

Следует также определить, что значительную роль в процессах викти-

мизации играет и поведение потерпевшего лица.

Поведение потерпевшего, в основе которого лежали корыстные мотивы или провоцировавшие преступника на совершение мошенничества. При рассмотрении или моделировании ситуаций следует иметь в виду, что здесь, как в любом мошенничестве, есть обман или злоупотребление доверием, а значит, чрезмерная доверчивость потерпевшего, однако превалирует по криминологическому значению все же корыстная заинтересованность, использованная преступником. Так, если потерпевший сам обращается с просьбой, в его действиях уже есть момент толчка, в других случаях – налицо не столь активное, но также корыстное поведение.

По данным изученных приговоров по уголовным делам (приложение Б) в 36,5% случаев для потерпевших характерно сознательное нарушение моральных норм, в основе их поведения лежит откровенный эгоизм. К потерпевшим такого рода относятся, на наш взгляд, игроки в онлайн–казино, вводящие реквизиты своих банковских карт в специальные поля на соответствующей странице фишингового сайта для регистрации и или подачи ставки в игре; вкладчики электронных финансовых пирамид и малоубедительных структур сетевого дистанционного маркетинга.

Поведение потерпевшего, в основе которого лежали излишняя доверчивость, некритичность, суеверие. Чрезмерная доверчивость потерпевшего иногда реализуется в ситуациях, где подозрительность должна была бы быть естественным следствием конкретной обстановки, такие случае в объеме изученных автором приговоров уголовных дел составили 29,2%. Поразительную доверчивость проявляют потерпевшие от мошенничеств, связанных с гаданием. Обычно потерпевшие поддаются на обещание излечить от болезни, возвратить или приворожить любовника, мужа, несколько реже – «навести порчу» на врага, соперника, для чего необходимо дистанционно оплатить услугу или произвести набор команд, по, как сообщают злоумышленники, подключению специальных платежных приложений, с которыми они работают на исключительных правах.

Положительное поведение потерпевшего, то есть не связанное с его негативными мотивами или некритичностью. Среди ситуаций подобного плана следует назвать приобретение вещей по нормальной цене и в обычной обстановке, не дающей оснований опасаться обмана. Относительная доля таких случаев в общей массе проанализированных данных невелика и составляет всего 14,6%. Профилактировать повышение виктимности в данном случае сложнее всего, так как добросовестность и внимательность потенциальной жертвы исключают обычные ошибки потерпевших от противоправных действий.

Поведение потерпевшего, которое создало условие, позволившее мошеннику не только совершить преступление, но и продолжить преступную деятельность. Практика насчитывает множество случаев, когда помимо или наряду с поведением потерпевшего, которое облегчило, сделало возможным совершение мошенничества в отношении его самого, поведение обманутого, последовавшее за совершенным преступлением, позволило преступнику продолжать преступную деятельность. В массе проанализированного материала (приложение Б) число таких случаев составляет 21,7%. Нередко потерпевший, передав деньги мошеннику (часто значительную сумму) и убедившись, что его обманули, требует деньги назад, но, не желая придавать делу уголовно–правовую окраску, в правоохранительные органы не обращается или, более того, пытается изменить последствия хищения незаконными способами (подлоги и фальсификация рабочих документов бухгалтером, злоупотребление должностным положением арбитражным управляющим).

К сожалению, в настоящее время отсутствует возможность установления статистически достоверных данных о моделях поведения жертв рассматриваемого вида преступлений ввиду отсутствия фиксации таковых данных в проанализированных материалах уголовных дел.

Несмотря на достаточно большой объем достоверной статистической информации о жертвах, как фактических, так и потенциальных, система виктимологической профилактики мошенничества, совершаемого с использова-

нием телекоммуникационных и компьютерных сетей в нашей стране практически отсутствует. Следует при этом отметить, что в России существует обширная теоретическая база, позволяющая современной виктимологии решать многие актуальные теоретические и научно–практические задачи. По мнению автора, в рамках настоящего раздела следует рассмотреть эти положения более подробно.

Проблема диагностики виктимогенности личности, а также виктимологическое прогнозирование в настоящее время являются одними из приоритетных направлений развития практической виктимологии. В настоящее время большое внимание исследователей привлекают вопросы защиты прав и оказания помощи жертвам преступлений. Однако, не менее актуальны социально–прикладные проблемы виктимологической профилактики, включая вопрос о соотношении между виктимизацией и страхом перед преступностью, а также между виктимизацией и общим подходом населения к проблемам уголовной политики.

Следует отметить, что вопросы виктимологической профилактики мошенничества в различных его направлениях в последние годы разрабатывались в рамках диссертационных исследований таких авторов как И.В. Ильин[120], Т.А. Малыхина[121], Д.О. Теплова[122], Д.А. Зыков[123], К.В. Астафьев[124] и др.

Так, например, И.В. Ильин в диссертационном исследовании 2000–го года сформулировал предложение о создании Центра учета и анализа экономического мошенничества и концепцию внутренней виктимологической профилактики данного вида мошенничества.

---

[120] Ильин И.В. Виктимологическая профилактика экономического мошенничества: дис. ... канд. юрид. наук. – Н. Новгород, 2000. 213 с.

[121] Малыхина Т.А. Виктимологическая характеристика и предупреждение мошенничества: дис. ... канд. юрид. наук. Иркутск, 2007.

[122] Теплова Д.О. Криминологическая характеристика и предупреждение организованного мошенничества: дис. ... канд. юрид. наук. М., 2014. 248 с.

[123] Зыков Д.А. Виктимологические аспекты предупреждения компьютерного мошенничества: дис. ... канд. юрид. наук. Владимир, 2002. 211 с.

[124] Астафьев К.В. Виктимологический аспект мошенничества (уголовно–правовое и криминологическое исследование): дис. ... канд. юрид. наук. Казань, 2007. 267 с.

Схожее предложение «о необходимости создания Центра учета и анализа компьютерного мошенничества, куда правоохранительные органы, различные организации и частные лица могли бы отправлять информацию о фактах совершения компьютерного мошенничества»,[125] было сформулировано в диссертационном исследовании Д.А. Зыкова двумя годами позднее.

В работе Т.А. Малыхиной были сформулированы положения о том, что «для осуществления виктимологической профилактики представляется необходимым:

– осуществление информационных мероприятий, направленных на информирование потенциальных жертв о способах и приемах совершения бытового мошенничества, а также на защиту реальных потерпевших от повторной виктимизации;

– организация аппарата взаимодействия ОВД и социальных служб для наиболее своевременного реагирования на совершаемые мошеннические акты; а также осуществление наиболее продуктивного взаимодействия указанных служб с общественностью и средствами массовой информации;

– совершенствование информационного обеспечения борьбы с мошенничеством, в первую очередь путем отслеживания данных, касающихся его виктимологических показателей»[126].

При изучении организованного мошенничества Д.О. Теплова сформулировала положение о том, что «исключительно репрессивный уклон в определении стратегии борьбы с ним <организованным мошенничеством> не способен дать заметные результаты без использования методов профилактики экономической, профессиональной, коррупционной и организованной преступности»[127].

В этой связи в качестве приоритетных направлений специально–криминологического предупреждения организованного мошенничества

---

[125] Зыков Д.А. Виктимологические аспекты предупреждения компьютерного мошенничества: дис. ... канд. юрид. наук. Владимир, 2002. 211 с.

[126] Малыхина Т.А. Виктимологическая характеристика и предупреждение мошенничества: дис. ... канд. юрид. наук. Иркутск, 2007.

[127] Теплова Д.О. Криминологическая характеристика и предупреждение организованного мошенничества: дис. ... канд. юрид. наук. М., 2014. 248 с.

Д.О. Теплова предлагала выделить: «осуществление оперативно–розыскных мероприятий, направленных на противодействие организованной и коррупционной преступности; разработку новых механизмов мониторинга и идентификации лиц – участников организованных групп и преступных сообществ; техническую и информационную поддержку подразделений, занимающихся борьбой с организованной и профессиональной преступностью; создание порталов правовой помощи жертвам мошенников; разработку информационных листов с описанием современных схем мошенничества»[128].

Фактически современные направления теоретических исследований при должном уровне практической реализации могут позволить снизить уровень совершаемых преступлений путем снижения значений определенных обобщенных виктимологических показателей.

Поскольку рассмотренные ранее типологии жертв не в полной мере отвечают запросам практической реализации виктимологической профилактики, автором предлагается применять типологию жертв, разработанную в рамках исследования Н.В. Ахмедшиной. «В основу данной типологии положен фактор взаимодействия виктимологической ситуации и личностных особенностей жертв преступлений (поведенческий аспект). Применение данной типологии жертв преступлений позволяет классифицировать жертв преступлений на следующие группы»[129]:

– случайные жертвы (лица, ставшие жертвами преступлений вследствие случайного стечения обстоятельств, не связанных с поведением жертвы или ее личными качествами);

– закономерные пассивные жертвы (лица, которые своим неосмотрительным либо неосторожным поведением способствуют созданию криминальной ситуации);

– закономерные активные жертвы (лица, которые своим аморальным либо противоправным поведением создают криминальную ситуацию и

[128] Там же.
[129] Ахмедшина Н.В. Криминологическая виктимология: современное состояние и перспективы развития : дис. … канд. юрид. наук. М, 2010.

провоцируют совершение в отношении них преступления).

Данная типологическая модель отличается от ранее разработанных своей ориентированностью на решение прикладных виктимологических задач, что в значительной степени отвечает интересам настоящего исследования.

Следует также отметить, что, по мнению ряда авторов, «организационная роль органов государственной власти и местного самоуправления в формировании единой системы виктимологической профилактики, разработка ее законодательной базы пока не соответствуют масштабу современных антикриминогенных задач»[130]. Опыт западных стран показывает, что в развитии виктимологического движения инициирующую роль выполняют институты гражданского общества[131]. В условиях их слабости и неразвитости в России, а также с учетом того, что необходимо ускоренными темпами преодолевать существующий разрыв, становится очевидной задача опережающего формирования и реализации государственной виктимологической политики.

Кроме того, в настоящее время достаточно сложно идет процесс интеграции правоохранительной системы с общественными институтами, работающими в сфере оказания помощи жертвам преступления. В то же время неправительственные, общественные организации и объединения являются одним из посредников в процессе социально–психологической адаптации жертв преступления.

Деятельность таких организаций охватывает широкий спектр социальных проблем, однако все их можно объединить в два основных направления: к первому относятся инициативные группы, объединившие-

---

[130] Вишневецкий К.В. Зарубежный опыт виктимологической профилактики преступлений и перспективы ее развития в России // Современное право. 2008. № 2.

[131] См.: Камко А.С. Зарубежная система профилактики и противодействия мошенничеству в сфере высоких технологий: законодательство и опыт // Библиотека уголовного права и криминологии. 2016. № 6.; Калашников О.Д. Виктимологическая профилактика – перспективное направление в борьбе с преступностью на современном этапе // Виктимология. 2017. № 1(11); Ревина Н.В., Ростокинский А.В. Опыт зарубежных стран в развитии виктимологической профилактики мошенничества // Бизнес в законе. 2010. № 1.

ся для оказания помощи и поддержки людям, оказавшимся в кризисных ситуациях и нуждающимся в психологической помощи, в эти группы входят лица, успешно преодолевшие социальные катаклизмы и выработавшие свои методы адаптации к ним. Такие общественные организации стремятся оказать помощь как самим потерпевшим, так и их родственникам, семьям. Помощь строится на основе консультаций – юридических, психологических; простого человеческого общения, обмена опытом, советов. Основой работы является вывод человека, его близких из сложной ситуации и помощь в адаптации к социальным условиям после совершения преступного посягательства.

Вторым направлением в работе общественных объединений можно назвать деятельность по оказанию помощи в экстремальной, кризисной ситуации, создание телефонов доверия, общественных приемных юристов и психологов, приютов для людей, подвергшихся насилию.

Одним из основных негативных для вышеобозначенной интеграции факторов является тот факт, что процесс взаимодействия между правоохранительными органами и общественными организациями зачастую натыкается на многочисленные ведомственные барьеры, нежелание менять стиль работы отдельными должностными лицами. В то же время поддержкой в реализации данного процесса часто является только личная инициатива сотрудников как правоохранительных органов, так и общественных организаций.

Одним из положительных примеров, на фоне всего выше обозначенного, можно считать разработанные в 2012 году Краснодарским Управлением МВД России методические рекомендации «Методика расследования преступлений, связанных с мошенническими действиями. Виктимологическая профилактика мошенничеств». В рамках методических рекомендаций были собраны и обработаны материалы различных научно–практических конференций и ведомственных мероприятий. Следует при этом

отметить, что данные методические рекомендации разработаны непосредственно для сотрудников правоохранительных органов.

Пособия аналогичной направленности, предназначенные для общественных объединений, в большей степени относятся к сфере социальной работы с населением: в них рассматриваются вопросы психологической помощи жертвам преступлений и некоторые иные аспекты деятельности общественных организаций, не имеющие направленности профилактики виктимности. Следует при этом отметить, что в рамках исследования рассматривается профиль мошенничества в сфере безналичных операций, для которого неприменимы такие мероприятия, как курсы самообороны и прочие, проводимые общественными организациями практические занятия.

Фактически, рассматривая вопросы виктимологической профилактики в нашей стране, следует отметить значительный объем теоретических разработок[132] и недостаточно высокий уровень их практической реализации. Это объясняется рядом факторов, первым из которых является отсутствие централизованного управления. Как было отмечено выше, развитие институтов гражданского общества происходит отдельно от развития правоохранительной системы и, по сути, представляет собой стихийное явление. Огромный объем криминологических исследований, связанных так или иначе с вопросами виктимологической профилактики преступлений в целом и мошенничества в сфере безналичного обслуживания в частности, не находит возможности реализации в практической деятельности правоохранительных органов. Это, в свою очередь, объясняется как менталитетом населения, не имеющего тенденции к самостоятельному личностному и профессиональному развитию посредством ин-

[132] См., например: Аракелян К.Н. Виктимология как отрасль юридической психологии: экскурс в историю возникновения // PsyJournals. 2011. № 2. С. 4–8; Астафьев К.В. Виктимологический аспект мошенничества (уголовно–правовое и криминологическое исследование) : дис. ... канд. юрид. наук. Казань, 2007. 267 с.; Ахмедшина Н. В. Криминологическая виктимология: современное состояние и перспективы развития: дис. … канд. юрид. наук. М, 2010.; Вишневецкий К.В. Криминогенная виктимизация социальных групп в современном обществе: монография. М.: ЮНИТИ– ДАНА, 2010. 295 с.; Задорожный В.И. Концептуальные основы виктимологической профилактики преступлений: дис. ... д–ра юрид. наук. М., 2007. 606 с.

теграции научных знаний в свою повседневную деятельность, так и ранее обозначенным отсутствием директивного управления. Из этого следует недостаточный качественный уровень виктимологической профилактики: правоохранительные органы не имеют возможности в полной мере взять на себя все функции общественных организаций, а общественные организации при реализации своих функций не обладают достаточным уровнем информированности в различных вопросах, относящихся к их компетенции.

В рамках практической реализации виктимологическая профилактика требует соответствующего уровня организационного и правового обеспечения. Эта необходимость обусловлена решением ряда существующих в современной действительности проблем, таких как:[133]

1. Подготовка специалистов, профилем которых станет виктимологическая профилактика.

2. Отбор кадров при приеме на службу в органы внутренних дел.

В настоящее время данная задача может считаться частично решенной в рамках системы отбора и подготовки кадров органов внутренних дел, однако требуется внесение ряда корректировок в систему первичной профессиональной подготовки личного состава.

3. Организация в рамках деятельности органов внутренних дел подразделений виктимологической профилактики, в составе которых должны находиться опытные оперативные сотрудники, специалисты в области обеспечения безопасности, психологи и педагоги. В обобщенном виде следует выделить два основных направления консультационной работы:

а) консультирование в части технических аспектов обеспечения безопасности собственности;

б) консультирование относительно поведенческих паттернов лиц, попавших в ситуацию или зону повышенной криминогенной опасности.

---

[133] Камко А.С. Виктимологическая профилактика преступлений в сфере безналичного обслуживания в России: состояние и перспективы развития, опыт // Библиотека криминалиста. 2016. № 6.

4. Организация «виктимологического учета», то есть профилактического учета лиц, которые уже являются либо с наибольшей долей вероятности могут стать потерпевшими от преступлений, если очевидна их повышенная уязвимость.

Система профилактического учета лиц, представляющих оперативный интерес, существующая в настоящий момент, не учитывает виктимных качеств личности, следовательно, она не может являться источником объективных данных. Также следует понимать, что законопослушные лица, обладающие высоким уровнем потенциальной виктимности, остаются вне поля зрения правоохранительных органов[134]. Ведение виктимологического учета в перспективе позволит существенно снизить численность лиц, состоящих на учете в качестве потенциальных правонарушителей, что даст возможность правоохранительным органам сосредоточить внимание на лицах, которые нуждаются в повышенных мерах обеспечения личной и имущественной безопасности.

Следует отметить, что подобная мера должна носить исключительно добровольный характер. Так, например, потерпевший при представлении своих персональных данных будет уведомляться сотрудником органов внутренних дел о предоставлении ему возможности включения в перечень рассматриваемой категории лиц. При этом потерпевший при согласии с такой мерой подписывает соглашение на обработку персональных данных в соответствии с Федеральным законом от 27 июля 2006 года № 152–ФЗ «О персональных данных». В дальнейшем лица, поставленные на подобный учет, будут получать актуальную информацию о мерах защиты своих имущественных интересах и отдельные (специальные) рекомендации, подготавливаемые для соответствующей группы потенциальных жертв преступлений.

С точки зрения организационных аспектов, объем финансовых затрат на подобные мероприятия будет стремиться к нулю, поскольку для создания

[134] Костыря Е.А. Виктимологическая профилактика и проблемы социально–психологической реабилитации потерпевших // Юридические науки: проблемы и перспективы: материалы Междунар. науч. конф. (г. Пермь, март 2012 г.). Пермь: Меркурий, 2012. С. 133–135.

подобной системы уже сформированы все необходимые технические условия. Дополнительное кадровое обеспечение также не потребуется ввиду привлечения к разрешению задач уже имеющегося кадрового состава органов внутренних дел.

Между тем следует отметить, что данное предложение в случае его практической реализации потребует значительной проработки отдельных организационных процессов, что может стать основой для самостоятельного исследования.

5. Разработка и внедрение информационных документов (карточек, дел) для наиболее опасных с точки зрения виктимологии объектов и территорий. В этих документах необходимо отразить:

а) статистические показатели преступлений, совершенных на данном объекте либо территории;

б) характерные для объекта либо территории личности преступников и их жертв;

в) шаблоны возникновения и реализации криминальных ситуаций на объекте либо территории.

Располагая достоверной статистической информацией подобного рода, непосредственное пресечение преступлений можно дополнить профилактическими мероприятиями по оздоровлению обстановки за счет количественного изменения групп – поставщиков лиц, являющихся потенциальными жертвами.

6. Формирование систематического взаимодействия всех аппаратов и служб органов внутренних дел, как между собой, так и с другими государственными органами и общественными организациями.

Реализация данного направления позволит использовать средства и методы оперативно–розыскной деятельности как в информационном плане, так и в качестве инструмента воздействия на профилактируемых индивидов.

Решение вышеобозначенных задач позволит сформировать систему общей виктимологической профилактики. Общая виктимологическая профилак-

тика не имеет в виду конкретное лицо, а осуществляется в отношении множества лиц, попавших либо способных оказаться в сфере действия негативных обстоятельств виктимологического характера. Данная профилактика в свою очередь реализуется по следующим направлениям:

а) выявление и устранение обстоятельств, выступающих в качестве внешних негативных воздействий, формирующих у личности качества повышенной виктимности;

б) выявление и устранение условий (обстановки, ситуаций), способствующих реализации виктимологически опасных качеств определенной группы лиц.

Таким образом, в общем виде виктимологическая профилактика мошенничества, совершаемого с использованием телекоммуникационного и компьютерного оборудования, включает:

а) информационно–профилактическую деятельность (правовая пропаганда, разъяснительная работа) в отношении населения, целью которой является демонстрация опасности и уровня распространения различных видов преступлений, способы их совершения и некоторые уловки преступников;

б) обучение определенных категорий лиц, занимающих должности или выполняющих обязанности, связанные с повышенной виктимологической угрозой;

в) мероприятия, направленные на активизацию населения (установка гражданами индивидуальных средств технической защиты жилья, принятие соответствующих шаблонов поведения);

г) меры, обеспечивающие сохранность имущества в гостиницах, общежитиях (обучение обслуживающего персонала, организация контрольно–пропускного режима);

д) непосредственное наблюдение за лицами, ведущими себя неосмотрительно в общественных местах, и своевременное вмешательство в виктимоопасные ситуации.

Организация профилактических мероприятий общей направленности должна быть ориентирована на группы лиц, наиболее виктимоопасные в отношении тех или иных видов преступлений, предусматривать меры, направленные на нейтрализацию обстоятельств, при которых личная виктимность реализуется. Из этого вытекает необходимость учитывать поведенческие качества виктимности, соответствующие ситуации, и «географию» реализации тех или иных преступлений, а также соотношения групп потерпевших и категорий преступников, характерные для преступлений того или иного рода.

«Поскольку различные группы лиц, объединенные общими для них социальными или психобиологическими качествами, могут быть уязвимы в отношении значительного круга преступных посягательств, постольку и общая профилактика, помимо ориентации на конкретный вид преступления, может организовываться непосредственно с прицелом на конкретные группы населения, граждан»[135].

В целом различные общепрофилактические меры можно разделить на две основные группы:

а) активизация личных защитных возможностей индивида.

К данной группе относятся такие меры, как правовая пропаганда, профессиональное обучение лиц из соответствующего перечня профессий, формирование у лиц с повышенной виктимностью необходимой предусмотрительности, критичности и т. д.;

б) обеспечение «внешней» безопасности.

Организация работы по соответствующим направлениям и с учетом соответствующих потребностей патрульно–постовой службы, установка охранной сигнализации в местах установки банкоматов и POS–терминалов, меры по обеспечению территории торговых помещений средствами видеофиксации.

В дальнейшем автором будет предпринята попытка разработки практических механизмов реализации вышеобозначенных направлений виктимологиче-

[135] Ахмедшина Н.В. Криминологическая виктимология: современное состояние и перспективы развития: дис. … канд. юрид. наук. М, 2010.

ской профилактики в комплексе мер по профилактике и противодействию преступлениям в сфере безналичного обслуживания.

Таким образом, для большинства случаев совершения мошенничества рассматриваемого вида значительным является половозрастная характеристика жертв: наиболее часто жертвами становятся женщины, возрастная группа (объединенно) – 25–45 лет; уровень образования – среднее специальное. Между тем невозможно рассматривать виктимологическую характеристику в разрыве с системой виктимологической профилактики, поскольку первая является следствием реализации последней.

В настоящее время в нашей стране отсутствует целенаправленная виктимологическая политика, а следовательно, не существует и комплексной системы виктимологической профилактики и виктимологической защиты населения. Актуальность же развития данного направления в существующих условиях является несомненным фактом. Эта необходимость подтверждается и зарубежным опытом. Оценивая предпосылки развития комплексной системы виктимологической профилактики в масштабах такой страны, как Российская Федерация, следует прежде всего отметить комплексную теоретическую базу, различные разработки которой находят свое отражение в практике некоторых регионов нашей страны.

Вопросы виктимологической профилактики рассматриваются отечественными исследователями не только в качестве отдельных научных статей, параграфов и глав диссертационных исследований и монографий, но и в качестве самостоятельных комплексных исследований.

На территории нашей страны уже существуют различные общественные объединения и организации виктимологической или частично виктимологической направленности (общества обманутых вкладчиков, общества защиты прав потребителей, Комитет солдатских матерей и т. п.). Однако большая часть данных организаций в своей идеологии имеет слабовыраженные криминально–виктимологические мотивы, отсутствует у них и сознание общности целей.

3 РАЗВИТИЕ СИСТЕМЫ ПРОТИВОДЕЙСТВИЯ МОШЕННИЧЕСТВУ, СОВЕРШАЕМОМУ С ИСПОЛЬЗОВАНИЕМ ТЕЛЕКОММУНИКАЦИОННОГО И КОМПЬЮТЕРНОГО ОБОРУДОВАНИЯ

3.1 Виктимологическая профилактика мошенничества, совершаемого с использованием телекоммуникационного и компьютерного оборудования, как основа системы предупреждения данной категории преступлений

Виктимологическая профилактика мошенничества, совершаемого с применением компьютерного и телекоммуникационного оборудования, равно как и преступности в целом, призвана оказывать соответствующее воздействие на причины и условия, способствующие повышению уровня виктимности населения, чтобы воспрепятствовать их возникновению, а виктимологическое предупреждение преступности – пресечь или нейтрализовать криминогенное воздействие тех из них, которые оказывают непосредственное влияние на процесс виктимизации[136].

В совокупности современных теоретических идей, взглядов и концепций отечественных исследователей по вопросам виктимологии прослеживаются элементы, обладающие определенной долей взаимосвязи как в части криминологических и уголовно–правовых процессов, так и с точки зрения общих социально–экономических принципов, характерных для современного общества, что позволяет объединить эти элементы в рамках некой модели, которую ряд авторов предлагает определить как «виктимологическое противодействие преступности», «виктимологическую профилактику» либо «виктимологическое предупреждение»[137]. Подобные элементы прослеживаются и

---

[136] Калашников О.Д. Виктимологическая профилактика – перспективное направление в борьбе с преступностью на современном этапе // Виктимология. 2017. № 1(11).

[137] См, например: Майоров А.В. О концепции виктимологического противодействия преступности // Юридическая наука и правоохранительная практика. 2015. № 4(34). С. 50–57; Жубрин Р.В. Предупреждение

активно разрабатываются в работах таких ученых, как Т.П. Будякова, К.В. Вишневецкий, Т.В. Варчук, А.А. Гаджиева, А.А. Глухова, В.И. Задорожный, В.Е. Квашис, В.С. Минская, А.Л. Ситковский, В.И. Полубинский, Д.В. Ривман и др.[138]

В рамках настоящего исследования нами будет определена концептуальная структура системы виктимологической профилактики рассматриваемого вида преступлений, а также определены некоторые конкретные ее части.

С точки зрения общенаучного подхода, систему виктимологической профилактики требуется определить в виде взаимосвязанных и взаимодействующих блоков, образующих единую систему воздействия как на некоторые факторы виктимности без разделения на отдельные и совокупные, так и на преступные элементы:[139]

1) цель и задачи виктимологической профилактики;

2) объекты позитивного воздействия и система субъектов;

3) меры профилактики и противодействия, включающие общие и индивидуальные виды профилактического воздействия, специальное (непосредственное) предупреждение, а также меры социальной помощи и защиты;

4) механизм реализации виктимологической профилактики и противодействия, включая различные виды деятельности субъектов с учетом их компетенций, осуществляемой по следующим направлениям:

– совершенствование виктимологической политики;

– правовое регулирование в области обеспечения виктимной безопасности, защиты жертв преступлений и обеспечение компенсации причиненного вреда;

преступности на современном этапе развития российского общества: понятие, содержание, принципы // Всероссийский криминологический журнал. 2016. № 4. С. 627–637.

[138] См.: Варчук Т.В. Виктимология: учеб. пособие / под ред. С.Я. Лебедева. М.: ЮНИТИ–ДАНА, 2009. 263 с.; Вишневецкий К. В. Криминогенная виктимизация социальных групп в современном обществе: монография. М.: ЮНИТИ– ДАНА, 2010. 295 с.; Задорожный В.И. Концептуальные основы виктимологической профилактики преступлений: дис. ... д–ра юрид. наук. М., 2007. 606 с.; Квашис В.Е. Основы виктимологии. М., 1999.; Ривман Д.В. Криминальная виктимология. СПб.: Питер, 2002. 304 с.

[139] Майоров А.В. О концепции виктимологического противодействия преступности // Юридическая наука и правоохранительная практика. 2015. № 4(34). С. 50–57.

– повышение эффективности взаимодействия субъектов системы виктимологической профилактики;

– создание, обеспечение и реализация необходимых условий для охраны имущественных интересов физических лиц, защиты их прав и свобод, прав и законных интересов юридических лиц, интересов общества и государства;

– выявление причин, порождающих повышение уровня виктимизации населения, и условий, ему способствующих, разработка и осуществление мероприятий, направленных на их устранение или нейтрализацию;

– принятие мер по повышению уровня защищенности и обеспечения безопасности граждан; принятие иных мер в области функционирования системы виктимологической профилактики и противодействия, предусмотренных законодательством РФ и международными нормативно–правовыми актами.

Целью виктимологической профилактики является оказание максимального профилактического и предупредительного воздействия на процессы, способствующие повышению уровня виктимности и развития виктимизации; устранение угроз правам, свободам и законным интересам граждан, возникающих в связи с реальной возможностью совершения в отношении них преступлений; повышение и активизация индивидуальных защитных свойств различных категорий граждан от рассматриваемого вида преступлений; оказание социально–правовой помощи гражданам, ставшим жертвами преступных посягательств[140].

Таким образом, конечной целью виктимологической профилактики должно стать обеспечение такого состояния защищенности личности и общества от создающих опасность угроз, при котором соответствующий уровень виктимности не оказывает существенного влияния на их законные интересы и способствует устранению процесса виктимизации.

---

[140] Якимова Е.Д. Виктимологическая профилактика преступности: содержание и задачи // Виктимология. 2014. № 1 (1). С.55–58.

В свою очередь, достижение обозначенных целей виктимологической профилактики предполагает решение следующих задач:[141]

– выявление причин и условий (факторов) виктимизации, их анализ и обобщение;

– разработка и реализация мер, направленных на устранение либо нейтрализацию виктимогенных факторов;

– реализация законодательных положений по защите прав и обеспечению безопасности жертв преступлений;

– создание новых государственных и негосударственных структур, работа которых направлена на поддержку и защиту жертв преступлений;

– выявление лиц, обладающих определенной виктимностью, и воздействие на них с целью снижения риска стать жертвами преступления;

– воспитание у граждан правового сознания и правовой культуры;

– обеспечение активного участия юридических лиц, общественных объединений и граждан в процессе противодействия преступности и государственная поддержка их участия.

К объектам комплексной виктимологической профилактики целесообразно отнести общепринятые в криминологии объекты, а именно[142]:

1) виктимность и ее виды. Виктимность так же, как и производимая ею преступность, обладает специфическими признаками (социальной обусловленностью, массовостью, системностью, причинением отрицательных последствий) и характеризуется количественными (состояние, уровень, динамика) и количественно–качественными (структура, территориальное распределение) показателями;

2) виктимогенные факторы и ситуации, формирующие виктимное поведение и обусловливающие совершение преступлений в отношении конкретных лиц;

---

[141]Ахмедшина Н.В. Криминологическая виктимология: современное состояние и перспективы развития: дис. … канд. юрид. наук. М, 2010.

[142] Воронин Ю.А., Майоров А.В. Виктимная безопасность: терминологическая интерпретация // Криминологический журнал БГУЭП. 2014. № 1. С. 43–48.

3) виктимогенные группы населения (общий уровень);

4) конкретные лица, являющиеся потенциальными жертвами преступлений вследствие своего социального положения, психофизического состояния, индивидуального поведения либо образа жизни (индивидуальный уровень).

Систему субъектов виктимологической профилактики рассматриваемого вида мошенничества исходя из сложившегося подхода в криминологии логично разграничить на три уровня, в зависимости от выполняемых ими функций: общесоциальнный, специально–криминологический и индивидуальный.

В качестве субъектов первого, общесоциального уровня выступают государство и его органы власти и управления, а также организации, общественные объединения, юридические лица, участвующие в системе профилактики правонарушений[143].

Государственные органы выполняют в рамках своей компетенции возложенные на них функции социального управления путем разработки, принятия и реализации законов, постановлений правительства, указов Президента, других нормативных актов, регламентирующих общественные отношения в тех или иных сферах жизнедеятельности общества и государства. Предупредительная роль подобных мер реализуется одновременно с разрешением значительных по своим масштабам социальных задач, которые носят общегосударственный характер и оказывают влияние на жизнь большого числа граждан, представляя собой единую систему социально–экономических, политических, правовых, организационных и иных мер, предпринимаемых обществом и государством в различных социальных сферах, которые сами по себе специально не направлены на девиктимизацию населения и предотвращение преступности.

[143] Задорожный В.И. Концептуальные основы виктимологической профилактики преступлений: дис. ... д–ра юрид. наук. М., 2007. 606 с.

Организации и общественные объединения, участвующие в системе виктимологической профилактики, по согласованным с органами государственной власти и органами местного самоуправления направлениям профилактической работы либо по собственной инициативе в пределах и формах, определяемых законодательством РФ в сфере профилактики правонарушений, в соответствии с компетенцией и уставными задачами выявляют процессы, явления, обстоятельства и ситуации, способствующие совершению преступлений, лиц, способных стать жертвами преступлений в силу присущих им субъективных качеств или объективных свойств; информируют об этом орган, учреждение, организацию, в компетенцию которых входит устранение (минимизация, нейтрализация) криминогенного влияния указанных факторов и обеспечение необходимого уровня защищенности граждан; оказывают правовую и иную поддержку жертвам преступлений, предусмотренную законодательством Российской Федерации[144].

К субъектам специально–криминологического уровня системы виктимологической профилактики относятся государственные органы, для которых предупреждение преступности и ее искоренение являются главной функциональной задачей (суды, прокуратура, органы внутренних дел). Виктимологическая профилактика на данном уровне, в отличие от общесоциального, охватывает мероприятия, непосредственно направленные на устранение причин и условий, связанных с совершением конкретных преступлений, отличаясь своим специальным предназначением и направленностью на конкретный объект воздействия[145].

Субъектами индивидуального уровня системы виктимологической профилактики следует определить самих физических лиц, ведущих законопослушный образ жизни, использующих системы и формы личной защиты, активно участвующих в обеспечении своей (своих близких) безопасности самостоятельно или совместно с другими гражданами в соответствии с феде-

[144] Там же.
[145] Воронин Ю.А., Майоров А.В. Теоретические основы формирования системы противодействия преступности в России // Всероссийский криминологический журнал. 2013. № 1. С. 7–16.

ральными законами; граждан, участвующих в системе профилактики правонарушений в пределах и формах, определяемых законодательством в сфере профилактики правонарушений и преступлений; лиц, способных выявить процессы, явления, обстоятельства и ситуации, способствующие совершению преступлений, принять законные меры и сообщить об этом в орган, учреждение, организацию, в компетенцию которых входит устранение криминогенных и виктимогенных факторов.

Деятельность субъектов виктимологической профилактики на общесоциальном и специально–криминологическом уровнях осуществляется в различных масштабах: на общегосударственном – в рамках конкретного региона, предприятия, учреждения, общественной группы, определенного контингента лиц и т. д. На индивидуальном уровне эта деятельность носит личностный характер и зависит от субъективных качеств и объективных свойств человека (пол, возраст, образование, социальное и семейное положение, психо–физические данные, материальное положение и т. д.).

Субъектов, решающих задачи по виктимологической профилактике, с учетом их компетенции (прав и обязанностей) можно также разделить на три категории:

1. Общие: коммерческие и некоммерческие организации с различной формой собственности, предприятия и учреждения; политические партии и массовые общественные организации, действующие на основе уставов и положений, имеющие вертикальную и горизонтальную структуру на различных уровнях, вплоть до микрорайонов; объединения и молодежные формирования; профсоюзы; кооперативные объединения; учреждения физической культуры и спорта, туризма и культуры; частные охранные службы; средства массовой информации; различные ассоциации и сообщества; благотворительные и религиозные организации; общественные организации и формирования, создаваемые на добровольной основе; общественность, участвующая в деятельности государственных, представительных и правоохранительных органов (внештатные сотрудники и общественные помощники), органов мест-

ного самоуправления и территориальных общин (органов территориального общественного самоуправления и т. п.).

2. Специальные, действующие в пределах своей компетенции государственные органы и органы местного самоуправления: исполнительные органы государственной власти и органы самоуправления; органы местного самоуправления; правоохранительные органы (суд, органы внутренних дел, прокуратура), адвокатура и нотариат; органы образования, здравоохранения, социальной защиты и занятости населения; юридические службы предприятий, учреждений.

3. Физические лица (индивидуально), то есть гражданин, ставший заложником виктимогенной ситуации и являющийся потенциальной жертвой в силу своих субъективных качеств и объективных свойств; активно использующий различные формы противодействия преступности (в разрезе рассматриваемого вида деяний – от средств защиты информации до предусмотрительности и осторожности в ежедневной деятельности) в целях снижения уровня своей (своих близких) виктимности и повышения уровня защищенности, а также обеспечения необходимой безопасности.

Функционирование системы виктимологической профилактики должно осуществляться на принципах: [146]

1) законности;

2) защиты и соблюдения прав и свобод человека и гражданина;

3) гласности;

4) социальной справедливости и гуманизма;

5) научной обоснованности;

6) системности и комплексности организационных, правовых, социально–экономических, информационных и иных мер воздействия;

7) своевременности и достаточности мер воздействия.

---

[146] Ахмедшина Н.В. Криминологическая виктимология: современное состояние и перспективы развития : дис. … канд. юрид. наук. М, 2010.

Меры виктимологической профилактики, таким образом, реализуются путем применения субъектами с учетом их компетенций: [147]

1) социально–экономических мер по оздоровлению экономики в целом и социальной защите наиболее уязвимых слоев населения;

2) организационно–управленческие меры, направленные на устранение ошибок и упущений в управлении экономикой, социальной сферой, правоохранительной деятельностью, в том числе объявление руководителю организации, а также другим соответствующим лицам обязательных для исполнения официальных предостережений о недопустимости действий, создающих условия для совершения преступлений, а также меры по совершенствованию нормативного, информационного, методического и ресурсного обеспечения виктимологического воздействия на преступность;

3) идеологические и воспитательные меры, устраняющие или ограничивающие криминогенные факторы через формирование у членов общества нравственной позиции, ориентированной на базовые общечеловеческие ценности, формирующие в общественном сознании нетерпимость к противоправному поведению и антиобщественным действиям, повышающие общую, бытовую и правовую культуру людей;

4) технические меры посредством использования достижений науки и техники, препятствующие совершению преступлений, в том числе с помощью аппаратно–программных комплексов технических средств контроля за состоянием правопорядка и безопасности;

5) правовые меры, включая разработку проектов нормативных правовых актов, в целях повышения эффективности виктимологического потенциала в сфере противодействия преступности, совершенствования действующего законодательства по защите жертв преступлений и обеспечения компенсации причиненного ущерба;

---

[147] Вишневецкий К.В. Криминогенная виктимизация социальных групп в современном обществе: монография. М.: ЮНИТИ–ДАНА, 2010. 295 с.

6) профилактические меры, реализуемые на общем, индивидуальном и специально–криминологическом уровнях, которые включают:[148]

– выявление виктимогенных ситуаций и лиц с повышенной виктимностью, принятие мер по их устранению;

– информирование населения о криминогенных и виктимогенных ситуациях и о поведении граждан, обеспечивающее их защиту от преступных посягательств;

– разъяснение категориям лиц, обладающим повышенной виктимностью, о направленности их поведения;

– выявление потенциальных жертв преступлений;

– информирование лиц о возможном совершении в отношении них преступлений, оказание помощи по обеспечению их защищенности;

– оказание помощи лицам с повышенной виктимностью с целью активизации их внутренних защитных возможностей, а также обеспечение их имущественной безопасности и безопасности их личных данных;

– обеспечение личной безопасности граждан, общественная и профессиональная деятельность которых обусловливает их повышенную виктимность;

7) научные меры, обусловливающие проведение правовых, криминологических, социологических, психологических, экономических и иных исследований с целью:[149]

– изучения статистических материалов, характеризующих виктимность, ее виды, а также жертв преступлений, их типологию;

– выявления особенностей и тенденций виктимности, выбора средств преодоления виктимогенных факторов и ситуаций;

– изучения и обобщения сведений, содержащихся в различных источниках правоохранительных и других органов и учреждений, материалах

---

[148] Камко А.С. Виктимологическая профилактика преступлений в сфере безналичного обслуживания в России: состояние и перспективы развития, опыт // Библиотека криминалиста. 2016. № 6. С. 176.

[149] Калашников О.Д. Виктимологическая профилактика – перспективное направление в борьбе с преступностью на современном этапе // Виктимология. 2017. № 1(11).

средств массовой информации, интернет–ресурсов, заявлениях и сообщениях граждан;

– выявления, обобщения и внедрения в практику новых форм и методов профилактической и предупредительной деятельности виктимологической направленности;

– выявления новых групп риска с повышенной виктимностью и воздействия на них в целях активизации их защитных свойств и девиктимизации.

Виктимологическая профилактика, как комплексное явление, должно являться элементом системы социального контроля над потенциальными актами нарушения прав и свобод отдельных граждан. Однако справедливо и мнение ряда отечественных исследователей (В.Е. Квашис, Е.А. Костыря, А.А. Ксеник и др.), согласно которому виктимологическая профилактика может рассматриваться в широком и узком (специально–криминологическом) аспектах как относительно самостоятельная система, функционирующая во взаимодействии с другими элементами системы общесоциальной профилактики и специально–криминологического предупреждения преступлений.

Описываемая выше система виктимологической профилактики является в большей степени теоретической моделью, реализация которой на практике позволит добиться снижения уровня виктимности и устранения процесса виктимизации населения, а также повышения защищенности и способности граждан противостоять проявлениям криминальной активности, о чем свидетельствуют исследования отечественных и зарубежных авторов, в рамках которых сделан вывод о том, что профилактические меры, направленные на блокирование, уменьшение влияния криминогенных факторов или их устранение, приводят к минимизации подобных преступлений.[150]

Анализ различных концептуальных взглядов на виктимологическую профилактику как социальное управление в условиях трансформации обще-

[150] Вишневецкий К.В. Криминогенная виктимизация социальных групп в современном обществе: монография. М.: ЮНИТИ– ДАНА, 2010. 295 с.

ства показывает, что в странах Западной Европы и США акцент делается на мягких регулирующих воздействиях субъекта управления на объект. Важнейшей функцией виктимологической профилактики становится поддержание в обществе необходимого соотношения между неизбежными, являющимися следствием объективных причин, процессами криминализации и процессами декриминализации социума[151]. Это означает, что в профилактической деятельности должны существовать достаточно большие зоны социальной самоорганизации, не подверженные прямому воздействию субъекта управления. Эти зоны представляют собой механизм развития способностей общества к самоорганизации, к поддержанию социального порядка и укреплению законности. К сожалению, в России отсутствует система виктимологической защиты населения и целенаправленная виктимологическая политика государства, которая была бы по своим масштабам сопоставима с западными аналогами. Актуальность ее развития в условиях глобализации и сопутствующей ей транснационализации криминальных угроз очевидна[152].

Между тем, противодействие преступности закреплено в Федеральном законе от 07.02.2011 года № 3–ФЗ «О полиции»[153] как одна из первостепенных задач полиции (ст. 1). Другим примером может служить Федеральный закон от 23.06.2016 № 182–ФЗ «Об основах системы профилактики правонарушений в Российской Федерации», предметом регулирования которого выступают «общественные отношения, возникающие в сфере профилактики правонарушений в Российской Федерации»[154].

Снижение уровня криминальной активности лиц, склонных к совершению противоправных деяний, всегда находится в центре внимания правоохранительных органов. Однако на сегодняшний день все более очевидным становится то, что развитие виктимологического потенциала предупреди-

---

[151] Там же.

[152] Фаргиев И. А. Виктимология в системе научного знания // Северо–кавказский юридический вестник. 2014.№ 4. С. 101–105.

[153] Федеральный закон от 07.02.2011 № 3–ФЗ (ред. от 05.12.2017) «О полиции» // Собрание законодательства РФ. 2011. № 7. Ст. 900.

[154] Федеральный закон от 23.06.2016 № 182–ФЗ «Об основах системы профилактики правонарушений в Российской Федерации» // Собрание законодательства РФ. 2016. № 26 (Часть I). Ст. 3851.

тельного воздействия имеет ряд преимуществ, таких как: совершенствование профилактики преступности; более точное определение размеров латентной преступности; расширение возможностей государства в организации предупредительного воздействия на преступность благодаря использованию материальных и иных ресурсов самих жертв и др[155].

Организационная роль государства и органов государственной власти в формировании единой системы виктимологической профилактики, разработка ее законодательной базы в РФ пока не соответствуют масштабу современных антикриминогенных задач.

Опыт западных стран, таких как Германия и Великобритания, свидетельствует, что в развитии виктимологического движения инициирующую роль выполняют институты гражданского общества. Однако в условиях их слабости и неразвитости в России, а также с учетом того, что необходимо ускоренными темпами преодолевать существующий разрыв, становится очевидной задача опережающего формирования и реализации государственной виктимологической политики[156]. Построение системы виктимологической профилактики в России предопределено и обосновано разработанной отечественной криминологической наукой теорией предупреждения преступности. Ее собственно криминологические аспекты достаточно легко ложатся в основу построения системы виктимологической профилактики в Российской Федерации.

Так, объектами общей виктимологической профилактики являются: виктимность и ее виды; виктимогенные факторы и ситуации, формирующие виктимное поведение и обусловливающие совершение преступлений в отношении конкретных лиц; виктимогенные (в наибольшей степени подверженные опасности стать жертвами преступлений) группы населения. Учитывая многоуровневость объектов общей виктимологической профилактики, а так-

---

[155] Степанов–Егиянц В. Г. Современная уголовная политика в сфере борьбы с компьютерными преступлениями // Российский следователь. 2012. № 24. С. 43–46.

[156] Сафонов О. М. Уголовно–правовая оценка использования компьютерных технологий при совершении преступлений: состояние законодательства и правоприменительной практики, перспективы совершенствования : дис. … канд. юрид. наук. М., 2015.

же ее специфические меры воздействия, характеризующиеся масштабностью и многосторонностью, следует отметить, что правоохранительные органы не могут воздействовать на все ее аспекты, тем более устранять их собственными силами. Здесь необходим комплексный подход различных органов государственной власти и общественного самоуправления, а также специализированных общественных организаций и объединений[157].

По аналогии с существующими криминологическими канонами предупреждения преступности общесоциальное предупреждение виктимизации представляет собой единую систему социально–экономических, политических, правовых, организационных и иных мер, предпринимаемых обществом и государством в различных социальных сферах, которые сами по себе не направлены на борьбу с преступностью.

Специально–криминологическая виктимологическая профилактика преступлений, осуществляемая правоохранительными органами – это специфическая деятельность специальных субъектов по осуществлению комплекса мер предупреждения преступности или отдельных видов преступлений нетрадиционным путем, прежде всего ориентированных на: выявление отдельных лиц и групп риска с повышенной степенью виктимности и воздействие на них в целях восстановления или активизации их защитных свойств и последующей девиктимизации; недопущение, устранение или нейтрализацию (совместно с другими субъектами этой деятельности) детерминационного комплекса виктимности – участие в разработке либо совершенствование в повседневной практической деятельности уже имеющихся специальных видов, форм и методов повышения охранно–защитных возможностей потенциальных жертв преступлений[158].

Поскольку общесоциальные меры предупреждения виктимизации носят комплексный характер, они должны учитывать особенности виктимиза-

---

[157] Вишневецкий К.В. Криминогенная виктимизация социальных групп в современном обществе: монография. М.: ЮНИТИ– ДАНА, 2010. 295 с.

[158] Вишневецкий К.В. Зарубежный опыт виктимологической профилактики преступлений и перспективы ее развития в России // Современное право. 2008. № 2.

ции каждой из социальных групп с учетом мировых тенденций глобализации, к числу которых возможно отнести и переход к безналичной системе расчетов, что неизменно приводит к увеличению числа банковских карт. Рассматривая данную тенденцию с точки зрения виктимизации населения можно отметить ее неоднозначность. С одной стороны, уменьшается опасность совершения карманной кражи, либо разбойного нападения с целью хищения наличных денежных средств, поскольку банковская карта защищена ПИН–кодом, без которого получить доступ к денежным средствам затруднительно.

С другой же стороны, повсеместное применение систем безналичного расчета приводит к ослаблению бдительности как отдельных индивидов, так и целых социальных групп. Так, установленное скимминговое оборудование может быть принято за вполне законное считывающее устройство, имеющее непривычную для конкретного индивида форму, размеры и (или) цвет. В случае с цветом гражданин также может принять это за соответствующие изменения, связанные с ребрендингом его кредитной организации и т. п.

При этом следует органично сочетать социальную профилактику виктимизации на индивидуальном уровне и на уровне социальной страты. Основу методов такой профилактики должна составить деятельность по девиктимизации социальных групп в сочетании с нейтрализацией негативных элементов образа жизни личности. В этой точке органично сочетаются и взаимодополняют друг друга меры общесоциальной и специальной (целенаправленной) виктимологической профилактики, имеющие прямой целью нейтрализацию виктимогенных факторов и условий, предотвращение фактов виктимизации личности и ее ближайшего социального окружения.

Проведенный в рамках настоящего исследования анализ позволил выявить направления деятельности по формированию системы виктимологической профилактики, направленной на предотвращение эпизодов мошенничества с использованием компьютерного и телекоммуникационного оборудования.

В соответствии с обозначенными теоретическими подходами определим, что целью виктимологической профилактики мошенничества, совершаемого с использованием телекоммуникационного и компьютерного оборудования, является *снижение количества правонарушений имущественного характера, связанного с неправомерным отчуждением материальных благ путем совершения мошенничества с использованием телекоммуникационного и компьютерного оборудования.*

Задачи виктимологической профилактики мошенничества, совершаемого с использованием телекоммуникационного и компьютерного оборудования, будут соответствовать общим задачам виктимологической профилактики, обозначенным нами выше.

Решение задач виктимологической профилактики рассматриваемого нами вида мошенничества будет достигаться путем взаимодействия ее субъектов (к числу которых будут относиться: органы внутренних дел, органы государственной и муниципальной власти, банковские и кредитные организации, а также представители иных видов коммерческой деятельности) с соответствующими объектами.

Так, основу комплексной системы виктимологической профилактики должна составить система «виктимологического учета», отдельные элементы которой были упомянуты нами в рамках второй главы настоящего исследования.

Предлагаемая система будет построена на применении уже имеющихся информационно–аналитических ресурсов органов внутренних дел с определенным объемом дополнений.

В настоящее время в деятельности МВД используется система баз данных, содержащих информацию по различным преступлениям. Достаточно простым решением вопроса анализа этих данных, включая и цели виктимологического учета, представляется внедрение программной надстройки, позволяющей группировать зарегистрированные преступления по соответству-

ющим статьям УК РФ; выводить данные о численности потерпевших; разграничивать их по территории проживания, а также персонифицировать их.

Конечным результатом анализа представляется разграничение данных по группам:

– *Уровень виктимологической безопасности отдельных территорий*, где будет отражаться информация о наиболее частых местах совершения преступлений. Следует пояснить, что в данном случае речь идет как об отдельных районах города (например, с высокой концентрацией банкоматов, на которые регулярно устанавливается незаконное оборудование для сбора данных с банковских карт), так и о конкретных местах (например, заведения общественного питания, в которых регулярно происходит незаконное получение данных банковских карт, включая ПИН–коды к ним; арендуемые объекты недвижимости, используемые мошенниками в качестве «офисных помещений» для организации телефонного мошенничества и т. д.).

– *Уровень виктимности отдельных социальных групп и индивидов,* в рамках которого будут отражаться статистические характеристики жертв рассматриваемого вида мошенничества, что позволит их объединять в соответствующие группы для последующей корректировки направлений виктимологической профилактики.

Так, например, представляется целесообразным проводить перекрестные исследования в отношении социальных страт, разделенных на два базовых класса. К первому классу могут быть отнесены страты, выделенные по социально–экономическому принципу (основной принцип стратификации): богатые, состоятельные, середина (аналог среднего класса), малообеспеченные, бедные[159].

Ко второму классу целесообразно отнести страты, выделенные по половозрастному принципу: женщины, мужчины, дети, лица младшего, средне-

[159] Волеводз А. Г. Противодействие компьютерным преступлениям: правовые основы международного сотрудничества: монография. М.: Юрлитинформ, 2001. 496 с.

го, преклонного возраста (наиболее изучаемые в западной виктимологии категории) и страты с лабильной виктимностью[160].

Ранговая корреляция данных, полученных в ходе таких исследований по второму и первому классам страт, позволит составить развернутую таблицу их качественно–количественных параметров, определяющих характер стратовой виктимности.

В качестве основных должны рассматриваться следующие зависимости: процент мужчин и женщин, являющихся жертвами преступных посягательств, по каждой страте; аналогичные показатели для числа преступников; процент лиц молодого и пожилого возраста, являющихся соответственно жертвами и преступниками в каждой из страт; мера соответствия стратовой виктимизации социально–демографической структуре региона; присутствие в регионе мигрантов, по своему социальному статусу близких представителям данной страты.

Подобные исследования позволят в определенном хронологическом периоде (полугодие, год и т. д.) формировать портрет личности как преступника, так и жертвы, что в свою очередь позволит своевременно корректировать сами мероприятия виктимологической профилактики.

Дополнительно могут выступать такие параметры, как зависимость виктимности от пьянства и наркомании; родственных, соседских и подобных отношений между жертвой и преступником; числа посягательств на незнакомых/знакомых лиц и т. п.

Одним из наиболее рациональных итогов внедрения подобной системы в структуру практической деятельности по виктимологической профилактике видится формирование структурированной базы данных виктимологического учета, в которой будут отражены как персональные данные, так и анализ таких признаков, как территория проживания жертв; территория совершения противоправных действий (например, места хищения данных банковских карт); количественные показатели преступлений, имеющие значение при

[160] Там же.

определении адресности и очередности проведения мер виктимологической профилактики.

Именно понимание виктимности как массового явления и как образа поведения и действия определенных людей, вызывающих повышенный к себе интерес лиц, склонных к совершению преступлений, открывает возможности для виктимологической профилактики[161].

Для организации виктимологической профилактики важно не просто выявить потенциальную жертву, а проследить связь возможного причинителя вреда и жертвы в различных криминогенных ситуациях. В настоящее время данная деятельность, в соответствии с Федеральным законом «О полиции» от 07.02.2011 № 3–ФЗ, относится к ведению полиции.

Сами ситуации различны по масштабу, степени развития и времени проявления в них негативных признаков. Так, по критерию масштабности проявления в социальной среде можно выделить макро– и микроситуации. Примером макроситуации может быть экономическая нестабильность в стране, возникшая вследствие кризиса и выражающаяся во всеобщей заинтересованности улучшить свое материальное положение за счет осуществления сомнительных, малопроверенных финансовых операций. Что касается микроситуации, то примером может служить конфликтная обстановка в неблагополучной семье, в результате которой лицо определенной половозрастной характеристики остается в одиночестве перед необходимостью реализовывать свои финансовые интересы.

Для данного примера необходимо отметить, что оказавшаяся в трудной жизненной ситуации личность может стать как жертвой рассматриваемого вида мошенничества (корыстный мотив доверия), так и одним из участников преступного сообщества, поскольку именно поиск дохода (не имеет значения дополнительного или основного) является основным мотивом на первоначальном этапе становления личности преступника.

---

[161] Вишневецкий К. В. Криминогенная виктимизация социальных групп в современном обществе: монография. М.: ЮНИТИ–ДАНА, 2010. 295 с.

Сами же мероприятия виктимологической профилактики мошенничества с использованием компьютерного и телекоммуникационного оборудования могут быть различными и сведены в две основные группы. К первой относятся меры, направленные на устранение ситуаций, чреватых возможностью причинения вреда:

1) изготовление и распространение специальных памяток–предостережений о том, как уберечься от преступника, не стать жертвой преступления.

Так, для эффективного управления рисками и сохранения деловой репутации руководство ОАО «Россельхозбанк» распространило меры по борьбе с хищением денежных средств с использованием дистанционного банковского обслуживания и отмыванием денег на все структурные подразделения, направления деятельности, банковские продукты и услуги, оказываемые банком. Другим примером могут служить текстовые сообщения, приходящие при совершении операций ДБО, основным содержанием которых является предупреждение клиентов банковских услуг о неразглашении данных своих банковских карт, а также о недопустимости передачи специальных подтверждающих кодов третьим лицам;[162]

2) извещение граждан через средства массовой информации об имеющихся на данной территории фактах совершения преступлений, типичных действиях преступников, о том, как следует поступать гражданам в случае контакта с преступниками (осуществляемого посредством использования сети Интернет или мобильной связи) или при нахождении в криминально опасной ситуации.

Так, например, на территории большинства крупных городов Российской Федерации на «медиабордах» и информационных экранах можно видеть информационные ролики, предупреждающие о необходимости проверять любые данные, поступающие по средствам телефонной связи, прежде чем

[162] Камко А.С. Виктимологическая профилактика преступлений в сфере безналичного обслуживания в России: состояние и перспективы развития, опыт // Библиотека криминалиста. 2016. № 6.

реагировать на них (не переводить деньги на основании смс от неизвестных абонентов о состоянии жизни и здоровья близких родственников и т. д.).

Со стороны банков и коммерческих организаций, в которых расположены банкоматы, эта деятельность может проявляться через размещение информационных плакатов о возможных способах совершения мошенничества и необходимости бдительно относиться к своей безопасности.

Аналогичные меры могут быть приняты операторами сотовой связи и мультибрендовыми компаниями–ретейлерами в масштабах своих офисов продаж;

3) оказание практической помощи гражданам в технической и физической защите от возможного несанкционированного доступа к их персональным данным (убеждение в недопущении форматирования зараженного вредоносным ПО коммуникационного устройства, передача его эксперту в области IT–технологий в соответствующее подразделение правоохранительных органов для последующей декомпиляции);

4) проведение целенаправленных бесед с родителями, работниками детских учреждений, педагогами, школьниками, учащимися других учебных заведений о том, как следует вести себя детям и подросткам для сохранения личной информации в сети и что делать в случае попытки со стороны преступника установить контакт с ребенком.

Данная мера в большей степени имеет целью формирование технически и юридически грамотного поколения граждан, которое будет в большей степени защищено от приемов «социальной инженерии», которые в настоящее время являются одними из самых действенных методов получения персональных данных мошенниками в сети Интернет. Однако следует также отметить, что некоторыми мошенниками дети используются в качестве наиболее уязвимой категории не только для получения данных о составе семьи и подобное, которые в последующем используются мошенниками для введения потерпевших в заблуждение с целью формирования у последних представления о своей благонадежности, но и для получения данных банковских карт

родителей. В этом случае мошенники под благовидным предлогом («сделать маме сюрприз» и т. п.) просят детей втайне от родителей посмотреть и передать им сведения, написанные на банковских картах;

5) проведение бесед с пожилыми людьми и инвалидами, а также проведение собраний, совещаний, занятий с бухгалтерами, кассирами, продавцами, работниками банковских и иных финансовых учреждений.

Ко второй группе относятся меры, позволяющие обеспечить личную безопасность возможной жертвы преступления. По существу, это меры индивидуальной виктимологической профилактики, которые, в свою очередь, можно разделить на две подгруппы. К первой относятся меры по обеспечению личной безопасности возможной жертвы преступления в случаях, когда иным способом устранить опасную ситуацию для данного лица по каким–либо причинам оказалось невозможным. Эти меры касаются, как правило, лиц, профессиональная деятельность или социальное положение которых предопределяют их виктимность.

Следует отметить, что к данной категории мер относится и упомянутая в рамках второй главы настоящего исследования система «добровольной постановки на учет» граждан из числа потерпевших, обратившихся в органы внутренних дел с заявлением о соответствующем правонарушении. В данном случае профилактическая мера будет изначально носить адресный характер, а потенциальная жертва будет, во–первых, в большей степени заинтересована в получении помощи, во–вторых, лояльнее воспримет попытку контакта со стороны субъектов виктимологической профилактики.

Сами меры выражаются в информировании и обучении таких лиц, установлении личной охраны, предоставлении средств индивидуальной технической защиты (специальные экраны, мощные антивирусные утилиты, система подтверждения операции электронным ключом), определении безопасных мест для временного проживания или пребывания и др.

Ко второй подгруппе относятся мероприятия, заключающиеся в воздействии на потенциальную жертву с тем, чтобы восстановить или активизи-

ровать в ней внутренние защитные возможности. Это могут быть разъяснительные беседы, обучение приемам самозащиты в сети и при пользовании средствами мобильной связи, оповещение о предстоящих ситуациях, ориентирование на поддержание постоянной связи с правоохранительными органами, контроль за поведением потенциальной жертвы и др. Использование тех или иных мер виктимологической профилактики зависит от многих факторов, в частности от вида, места, времени и способов совершения преступления, способности жертвы оказать противодействие преступнику, наличия у соответствующих органов и должностных лиц достаточных сил и средств для оказания поддержки жертвам и др. В каждом конкретном случае набор мероприятий определяется с учетом реальной обстановки.

Так, например, резюмируя описание форм, методов, направлений профилактики по снижению уровня виктимности населения и участников предоставления услуг в сфере ДБО, субъектам виктимологической профилактики (как правоохранительным органам, так и сотрудникам различных учреждений) необходимо принять к практике реализации определенный алгоритм действий, оформленный в соответствующие рекомендации потенциальной жертве и (или) потерпевшему от мошенничества рассматриваемого вида.

Осуществлять профилактические мероприятия по снижению виктимности населения необходимо комплексно, основываясь на принципах рационального и своевременного взаимодействия всех субъектов профилактики, стараясь охватить все уровни воздействия (общую профилактику – на все население, групповую – на отдельные категории граждан, индивидуальную).

Исключительно комплексные, организационные и технические меры безопасности информационной инфраструктуры могут обеспечить минимизацию последствий преступных посягательств злоумышленников, однако только при условии тесного взаимодействия кредитных учреждений, операторов мобильной связи и иных коммерческих и некоммерческих структур с соответствующими правоохранительными органами возможно как снижение

уровня виктимизации населения, так и успешное пресечение преступной деятельности злоумышленников.

Следует также отметить, что сама система виктимологической профилактики будет претворяться в жизнь через соответствующие субъекты виктимологической профилактики, что приводит к необходимости формирования межведомственных структурных связей как основы взаимодействия субъектов виктимологической профилактики.

3.2 Формирование межведомственных структурных связей в среде предупреждения мошенничества, совершаемого с использованием телекоммуникационного и компьютерного оборудования

В Конституции Российской Федерации[163] и других законодательных актах внушительное место отводится защите от противоправных посягательств на различные сферы общественных отношений, в том числе и экономическую безопасность. Это свидетельствует, с одной стороны, о серьезном внимании со стороны государства к охране общественных отношений, а с другой – о стремлении государства совместно с общественными объединениями вести борьбу с посягательствами на национальную безопасность всеми организационными, правовыми и другими средствами.

Следует отметить, что кредитно–банковский сектор, как важнейшая составляющая финансово–кредитной системы в экономике России, имеет без преувеличения системообразующее значение.

Во–первых, он предназначен для обеспечения бесперебойного функционирования платежной системы, проведения единой денежно–кредитной политики, организации и осуществления валютного регулирования и валютного

[163] Конституция Российской Федерации (принята всенародным голосованием 12.12.1993) (с учетом поправок, внесенных Законами РФ о поправках к Конституции РФ от 30.12.2008 № 6–ФКЗ, от 30.12.2008 № 7–ФКЗ, от 05.02.2014 № 2–ФКЗ, от 21.07.2014 № 11–ФКЗ) // Собрание законодательства РФ. 2014. № 31. Ст. 4398.

контроля. Во–вторых, банковский сектор выступает в качестве главного источника кредитования всех сфер экономики. Всестороннее обеспечение безопасности банковской деятельности является обязательным условием нормального функционирования экономики страны, поэтому входит в число важнейших функций государства. Противоправные посягательства на имущество граждан (денежные средства), совершаемые в процессе банковского обслуживания, наносят вред не только самим гражданам, но и кредитным организациям (финансовая устойчивость, защищенность, деловая репутация и подобное), а как следствие – нормальному функционированию денежного обращения и экономике государства в целом, что, собственно, ставит под угрозу национальную безопасность.

Учитывая уровень латентности таких видов деяний, как мошенничество, совершаемое с применением телекоммуникационного и компьютерного оборудования, степень криминализации данной сферы в настоящее время следует оценить как чрезвычайно высокую[164].

Совершая действия по обеспечению экономической безопасности, органы внутренних дел, как следствие, обеспечивают личную безопасность граждан, общественную безопасность, охрану собственности и общественного порядка, защиту прав и законных интересов граждан и организаций от преступных и иных противоправных посягательств, осуществляют предупреждение и пресечение преступлений, их расследование и раскрытие, а также розыск и установление виновных лиц и наоборот. То есть все то, для чего и они предназначены (ст. 1, 2 ФЗ «О полиции»)[165].

Будучи правоохранительными органами, органы внутренних дел осуществляют борьбу с преступлениями преимущественно уголовно–правовыми и оперативно–розыскными средствами. Административно–правовые средства борьбы с преступлениями рассматриваемого вида органы внутренних

[164] Астишина Т.В., Маркелова Е.В. Проблемы расследования преступлений, связанных с мошенническими действиями, совершенных с использованием средств сотовой телефонной связи // Вестник Казанского юридического института МВД России. 2014. № 2(16).
[165] Федеральный закон от 07.02.2011 № 3–ФЗ (ред. от 05.12.2017) «О полиции» // Собрание законодательства РФ. 2011. № 7. Ст. 900.

дел могут использовать лишь в процессе выявления и предупреждения преступлений такого рода.

При этом вопрос о роли органов внутренних дел в предупреждении экономических преступлений в отечественной науке является дискуссионным.

Так, В.Д. Ларичев и О.Ю. Исаев пишут: «анализ полномочий правоохранительных органов, в том числе органов внутренних дел, позволяет утверждать, что они не являются специализированными субъектами предупреждения преступлений против собственности, поскольку не обладают для этого никакими полномочиями». Эти органы «…предназначены в основном для выявления и раскрытия преступлений, а не для их предупреждения». В то же время эти авторы признают, что «они могут играть в предупреждении преступлений в сфере экономики вспомогательную роль, в частности, участвовать в проведении различных проверок совместно с контролирующими органами, проверить отдельных лиц на судимость и др.»[166].

Однако полностью согласиться с данным утверждением, по нашему мнению, невозможно, поскольку на органы внутренних дел возложены функции разработки и принятия в пределах своей компетенции мер по предупреждению преступлений, по выявлению и устранению причин и условий, способствующих их совершению (подп. 9 п. 12 Положения о Министерстве внутренних дел Российской Федерации, утвержденного Указом Президента РФ от 01 марта 2011 года № 248).

Содержание административной деятельности ОВД по профилактике преступлений, как представляется, включает в себя:

– прогнозирование криминогенной ситуации;

– определение задач и формирование целей профилактической деятельности;

---

[166] Ларичев В. Д., Исаев О. Ю. Понятие и характеристика основных субъектов предупреждения преступлений в сфере экономики в современных условиях // Общество и право. 2010. № 1. С. 202–206.

– получение, накопление и анализ информации о причинах и условиях, способствующих совершению противоправных посягательств;

– информационный обмен и оповещение;

– применение административно–правовых мер убеждения.

В большинстве случаев данная деятельность осуществляется в организационных, а не в правовых формах.

Безусловно, эти меры органы внутренних дел должны осуществлять в тесном взаимодействии с надзорным органом в банковской сфере – Банком России[167]. Именно надзорные органы осуществляют устранение криминогенных детерминант в результате непосредственного осуществления своих функций по контролю за определенными объектами и субъектами. Следует отметить также, что Центральный банк заключил соответствующие соглашения со всеми правоохранительными органами: с Генеральной прокуратурой, МВД, ФСБ и т. д. Однако, исходя из особенностей правового статуса Центрального банка (цели, задачи, функции, объем его прав и обязанностей, способы правового воздействия), механизмы профилактики, реализуемые, им предельно отличны от мер, применяемых вышеуказанными правоохранительными органами.

Таким образом, одной из основных проблем практического противодействия мошенничеству с использованием телекоммуникационного и компьютерного оборудования является отсутствие устойчивых межведомственных структурных связей. При этом в данном случае под межведомственными связями следует понимать такие методы и механизмы взаимодействия всех затронутых учреждений, при которых процессы нивелирования последствий совершенного противоправного деяния, блокирования путей совершения мошенничества, а также идентификации преступника и подобного будут реализованы в кратчайшие сроки.

---

[167] Майоров А.В. Виктимологическая модель противодействия преступности: монография. М.: Юрлит–информ, 2014. 224 с.

В пользу этого утверждения говорят и актуальные исследования отечественных ученых, посвященные вопросам преступлений в сфере электронной коммерции. Так, А.Ю. Чупрова[168] подчеркивает, что «борьба с преступностью, в том числе экономической, приносит весьма скромные плоды, поскольку ведется бессистемно. Государство должно выработать логически выстроенный и научно обоснованный комплекс мер законодательного, организационного, социального, морально–этического характера и настойчиво претворять их в жизнь, используя в том числе и принудительные меры воздействия».

В начале 2013 года расширенная рабочая группа экспертов, образованная при Министре внутренних дел Российской Федерации, подготовила предложения по дальнейшему реформированию органов внутренних дел Российской Федерации. Данный документ был обозначен как «Дорожная карта». В п.п. 5.6 данного документа было обозначено, что экспертам «представляется важным активизировать деятельность по противодействию киберпреступности. Следует разработать меры, в том числе законодательного плана, стимулирующие взаимодействие специализированных подразделений и операторов связи (сотовой связи, провайдеров и контент–провайдеров) в области обмена информацией и технологией; организовать целевую подготовку кадров в профильных гражданских вузах; шире использовать положения Федерального закона «Об оперативно–розыскной деятельности» в части организации этого вида деятельности; обратить особое внимание на международное взаимодействие в данной сфере»[169].

Следует отметить также Федеральный закон от 23.06.2016 № 182–ФЗ «Об основах системы профилактики правонарушений в Российской Федерации», который ввел единообразие и системность правового обеспечения профилактической деятельности.

---

[168] Чупрова А.Ю. Уголовно–правовые механизмы регулирования отношений в сфере электронной коммерции: дис. … д–ра юрид. наук. М., 2015. С. 479.

[169] Майоров А.В. Содержание системы виктимологического противодействия преступности // Юридическая наука и правоохранительная практика. 2017. № 3(41).

В нем определены основные принципы и направления профилактики правонарушений; разграничены полномочия органов госвласти и местного самоуправления в данной сфере. Закреплено право граждан и организаций участвовать в профилактике правонарушений.

Закон выделяет виды профилактики. Общая предполагает выявление и устранение причин и условий для правонарушений; повышение уровня правовой грамотности и правосознания граждан. На коррекцию поведения конкретного лица направлена индивидуальная профилактика[170].

Устанавливаются основания и порядок применения специальных мер профилактики правонарушений административного, уголовного, уголовно–процессуального, уголовно–исполнительного и оперативно–розыскного характера[171].

Под профилактикой понимается совокупность мер социального, правового, организационного, информационного и иного характера, направленных на выявление и устранение причин и условий, способствующих совершению правонарушений. Кроме того, профилактика подразумевает оказание воспитательного воздействия на лиц в целях недопущения совершения правонарушений или антиобщественного поведения[172]. При этом установлено, что антиобщественное поведение – это действия лица, не влекущие административную или уголовную ответственность, но нарушающие общепринятые нормы поведения и морали, права и законные интересы других лиц.

Осуществлять такую профилактику будут федеральные органы исполнительной власти, прокуратура, органы Следственного комитета РФ, а также региональные и местные органы (ч. 1 ст. 5 закона о профилактике правонарушений). Указанные органы будут разрабатывать соответствующие государственные и муниципальные программы, выявлять лиц, пострадавших от правонарушений, граждан, склонных к их совершению, проводить монито-

[170]Об основах системы профилактики правонарушений в Российской Федерации: федер. закон от 23.06.2016 № 182–ФЗ // Собр. законодательства РФ. 2016. № 26 (Часть I). Ст. 3851.
[171] Так же.
[172] Калашников О. Д. Виктимологическая профилактика – перспективное направление в борьбе с преступностью на современном этапе // Виктимология. 2017. № 1 (11).

ринг в сфере профилактики правонарушений и осуществлять иные полномочия[173].

Что интересно, такую профилактику смогут осуществлять и граждане, к примеру, посредством добровольного участия в мероприятиях по охране общественного порядка, содействия правоохранительным органам и т. д. (ч. 2 ст. 13 закона о профилактике правонарушений).

Указанным законом установлены два вида профилактики правонарушений (ст. 15 закона о профилактике правонарушений). Общая профилактика направлена на выявление и устранение причин, порождающих правонарушения, и условий, способствующих их совершению или облегчающих его. Также ее целью является повышение уровня правовой грамотности и развитие правосознания граждан. Второй вид, индивидуальная профилактика, будет использоваться уже относительно конкретных лиц, в частности, безнадзорных и беспризорных несовершеннолетних, граждан, отбывающих уголовное наказание, не связанное с лишением свободы, лиц, занимающихся бродяжничеством и попрошайничеством, и других. Указано, что такая профилактика предназначена для воспитательного воздействия на указанных лиц, устранение факторов, отрицательно влияющих на их поведение, а также для оказания помощи лицам, пострадавшим от правонарушений или рискующим стать таковыми.

Между тем в настоящее время вопросы взаимодействия правоохранительных органов и коммерческих структур, таких как банки, операторы связи (как мобильной, так и интернет–провайдеры) и прочие, остаются недостаточно проработанными с точки зрения рассматриваемой проблемы.

Как справедливо отмечает И.Р. Бегишев, ряд схем взаимодействия правоохранительных органов с такими коммерческими структурами, как интернет–провайдеры и операторы мобильной связи, а также при участии Федеральной службы по надзору в сфере связи, информационных технологий и

[173] Об основах системы профилактики правонарушений в Российской Федерации: федер. закон от 23.06.2016 № 182–ФЗ // Собр. законодательства РФ. 2016. № 26 (Часть I). Ст. 3851.

массовых коммуникаций (Роскомнадзор) «успешно применяется на практике в отношении:

а) материалов с порнографическими изображениями несовершеннолетних и (или) объявлений о привлечении несовершеннолетних в качестве исполнителей для участия в зрелищных мероприятиях порнографического характера;

б) информации о способах, методах разработки, изготовления и использования наркотических средств, психотропных веществ и их прекурсоров, местах приобретения таких средств, веществ и их прекурсоров, о способах и местах культивирования наркосодержащих растений;

в) информации о способах совершения самоубийства, а также призывов к совершению самоубийства; <…>«[174].

Следует отметить, что для различных организаций характерны разные подходы к вопросам управления рисками, связанными с мошенничеством, а также разная степень интенсивности соответствующих мер. Кроме того, мошенничество может принимать весьма разнообразные формы, а масштабы мошеннических действий, совершаемых сотрудниками и (или) сторонними организациями и физическими лицами, значительно различаются в зависимости от того, о какой именно организации идет речь.

Так, например, рассматривая вопросы взаимодействия правоохранителей с банковским сектором можно отметить следующее.

Современные банковские учреждения являются относительно закрытыми для контроля со стороны государства, в связи с чем в случае выявления признаков преступлений руководители банков обращаются за помощью в правоохранительные органы лишь в единичных случаях. Данное обстоятельство стало объективным условием выявления и документирования мошенничеств, совершаемых в сфере функционирования электронных расчетов, сотрудниками служб безопасности банков. Такое положение вещей вполне

[174] Бегишев И.Р. Некоторые вопросы противодействия мошенничеству в сфере компьютерной информации // Вестник Казанского юридического института МВД России. 2016. № 3(25). С. 112–117.

обоснованно, поскольку нормативные документы большинства банковских учреждений РФ закрепляют такие обязанности служб банковской безопасности, как:

– выявление признаков подготавливаемых и совершенных преступлений, применение мер по их предупреждению и прекращению; подготовка материалов в правоохранительные органы для решения вопроса о возбуждении уголовного дела;

– участие в предварительном расследовании уголовных дел;

– направление правоохранительным органам информации, имеющей отношение к расследованию;

– применение в пределах компетенции мер по возмещению причиненного банку вреда.

Среди прочего такие обязанности были закреплены в Приказе МВД России от 04.01.1996 № 4 «О реализации Соглашения между МВД России и Ассоциацией российских банков». Однако указанный Приказ утратил силу на основании Приказа МВД России от 26.02.2008 № 176 «О признании утратившим силу Приказа МВД России от 4 января 1996 г. № 4». Таким образом, отсутствие в законодательстве прямых предписаний по выполнению вышеперечисленных обязанностей приводит к тому, что на практике в большинстве случаев они не выполняются.

Между тем данная ситуация является одной из основных причин столь высокого уровня латентности рассматриваемого вида деяний[175].

Как правило, в процессе «внутренних» проверок нарушения порядка осуществления банковских операций сотрудникам служб безопасности банков удается выявить приблизительно 10–15% мошенничеств, совершенных уполномоченными сотрудниками банков. Между тем, как справедливо указывает А.Ф. Волобуев, деятельность банков как структур рыночной экономики во многих аспектах связана с сохранением коммерческой (банковской)

[175] Якимова Е.Д. Виктимологическая профилактика преступности: содержание и задачи // Виктимология. 2014. № 1 (1). С. 55–58.

тайны. Поэтому различного рода имущественные злоупотребления персонала банка становятся известными правоохранительным органам только тогда, когда на это даст разрешение руководство учреждения. Следует при этом отметить, что сотрудники банков, в частности сотрудники «младшего звена», занятые в работе с клиентами в операционных залах, регулярно фигурируют как лица, незаконно получающие и передающие (зачастую на возмездной основе) сведения, содержащиеся на банковских картах граждан.

Более тесное взаимодействие банков с органами предварительного расследования при этом могло бы значительно ускорить процесс расследования преступлений данного вида, сделать его более эффективным. Результаты опроса, проведенного В.А. Финагеевым, показали, что совместная деятельность сотрудников банковской безопасности и следователей целесообразна в случае:[176]

– предоставления службами безопасности правоохранительным органам материалов для решения вопроса о возбуждении уголовного дела (88 и 92 %);

– доступа в помещения, к документам и техническим средствам банка, необходимым для проведения следственных действий, и оказания помощи в их применении (51 и 76%);

– налаживания связей и получения информации от иных банков по вопросам незаконного перечисления средств (42 и 68%);

– сбора и предоставления фактических данных, имеющих отношение к процессу расследования, с целью получения новых доказательств (74 и 92%);

– участия в розыске лиц, посягавших на интересы банка или подозреваемых в их совершении, а также применения в пределах компетенции мер по возмещению причиненного ущерба (35 и 44 %).

Указанные данные свидетельствуют об осознании сотрудниками–практиками, как со стороны правоохранительных органов, так и со стороны

[176] Финагеев В.А. Проблемы взаимодействия правоохранительных органов и подразделений банковской безопасности в выявлении и расследовании преступлений // Таможенное дело. 2013. № 2(86). С. 264–270.

банковских учреждений, необходимости разрешения отмеченных вопросов взаимодействия и закрепления их на законодательном уровне.

Ряд отечественных исследователей[177] в целях разрешения возникающих проблем взаимодействия правоохранительных органов с банковскими учреждениями, предлагают установить исчерпывающий перечень органов государственной власти, имеющих право получения из банков сведений, составляющих банковскую тайну, а также сроки предоставления информации, предусмотрев возможность их увеличения по просьбе банков. Кроме того, с целью сокращения временных рамок исполнения запросов правоохранительных органов, а также устранения необходимости нагромождения уголовного дела лишней информацией рекомендуется предоставить банкам возможность передавать сведения, составляющие банковскую тайну, на электронных носителях с заверением ее подлинности в сопроводительных письмах.

Следует также отметить, что такие учреждения, как операторы связи (как мобильной связи, так и интернет–провайдеры), а также организации, деятельность которых связана с так называемыми «виртуальными деньгами», также «неохотно идут на контакт» с правоохранительными органами.

Это порождает ситуацию, при которой само пострадавшее лицо вынуждено в ущерб прочим собственным интересам самостоятельно запрашивать и получать информацию от каждой из указанных структур. Однако в этом случае правоохранители получают лишь объем данных, ограниченный полем деятельности, либо контакты потерпевшего лица. Вопросы идентификации злоумышленника либо блокировки счетов в различных системах остаются отложенными на неопределенный срок. Во избежание «затягивания» проблемной ситуации в объеме предыдущего параграфа нами уже была указана потребность адресного обращения в соответствующие инстанции со стороны граждан. Подобный под-

---

[177] См. например: Матвеев А.В., Федоренко В.И. Массовая виктимность как аспект социальной напряженности в обществе // XXXX неделя науки СПбГПУ: материалы Международной научно–практической конференции. Ч. XVIII. СПб.: Изд–во Политехн. ун–та, 2011. С. 72–75.; Майоров А.В. О концепции виктимологического противодействия преступности // Юридическая наука и правоохранительная практика. 2015. № 4(34). С. 50–57.

ход, по нашему мнению, не является объективно исчерпывающим проблемную ситуацию и требует дальнейшей проработки.

Ряд исследователей в настоящее время сходятся на идее о необходимости законодательного закрепления методов и механизмов взаимодействия правоохранительных органов с вышеобозначенными коммерческими структурами, четкой регламентации сроков предоставления данной информации и т. д.

По мнению автора, данный подход имеет рациональное основание, однако не учитывает различных аспектов социально–экономического взаимодействия субъектов российской экономики, ввиду которых столь радикальное влияние на права одних из крупнейших по своей структуре и финансовому обороту предприятий вызовет ряд значительных по своим масштабам негативных последствий[178].

При этом в отечественной практике существуют примеры разрешения подобных ситуаций, в которых требуется урегулировать вопросы общественных отношений в части интересов коммерческого сектора, государственных структур и неопределенного круга лиц аналогичными, но менее «жесткими» методами. Так, например, в марте 2015 года ОАО «НК «Роснефть» и Федеральная антимонопольная служба России согласовали Стандарт, регламентирующий принципы ценообразования и порядок реализации компанией моторного топлива на внутреннем рынке РФ. Указанному Стандарту в настоящее время следуют все крупнейшие предприятия данного сектора экономики, а сам факт его принятия позволил урегулировать проблемы взаимодействия предприятий нефтеперерабатывающего комплекса и ФАС РФ в вопросах, вызывающих некоторый общественный резонанс уже более десяти лет.

По аналогии с данным примером в настоящее время для разрешения вопросов взаимодействия правоохранительных органов и коммерческого сектора требуется разработка некоторого Регламента взаимодействия МВД, предприятий финансового сектора и операторов связи (далее – Регламент).

---

[178] Камко А.С. Виктимологическая профилактика преступлений в сфере безналичного обслуживания в России: состояние и перспективы развития, опыт // Библиотека криминалиста. 2016. № 6.

В рамках данного Регламента требуется определить:

– шаблон запроса на предоставление информации правоохранительным органам со стороны предприятий коммерческого сектора;

– сроки предоставления информации представителями коммерческого сектора по запросу из правоохранительных органов;

– формат предоставления данных (на бумажном или электронном носители);

– способы заверения подлинности передаваемых данных;

– иные вопросы, относящиеся к полю деятельности правоохранительных органов.

Следует отметить, что обозначенный Регламент может являться частью некоторого Соглашения между всеми заинтересованными сторонами либо быть самостоятельным нормативным актом.

Предметом соглашения сторон в данном случае будет являться информационное взаимодействие и координация усилий по предотвращению случаев мошенничества с использованием телекоммуникационного и компьютерного оборудования (включая, но не ограничиваясь системами ДБО; оплаты услуг путем отправки смс–сообщений на «короткие номера»; оформление незаконных «телефонных подписок»; мошенничество с применением банковских карт и т. д.) и иных правонарушений в сфере обеспечения имущественных прав и законных интересов граждан.

Целями соглашения будут являться:

– предотвращение случаев мошенничества, минимизации ущерба и локализация последствий от неправомерных и недобросовестных действий сотрудников коммерческих учреждений и третьих лиц;

– предотвращения выплаты денежных средств, а также оплаты товаров и услуг по средствам поддельных и фальсифицированных платежных карт;

– пресечение сделок с похищенным имуществом (банковскими картами, телекоммуникационным оборудованием) и имуществом, находящимся в розыске;

– выявление похищенного имущества граждан;

– профилактика мошенничества со стороны работников организаций–участников соглашения.

В рамках такового соглашения стороны–участники будут иметь обязательства:

Коммерческие структуры:

– обеспечивать материально и организационно информационно–аналитическую работу по выявлению случаев и признаков мошенничества со стороны злоумышленников в пределах своей компетенции;

– обрабатывать запросы сотрудников и представителей ОВД в соответствии с технологией и регламентом информационного взаимодействия, определенными в ходе обсуждения и анализа технических возможностей, а также рациональных сроков исполнения обязательств сторон при согласовании проекта нормативного документа;

– использовать внешние источники информации и банки данных других ведомств в целях повышения эффективности информационного взаимодействия, при условии не нарушения прав и законных интересов третьей стороны;

– оказывать содействие сотрудникам, либо уполномоченным представителям ОВД в получении иной дополнительной информации о запрашиваемых объектах в интересах других организаций, подписавших аналогичное Соглашение, а также в интересах граждан (физических лиц), имущественные права которых были нарушены при совершении преступления.

Органы внутренних дел:

– оказывать содействие и методическую помощь организациям–участникам соглашения по вопросам выявления, профилактики и противодей-

ствия мошенничеству, совершаемому с использованием телекоммуникационного оборудования и компьютерных сетей;

– привлекать через заключение аналогичного Соглашения к участию в формировании системы профилактики и противодействия иные организации вне зависимости от формы собственности, при условии, что деятельность (практически осуществляемая или информационного характера) данных организаций будет объективно полезна для функционирования указанной системы;

– обеспечивать непрерывность информационного взаимодействия и его инструктивно–методического сопровождения путем проведения информационно–практических мероприятий либо участия сотрудников правоохранительных органов в таковых по запросу от сторон–участников соглашения;

– периодически, при наличии возможности, направлять в адрес организаций – участников Соглашения в виде информационных записок и методических рекомендаций обобщенные материалы об имеющемся положительном опыте работы по профилактике правонарушений и проблемным вопросам защиты от мошенничества, а также событиях и фактах, требующих оперативного реагирования.

Следует также отметить, что при разработке и согласовании подобного соглашения требуется учитывать существующую отечественную практику по вопросам информационного взаимодействия предприятий коммерческого сектора с правоохранительными органами и структурами государственной безопасности. Так, например, в соответствии с Постановлением Правительства РФ от 27.08.2005 № 538 «Об утверждении Правил взаимодействия операторов связи с уполномоченными государственными органами, осуществляющими оперативно–розыскную деятельность» одним из этапов определено предоставление оператором связи УФСБ по субъекту РФ – местонахождению сети связи баз данных (далее – БД) об абонентах, оказанных услугах связи (в том числе о соединениях, трафике и платежах абонентов). При этом информация предоставляется Управлению путем осуществления круглосуточного удаленного доступа к БД и хранится в течение трех лет.

Таким образом, существует возможность игнорировать отказ от участия в предполагаемом соглашении со стороны операторов связи при условии, что будет определен порядок предоставления доступа к имеющимся у них БД через технические возможности, либо по запросу о предоставлении информации к УФСБ по субъекту РФ – местонахождению сети связи.

Необходимо также отметить, что вовлечение коммерческих банков в систему профилактики и предупреждения рассматриваемого вида деяний необходимо строить из понимания следующей концепции, содержание которой следует доносить до представителей кредитной организации непосредственно или через банковские сообщества (союзы, ассоциации и объединения), поскольку они могут формировать политику поведения не одного конкретного банка, а всех банков, включенных в ту или иную ассоциацию.

Включение в систему предупреждения и профилактики банка грозит ему дополнительными затратами времени, денег и прочих ресурсов, поэтому банки не часто соглашаются на сотрудничество с органами внутренних дел. Для того чтобы получить необходимый результат, следует понимать, что механизм обеспечения экономической безопасности кредитной организации зависит в большей степени от самой кредитной организации, профилактика и предупреждение мошенничества прицельно подрывают репутацию банка и его финансовую устойчивость, что сказывается на жизнеспособности конкретного бизнеса.

Базовым элементом обеспечения экономической безопасности кредитной организации является его финансовая стабильность как результат системы институционально–управленческих, организационно–технических и информационных мер, направленных на обеспечение воспроизводственно–устойчивого режима функционирования банка, защиту его прав и интересов, рост уставного капитала, повышение ликвидности активов, сохранность финансовых и материальных ценностей, а также на обеспечение возвратности размещенных денежных средств. А фактически – это готовность кредитной организации противостоять различным угрозам, которые могут произойти.

Таким образом, обеспечение безопасности кредитной организации представляется и элементом, и основой его деятельности. Состояние защищенности представляет собой умение и способность кредитной организации надежно противостоять в том числе любым попыткам криминальных структур или недобросовестных конкурентов нанести ущерб законным интересам банка.

Таким образом, при заключении органами внутренних дел соглашений с коммерческими банками о взаимодействии по вопросам профилактики и предупреждения мошенничества, совершаемого с использованием телекоммуникационного оборудования и компьютерных сетей, рекомендуется делать упор на то, что при всех самых смелых представлениях об организации безопасности банка предотвращению противоправных посягательств банк без взаимодействия с правоохранительными органами (прежде всего полицией) противостоять не сможет.

Логично определить, что взаимодействие кредитных организаций и органов внутренних дел по вопросам профилактики и предупреждения мошенничества должны строиться на основе следующих принципов:

– законности;

– соблюдения и уважение прав и свобод человека и гражданина;

– открытости, публичности и доверия;

– согласованности действий и взаимного информирования;

– использования достижений науки и техники, современных технологий и информационных систем;

– добросовестности, надежности и взаимной ответственности.

Основными направлениями взаимодействия кредитных организаций и органов внутренних дел должны являться:

1) непосредственно профилактика и предупреждение:

– проведение обязательной разъяснительной работы сотрудниками банков, которые непосредственно обслуживают клиентов с момента первого обращения и в повседневной работе с уже имеющимися клиентами. Данная работа должна заключаться в разъяснении клиенту:

а) возможностей (в том числе и технических) систем дистанционного банковского обслуживания (в том числе банкоматов и терминалов);

б) инструкции и правил работы систем дистанционного банковского обслуживания (включая банкоматы и терминалы);

в) сведений об основных способах совершения хищений, о признаках того, что возможно клиент банка находится именно в той ситуации, когда в отношении него может быть совершено противоправное деяние (например, звонки или электронные почтовые сообщения с просьбами вернуть ошибочно перечисленные денежные средства или о блокировании банковской карты, некорректно работающая интернет–страница банка, необычно прикрепленная или не стандартная клавиатура в банкомате или платежном терминале, а так же отсутствие на них идентифицирующих номеров и подобное), и правил безопасного поведения в различных ситуациях;

г) о возможности круглосуточного обращения в банк при возникновении необходимости проверить полномочия лиц, представляющихся сотрудниками банка, реальность предлагаемых сделок, уточнить состояние счетов и движение денежных средств по ним (предоставление контактных телефонов специалистов, идентификационных номеров или паролей и т. д.);

д) необходимости немедленного сообщения не только в кредитную организацию, но и органы внутренних дел (полицию) сведений о том, что возможно клиент банка находится именно в той ситуации, когда в отношении него или иных лиц может быть совершено противоправное деяние, о признаках, которые могут способствовать возможности совершения преступления.

В определенной степени в практике реализации потребуется совместная разработка информационных материалов, содержащих сведения, описанные в вышеуказанных пунктах.

Данному направлению следует уделять большее внимание, поскольку клиент банка, как правило, в момент общения с банковским сотрудником находится в психофизическом состоянии, характеризуемом повышенной степенью доверия и впечатлительностью, а соответственно внушаемостью (особенно те

лица, которые являются основной категорией: престарелые, молодежь, лица, чей образ жизни далек от «городского», лица с ограниченными возможностями или страдающие определенными заболеваниями, лица с низкой социальной адаптацией и подобные), что может привести к формированию в человеке бдительности и значимости своей гражданской позиции по содействию полиции.

Следует отметить, что эффективность данного подхода имеет место только при условии, что клиент банка получает не просто описанную информацию в виде памятки, инструкции на бумажном носителе (что в целях профилактики и предупреждения является необходимым!), но и соответствующие разъяснения устно.

– оповещение населения:

а) размещение плакатов, стендов в помещениях кредитных организациях с необходимой информацией;

б) освещение в средствах массовой информации о способах совершения преступлений, признаках и должном порядке поведения (данное мероприятие может осуществляться банками и органами внутренних дел как отдельно друг от друга, так и совместно);

в) приглашение сотрудников банков к участию в проводимых органами внутренних дел (полиции) и их должностными лицами мероприятиях: брифинги, совещания, обсуждения проектов нормативных и нормативных правовых актов, публичные слушанья, мероприятия, проводимые сотрудниками (участковыми уполномоченными полиции, инспекторами ПДН при проведении профилактических бесед со школьниками, студентами, воспитанниками, престарелыми и другими, а также при регулярных отчетах перед населением);

2) содействие службам безопасности кредитных организаций в реализации их полномочий.

Безусловно, речь идет лишь о противодействии угрозам, реагирование на которые входит в компетенцию соответствующих государственных органов.

Такое содействие, на наш взгляд, может осуществляться в формах:

– участия в обучении персонала выявлению признаков противоправных посягательств и действиям по их предупреждению и пресечению;

– осуществления правового консультирования по вопросам выявления признаков и защите от противоправных посягательств, в том числе и в экстренном режиме;

– рассылки рекомендаций по защите от выявленных угроз;

– в проверки защищенности информационных систем и др.;

– защиты коммерческих банков от проникновения организованных преступных групп в их среду;

– разработки и внедрения специальных технологий по выявлению возможностей и фактов незаконного вмешательства злоумышленников в телекоммуникационные банковские системы, компьютерные программы, дающие возможность клиенту банка дистанционно (используя различные каналы связи) пользоваться и распоряжаться собственными денежными средствами, находящимися на банковских счетах; технологий, позволяющих проведение анализа информации о проводимых операциях, вызывающих подозрения; технологий и систем, значительно повышающих безопасность и защищенность систем дистанционного банковского обслуживания;

3) оперативная обработка, анализ и предоставление органам внутренних дел информации о состоянии защищенности и безопасности банка (систем дистанционного банковского обслуживания, в том числе банкоматов и терминалов), на предмет выявления признаков противоправных посягательств и иного нарушения законодательства, а также экстренное реагирование первых на полученные сведения;

4) разработка совместных предложений по совершенствованию правовой основы обеспечения банковской безопасности в интересах укрепления законности и обеспечения безопасности в кредитно–финансовой системе страны.

Таким образом, следует сделать вывод о взаимной заинтересованности всех потенциальных участников процесса межведомственного информационного взаимодействия в части профилактики и противодействия мошенничеству с

использованием телекоммуникационных и компьютерных сетей, а также о значительном потенциале реализации мер нормативного закрепления условий данного взаимодействия.

ЗАКЛЮЧЕНИЕ

Итоги выполненного исследования. В ходе проведенного криминологического исследования можно сформулировать следующие выводы:

Несмотря на международный характер рассматриваемого вида правонарушений и сущностное отсутствие ограничений в географии совершения правонарушений, в нашей стране мошенничество с использованием телекоммуникационного и компьютерного оборудования имеет собственные особенности, обусловленные, в первую очередь, менталитетом населения. Так, если для зарубежного преступного сообщества характерной чертой является некоторая обособленность лиц, совершающих подобного рода правонарушения, то для отечественного сегмента, напротив, характерной чертой является объединение в преступные группы.

Проводя анализ «портрета» личности мошенника, совершающего преступление с использованием телекоммуникационного и компьютерного оборудования, нами было определено отсутствие конкретной системы классификации правонарушителей данной категории, между тем, учитывая специфические черты личности этих преступников, подобная система является необходимой для достижения положительных результатов в системе профилактики и противодействия мошенничествам заявленного вида. Автором была разработана собственная система классификации преступников данной категории, а также приведен пример корректного ее применения.

Проводя анализ зарубежного опыта профилактики и пресечения мошенничества с применением телекоммуникационных и компьютерных сетей, автором помимо выводов об определенной эффективности отдельных систем уголовного законодательства было определено, что основным механизмом снижения числа самих преступных эпизодов, а также объема причиняемого ими материального ущерба является система виктимологической профилактики.

В ходе проведенного исследования были также обобщены и сформулированы основные концептуальные принципы системы виктимологической профилактики преступлений рассматриваемого вида, практическая потребность в которой в настоящее время неоспоримо велика.

Кроме того, было определено, что потенциал эффективности взаимодействия ОВД и финансово-кредитных организаций, имеющий значительные по своим масштабам перспективы в части выявления, пресечения, раскрытия, а также профилактики и предупреждения рассматриваемого вида преступлений к настоящему времени практически не реализован.

Перечень причин в данном случае достаточно значителен, хоть и не имеет в себе новых для нашей страны положений. Среди них основными являются: недостаточность ресурсов, выделяемых на формирование необходимых для подобного взаимодействия компьютерных сетей и оборудования (в данном случае речь идет о защищенных каналах передачи данных, для создания которых требуются различные дополнительные технические средства, такие как криптомаршрутизаторы и т.д.); недостаточный уровень правовой культуры сотрудников финансово-кредитных учреждений (свойственный отдельным гражданам правовой инфантилизм и нигилизм); чрезмерная загруженность представителей обеих сторон и т.д.

Вместе с тем предпосылки такого взаимодействия имеются. К ним относятся:

– значительная потребность ОВД в своевременном (оперативном) получение различных сведений, которые должны служить основанием для начала оперативно-следственных мероприятий, либо же в существенной степени влияющих на результативность этих мероприятий;

– наличие у представителей коммерческого сектора потребности в защите своих интересов, обусловленная как негативными финансовыми последствиями для организаций кредитно-финансового сектора, вызванными противоправными действиями рассматриваемого вида, так и значительными

репутационными рисками, что обусловлено уже субъективным суждением граждан, ставших непосредственными жертвами преступления;

– происходящие в нашей стране реформы привели к отмене ряда ранее действовавших нормативно-правовых актов, регулировавших отдельные аспекты взаимодействия организаций кредитно-финансового сектора и ОВД, что стало значительным пробелом в системе административно-правового регулирования рассматриваемого вида взаимодействия;

Рекомендации. На основе вышепредставленных результатов исследования следует определить следующие рекомендации:

– внедрить предлагаемую систему классификации лиц, совершивших мошенничество с использованием телекоммуникационного и компьютерного оборудования, в повседневную деятельность правоохранительных органов и судебной системы с целью повышения эффективности системы предупреждения соответствующего вида противоправных деяний;

– внедрить в деятельность органов внутренних дел комплекс мер виктимологической профилактики в контексте предупреждения мошенничества, совершаемого с использованием телекоммуникационного и компьютерного оборудования;

– сформировать единый механизм взаимодействия правоохранительных органов, коммерческих структур и гражданского общества в контексте системы предупреждения и противодействия мошенничеству, совершаемому с использованием телекоммуникационного и компьютерного оборудования.

Перспективы дальнейшей разработки темы исследования представляют значительный потенциал для развития как теории криминологической науки, так и практики предупреждения рассматриваемого вида противоправных деяний корыстной направленности. В определенной степени приоритетными представляются направления виктимологической профилактики и исследования личности преступника. Соотношение этих двух компонент

позволит в должной степени обеспечить экономическую безопасность как отдельных граждан и организаций, так и всего государства.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Конституция Российской Федерации (принята всенародным голосованием 12.12.1993) (с учетом поправок, внесенных Законами РФ о поправках к Конституции РФ от 30.12.2008 № 6–ФКЗ, от 30.12.2008 № 7–ФКЗ, от 05.02.2014 № 2–ФКЗ, от 21.07.2014 № 11–ФКЗ) // Собрание законодательства РФ. – 2014. – № 31. – Ст. 4398.

2. Налоговый кодекс Российской Федерации (часть первая) от 31 июля 1998 № 146–ФЗ (ред. от 28.12.2013) // Собрание законодательства РФ. – 1998. – № 31. – Ст. 3824.

3. Уголовный кодекс Российской Федерации от 13 июня 1996 № 63–ФЗ (ред. от 10 октября 2015) // Собрание законодательства РФ. – 1996. – № 25. – Ст. 2954.

4. Гражданский кодекс Российской Федерации (часть первая) от 30.11.1994 № 51–ФЗ (ред. от 31.12.2014)// Собрание законодательства РФ. – 1994. – № 32. – Ст. 3301.

5. Федеральный закон от 02 декабря 1990 № 395–1 (ред. от 30 сентября 2013) «О банках и банковской деятельности»// Собрание законодательства РФ. – 1996. – №6. – Ст. 492.

6. Федеральный закон от 07 февраля 2011 № 3–ФЗ (ред. от 05.12.2017) «О полиции» // Собрание законодательства РФ. – 2011. – № 7. – Ст. 900.

7. Федеральный закон от 21 июля 2014 № 242–ФЗ (ред. от 31 декабря 2014) «О внесении изменений в отдельные законодательные акты Российской Федерации в части уточнения порядка обработки персональных данных в информационно–телекоммуникационных сетях» // Собрание законодательства РФ. – 2014. – № 30 (Часть I). – Ст. 4243.

8. Федеральный закон от 23 июня 2016 № 182–ФЗ «Об основах системы профилактики правонарушений в Российской Федерации» // Собрание законодательства РФ. – 2016. – № 26 (Часть I). – Ст. 3851.

9. Федеральный закон от 27 июля 2006 № 149–ФЗ (ред. от 21 июля 2014) «Об информации, информационных технологиях и о защите информации»// Собрание законодательства РФ. – 2006. – № 31 (1 ч.). – Ст. 3448.

10. Федеральный закон от 27 июля 2006 № 152–ФЗ (ред. от 21 июля 2014) «О персональных данных»// Собрание законодательства РФ. – 2006. – № 31 (1 ч.). – Ст. 3451.

11. Федеральный закон от 27 июня 2011 № 161–ФЗ (ред. от 25декабря 2012) «О национальной платежной системе» // Собрание законодательства РФ. – 2011. – № 27. – Ст. 3872.

12. Федеральный закон от 29 декабря 2006 № 244–ФЗ (ред. от 23 июля 2013) «О государственном регулировании деятельности по организации и проведению азартных игр и о внесении изменений в некоторые законодательные акты Российской Федерации»// Собрание законодательства РФ. – 2007. – № 1(1ч.). – Ст. 7.

13. Федеральный закон от 29 ноября 2012 № 207–ФЗ «О внесении изменений в Уголовный кодекс Российской Федерации и отдельные законодательные акты Российской Федерации»// Собрание законодательства РФ. – .2012. – № 49. – Ст. 6752.

14. Федеральный закон от 29.12.2006 № 244–ФЗ (ред. от 23.07.2013) «О государственном регулировании деятельности по организации и проведению азартных игр и о внесении изменений в некоторые законодательные акты Российской Федерации» // Российская газета. – 2006. – № 297.

15. Федеральный закон от 7 июля 2003 № 126–ФЗ (ред. от 21 июля 2014, с изм. от 01 декабря 2014) «О связи» // Собрание законодательства РФ. – 2003. – № 28. – Ст. 2895.

16. Алексеев, А. И. Криминология: Курс лекций / А. И. Алексеев. – М.: Щит–М, 1999. – С. 123.

17. Анапольская, А. И. Деятельность преступных организаций, осуществляющих «отмывание» денежных средств с использованием электронных расчетных операций / А. И. Анапольская // Общественная безопасность как уголовно–правовая и криминологическая категория: материалы Международной научно–практической конференции. Тамбов, 2015. – С. 52–56.

18. Анапольская, А. И. Использование оперативно–технических средств подразделениями уголовного розыска в процессе раскрытия хищений денежных средств в сфере электронных расчетов / А. И. Анапольская // Научные перспективы XXI века. Достижения и перспективы нового столетия: материалы 5 Международной научно–практической конференции. – 2014. – № 5. – С. 96– 100.

19. Анапольская, А. И. Порядок взаимодействия правоохранительных органов с банковскими учреждениями при расследовании мошенничеств, совершаемых в сфере функционирования электронных расчетов / А. И. Анапольская // Вестник ТГУ. – 2015. – № 5 (145). – С.221–224.

20. Антропцева, И. О. Обеспечение стабильности и развития национальной платежной системы Центральным Банком Российской Федерации (Национальная платежная система) / И. О. Антропцева // Банковское право. – 2011. – № 4. – С. 25–29.

21. Аракелян, К. Н. Виктимология как отрасль юридической психологии: экскурс в историю возникновения / К. Н. Аракелян // PsyJournals. – 2011. – № 2. – С. 4–8.

22. Астафьев, К. В. Виктимологический аспект мошенничества (уголовно–правовое и криминологическое исследование) : дис. ... канд. юрид. наук. / К. В. Астафьев. – Казань, 2007. – 267 с.

23. Астишина, Т. В. Проблемы расследования преступлений, связанных с мошенническими действиями, совершенных с использованием средств сотовой телефонной связи / Т. В. Астишина, Е. В. Маркелова // Вестник Казанского юридического института МВД России. – 2014. – № 2 (16).

24. Ахмедшина, Н. В. Криминологическая виктимология: современное состояние и перспективы развития : дис. … канд. юрид. наук / Н. В. Ахмедшина. М, 2010.

25. Бабаева, Ю. Д. Интернет: воздействие на личность / Ю. Д. Бабаева, А. Е. Войскунский, О. В. Смыслова [Электронный ресурс] // Режим доступа: http://www.relarn.ru/human/pers.html.

26. Банкоматное мошенничество в России: цифры, факты и комментарии. [Электронный ресурс] // Режим доступа: ПЛАС. URL:http://pda.plusworld.ru/joumal_1/2012/335/2978

27. Бегишев, И. Р. Некоторые вопросы противодействия мошенничеству в сфере компьютерной информации / И. Р. Бегишев // Вестник Казанского юридического института МВД России. – 2016. – № 3(25). – С. 112–117.

28. Белозерцев, С. М. Профилактика мошенничеств с использованием мобильных устройств и банковских карт в Иркутской области: проблемы и пути их решения / С. М. Белозерцев // Вестник Восточно–Сибирского института МВД России. – 2015. – № 4 (75). – С. 9–14.

29. Бельская, З. В. Тесты интеллекта в диагностической практике психолога / З. В. Бельская // Актуальные вопросы современной психологии: материалы III Междунар. науч. конф. (г. Челябинск, февраль 2015 г.). – Челябинск: Два комсомольца, 2015. – С. 77–80.

30. Березина, М. П. Карточные инновации в России: от истоков к мегапроекту УЭК (Аналитика. Платежные расчеты и системы) / М. П. Березина // Банковское дело. – 2011. – № 11. – С. 44–47.

31. Березуцкая, А. Г. Современные проблемы безопасности пластиковых карт в платежной системе России / А. Г. Березуцкая, А. Е. Яблонская // ЭПП. – 2016. – № 3. – С.195–202.

32. Боголюбова, Т. А. Предупреждение преступности: современный взгляд на проблему / Т. А. Боголюбова // Вестник Академии Генеральной прокуратуры Российской Федерации. – 2014. – № 4 (42). – С. 112–116.

33. Боголюбова, Т. А. Современные проблемы теории предупреждения преступности в российском обществе / Т. А. Боголюбова // Актуальные проблемы предупреждения преступности на современном этапе развития российского общества : сборник материалов круглого стола, Москва, 21 мая 2014 г. / под ред. Т.Л. Козлова. – М. : Акад. Ген. прокуратуры Рос. Федерации, 2014. – С. 14–16.

34. Бойцов, А. И. Преступления против собственности: учебное пособие / А.И. Бойцов. − СПб., Юридический центр ПРЕСС. 2002. − 775 с.

35. Бумаженко, Н. И. Виктимология / Н. И. Бумаженко. – Витебск: ВГУ им. П.М. Машерова, 2010.

36. Быстрова, Ю. В. Причины и условия распространения легализации (отмывания) преступных доходов в России / Ю. В. Быстрова // Научный портал МВД России. – 2010. – № 1. – С. 53–56.

37. Быстрова, Ю. В. Система предупреждения легализации (отмывания) денежных средств или иного имущества, приобретенных преступным путем в Российской Федерации : автореф. дис. ... канд. юрид. наук / Ю. В. Быстрова. – М., 2010. – 20 с.

38. Варчук, Т. В. Виктимология / Т. В. Варчук, К. В. Вишневецкий. – М.: Закон и право, 2012. – С. 184.

39. Варчук, Т. В. Виктимология: учеб. пособие / под ред. С.Я. Лебедева. – М.: ЮНИТИ–ДАНА, 2009. – 263 с.

40. Вехов, В. Б. Хакеры, крэкеры, фрикеры,кардеры – кто они? / В. Б. Вехов // Информационно–методический журнал «Защита информации. Инсайд» – 2005. – № 5.

41. Вишневецкий, К. В. Зарубежный опыт виктимологической профилактики преступлений и перспективы ее развития в России / К. В. Вишневецкий // Современное право. – 2008. – № 2.

42. Вишневецкий, К. В. Криминогенная виктимизация социальных групп в современном обществе: монография / К.В. Вишневецкий. – М.: ЮНИТИ–ДАНА, 2010. – 295 с.

43. Вишневецкий, К. В. Место виктимологической теории в криминологии / К. В. Вишневецкий // Наука и практика. – 2011. – №3 (48).

44. Волеводз, А. Г. Конвенция о киберпреступности: новации правового регулирования / А. Г. Волеводз // Правовые вопросы связи. – 2007. – № 2. – С. 17–25.

45. Волеводз, А. Г. Противодействие компьютерным преступлениям: правовые основы международного сотрудничества: монография / А. Г. Волеводз. − М.: Юрлитинформ, 2001. − 496 с.

46. Волеводз, А. Г. Следы преступлений, совершаемых в компьютерных сетях / А. Г. Волеводз // Российский следователь. – 2002. – № 1. – С. 4–12.

47. Воронин, Ю. А. Виктимная безопасность: терминологическая интерпретация / Ю. А. Воронин, А. В. Майоров // Криминологический журнал БГУЭП. – 2014. – № 1. – С. 43–48.

48. Воронин, Ю. А. Теоретические основы формирования системы противодействия преступности в России / Ю. А. Воронин, А. В. Майоров // Всероссийский криминологический журнал. – 2013. – № 1. – С. 7–16.

49. Гаджиев, М. С. Криминологический анализ преступности в сфере компьютерной информации (по материалам Республики Дагестан): дис.... канд. юрид. наук. / М. С. Гаджиев. – Махачкала, 2004. – С. 81–85.

50. Герасимов, С. И. Концептуальные основы и научно–практические проблемы предупреждения преступности : дис. ... д–ра юрид. наук / С.И. Герасимов. – М., 2001. – 446 с.

51. Громов, Е. В. Развитие уголовного законодательства о преступлениях в сфере компьютерной информации в зарубежных странах (США, Великобритании, ФРГ, Нидерландах, Польше) / Е. В. Громов // Вестник томского государственного Педагогического университета. – 2006. –№ 11. – С. 30–35.

52. Гузеева, О. С. Квалификация мошенничества в российском сегменте сети Интернет / О. С. Гузеева // Законность. − 2013. − №3 (941). − С. 21–24.

53. Дагель, П.С. Учение о личности преступника в советском уголовном праве. Учебное пособие / Дагель П.С. – Владивосток: Изд-во Дальневост. ун-та, 1970. – 132 с.

54. Данилова, Н. А. Преступления в сфере банковской деятельности как высокотехнологичные преступные посягательства международного характера / Н. А. Данилова, С. П. Кушниренко, А. Н. Саржин // Вестник Санкт–Петербургского университета МВД России. – 2006. – № 2. – С. 329–333.

55. Дремлюга, Р. И. Интернет–преступность / Р. И. Дремлюга. – Владивосток: изд–во Дальневосточного университета, 2008. – 240 с.

56. Дремлюга, Р. И. Международно–правовое регулирование сотрудничества в сфере борьбы с Интернет–преступностью / Р. И. Дремлюга // Библиотека криминалиста.− 2013. − №5(10). – С.339–346.

57. Дыкусова, А. Г. Экономическое значение и роль системы пластиковых карт в России / А. Г. Дыкусова, И. Г. Дыкусова // Вестник ИрГТУ. – 2014. – № 8 (91). – С.175–179.

58. Желудков, М. А. Новый взгляд на концепцию объекта защиты от корыстных преступлений против собственности / М.А. Желудков // Вестник Воронежского института МВД России. − 2011. − №1.– С.47–51

59. Жубрин, Р. В. Предупреждение преступности на современном этапе развития российского общества: понятие, содержание, принципы / Р. В. Жубрин // Всероссийский криминологический журнал. – 2016. – № 4. – С. 627–637.

60. Задорожный, В. И. Концептуальные основы виктимологической профилактики преступлений: дис. ... д–ра юрид. наук / В.И. Задорожный. – М., 2007. – 606 с.

61. Зимин, О. В. Факторы легализации (отмывания) денежных средств или иного имущества, приобретенных преступным путем / О. В. Зимин // Вестник Академии экономической безопасности МВД России. – 2009. – № 9. – С. 62–75.

62. Зыков, Д. А. Виктимологические аспекты предупреждения компьютерного мошенничества: дис.... канд. юрид. наук. / Д. А. Зыков. – Владимир, 2002. – С. 156–165.

63. Иванова, И. Г. Выявление и расследование неправомерного доступа к компьютерной информации: дис. ... канд. юрид. наук. / И. Г. Иванова. – Барнаул, 2007. – С. 7.

64. Иванченко, Р. Б. Проблемы квалификации мошенничества в сфере компьютерной информации / Р. Б. Иванченко, А. Н. Малышев // Вестник ВИ МВД России. – 2014. – № 1. – С.194–200.

65. Изотов, Д. С. Виды мошенничества с банковскими картами / Д. С. Изотов Н. Н. Быкова // Вестник НГИЭИ. – 2015. – №3 (46). – С. 49–53.

66. Иконников, Д. Н. Предупреждение преступлений, совершаемых с использованием банковских карт / Д. Н. Иконников // Расчеты и операционная работа в коммерческом банке. – 2011. – № 3.

67. Илинич, Е. В. Мошеннические операции с банковскими пластиковыми картами как угроза экономической безопасности в сфере банковской деятельности / Е. В. Илинич // Статистика и экономика. – 2013. – № 6. – С. 41–45.

68. Ильин, И. В. Виктимологическая профилактика экономического мошенничества : Дис. ... канд. юрид. наук. / И. В. Ильин. – Н. Новгород, 2000. – 213 с.

69. Кабурган, И. И. Безопасность применения банкоматов и предупреждение мошенничества с банковскими картами / И. И. Кабурган, А. П. Стерхов // Вестник ИрГТУ. – 2014. – №4 (87). – С.181–186.

70. Калашников, О. Д. Виктимологическая профилактика – перспективное направление в борьбе с преступностью на современном этапе / О. Д. Калашников // Виктимология. – 2017. – № 1 (11).

71. Камко, А. С. Виктимологическая профилактика преступлений в сфере безналичного обслуживания в России: состояние и перспективы развития опыт / А. С. Камко // Библиотека криминалиста. – 2016. – № 6.

72. Камко, А. С. Зарубежная система профилактики и противодействия мошенничеству в сфере высоких технологий: законодательство и опыт / А. С. Камко // Библиотека уголовного права и криминологии. – 2016. – № 6.

73. Камко, А. С. Особенности мошенничества с банковскими картами и АТМ–терминалами в России / А. С. Камко // Библиотека криминалиста. – 2016. – № 1.

74. Камко, А. С. Проблемы и перспективы системы противодействия мошенничеству с использованием телекоммуникационного и компьютерного оборудования / А. С. Камко // Власть и управление на Дальнем Востоке. – 2017. – № 4. – С. 182–187.

75. Камко, А. С. Уголовно–правовые вопросы противодействия преступности в сфере безналичных расчетов / А. С. Камко // Сборник материалов научно–практической конференции «Актуальные вопросы обеспечения прав и свобод человека и гражданина: региональное измерение», Хабаровск, 2017. – С. 187–193.

76. Камко, А. С. Портрет современной преступности Хабаровского края / А. С. Камко // Молодёжь Востока России: история и современность :материалы VI Всероссийской научно-практической конференции 1 ноября 2019 г. – Хабаровск : Дальневосточный институт управления – филиал РАНХиГС, 2019. – С. 120-123.

77. Карева, Е. И. Мошенничество с пластиковыми картами в России / Е. И. Карева // Молодой ученый. – 2015. – № 1. – С. 325–328.

78. Карнаухова, Е. Ю. Мошенничество в сфере безналичных расчетов с использованием банковских платежных карт / Е. Ю. Карнаухова //

Юридические науки: проблемы и перспективы: материалы II Междунар. науч. конф. (г. Пермь, январь 2014 г.). – Пермь: Меркурий, 2014. – С. 42–44.

79. Кауфман, Ю. С. Законодательное регулирование мошенничества в сфере компьютерной информации / Ю. С. Кауфман // Вестник ТГУ. – 2014. – № 3 (131). – С. 213–216.

80. Квашис, В. Е. Основы виктимологии / В. Е. Квашис. – М., 1999.

81. Кесареева, Т. П. Криминологическая характеристика и предупреждение преступности в Российском сегменте сети Интернет: дис. ... канд. юрид. наук. / Т. П. Кесареева. – М., 2002. – С. 103.

82. Киселев, А.К. Киберпреступность – взгляд из Европы / А.К. Киселев // Библиотека криминалиста.− 2013. − №5(10). − С.309–313.

83. Клейменов, М. П. Криминология / М. П. Клейменов. – М. : Норма : Инфра–М, 2014. – 432 с.

84. Клепицкий, И. А. Собственность и имущество в уголовном праве / И. А. Клепицкий // Государство и право. – 1997. – № 5. – С. 78.

85. Козаев, Н. Ш. Некоторые новеллы уголовного законодательства, направленные на обеспечение экономической безопасности в условиях научно–технического прогресса / Н.Ш. Козаев // Библиотека криминалиста.− 2013. − №5(10). – С.15–21.

86. Козаченко, И. Я. Криминология / И. Я. Козаченко, К. В. Корсаков. – М. : Норма : Инфра–М, 2014. – 304 с.

87. Комаров, А. А. Интернет–мошенничество: проблемы детерминации и предупреждения : монография / А. А. Комаров. – М.: Юрлитинформ, 2013. – 179 с.

88. Костыря, Е. А. Виктимологическая профилактика и проблемы социально–психологической реабилитации потерпевших / Е. А. Костыря // Юридические науки: проблемы и перспективы: материалы междунар. науч. конф. (г. Пермь, март 2012 г.). – Пермь: Меркурий, 2012. – С. 133–135.

89. Кочои, С. М. Новые нормы о мошенничестве в УК РФ: особенности и отличия / С. М. Кочои // Криминологический журнал Байкальского государственного университета экономики и права. − 2013. − № 4. – С. 104–110.

90. Кравцов, И. А. К вопросу о социально–демографических признаках личности преступника, совершающего хищение чужого имущества с использованием служебного положения, на территории Центрально–Черноземного региона / И. А. Кравцов // Вестник ВИ МВД России. – 2011. – № 3.

91. Кравцов, И. А. Криминологические особенности личности преступников, совершающих мошенничества в России / И. А. Кравцов // Вестник ВИ МВД России. – 2017. – № 3.

92. Кредитно–карточное мошенничество растет и процветает // «Бизнес&Балтия», 2011. [Электронный ресурс] // Режим доступа: http://bb.lv/bb/all/2857/

93. Криминология / под общ. ред. А. И. Долговой. – М. : Норма : Инфра–М, 2010. – 1008 с.

94. Ксеник, А. А. Зарубежный опыт виктимологической профилактики преступлений / А. А. Ксеник // Молодой ученый. – 2017. – №12. – С. 412–415.

95. Кудрявцев, В. Н. Причинность в криминологии (О структуре индивидуального преступного поведения) / В. Н. Кудрявцев. – М.: Изд–во «Юрид. лит.», 1968. – С. 22–23.

96. Кудрявцев, В. Н. Причины преступности в России: криминологический анализ / В. Н. Кудрявцев, В. Е. Эминов. – М.: Юристъ, 2006. – С. 71.

97. Кузнецов, А. П. Ответственность за преступления в сфере компьютерной информации по зарубежному законодательству / А. П. Кузнецов // Международное публичное и частное право. – 2007. – № 3.– С. 60–62.

98. Куликов, Н. И. Анализ схем правонарушений в области использования пластиковых карт / Н. И. Куликов, А. А. Сизов // Экономика и экологический менеджмент. – 2015. – № 2. – С.61–69.

99. Кутякин, С. А. Некоторые аспекты современного состояния разработки понятия «противодействие преступности» в юридической науке и законодательной практике / С. А. Кутякин // Юридическая наука и правоохранительная практика. – 2009. – № 2 (8). – С. 40–51.

100. Лапутин, М.М. Уголовная ответственность за неправомерный доступ к компьютерной информации: общая характеристика и некоторые проблемы квалификации / М.М. Лапутин // Библиотека криминалиста.− 2013. − №5(10). – С.23–31.

101. Ларичев, В. Д. Понятие и характеристика основных субъектов предупреждения преступлений в сфере экономики в современных условиях / В. Д. Ларичев, О. Ю. Исаев // Общество и право. – 2010. – № 1. – С. 202–206.

102. Левченко, И. В. К вопросу об особенностях личности мошенника / И. В. Левченко, О. С. Демко // Научный альманах. – 2015.·– № 11–4(13). – С. 458–461.

103. Лелетова, М. В. Предупреждение виктимизации / М. В. Лелетова // Следователь. – 2007. – № 4. – С. 42–45.

104. Лопатина, Т. М. Проблемы формирования уголовно–правового способа борьбы с компьютерным мошенничеством / Т.М. Лопатина // Библиотека криминалиста.− 2013. − №5(10). – С.32–41

105. Лукьянов, С. О. мошенничество с использованием банковских карт в России: современное состояние и виды защиты / С. О. Лукьянов // Вестник ТГЭУ. – 2012. – № 2.

106. Майоров, А. В Содержание системы виктимологического противодействия преступности / А. В. Майоров // Юридическая наука и правоохранительная практика. – 2017. – № 3 (41).

107. Майоров, А. В. Виктимологическая модель противодействия преступности: монография. / А. В. Майоров. – М.: Юрли–тинформ, 2014. – 224 с.

108. Майоров, А. В. О концепции виктимологического противодействия преступности / А. В. Майоров // Юридическая наука и правоохранительная практика. – 2015. – № 4 (34). –С. 50–57.

109. Майоров, А. В. Понятие и структура системы противодействия преступности / А. В. Майоров // Правопорядок: история, теория, практика. – 2014. – № 1 (2). – С. 112–116.

110. Майоров, А. В. Противодействие преступности – приоритетное направление в уголовной политике государства / А. В. Майоров // Вопросы современной юриспруденции. – 2014. – № 34. – С. 128–132.

111. Малиновский, А. А. Сравнительное правоведение в сфере уголовного права / А. А. Малиновский. – М.: Юристъ, 2002. – С. 4.

112. Малыхина, Т. А. Виктимологическая характеристика и предупреждение мошенничества : дис. ... канд. юрид. наук / Т. А. Малыхина. – Иркутск, 2007.

113. Матвеев, А. В. Виктимологический аспект коррупции в системе государственного управления / А. В. Матвеев, В. И. Федоренко // XXXX неделя науки СПбГПУ: материалы международной научно–практической конференции. Ч.XVIII. – СПб.: Изд–во Политехн. ун–та, 2011. – С. 15 – 17.

114. Матвеев, А. В. Массовая виктимность как аспект социальной напряженности в обществе / А. В. Матвеев, В. И. Федоренко // XXXX неделя науки СПбГПУ: материалы международной научно–практической конференции. Ч.XVIII. – СПб.: Изд–во Политехн. ун–та, 2011. – С. 72 – 75.

115. Материалы Главного информационно–аналитического центра МВД РФ [Электронный ресурс] // Режим доступа: https://xn—b1aew.xn—p1ai/folder/101762/item/11341800/

116. Мегрелишвили, Г. Т. Криминологический и психологический портрет личности преступников в сфере высоких технологий / Г. Т. Мегрелишвили // Вестник Томского государственного университета. – 2007. – № 299. – С. 180–181.

117. Медведев, С. С. Мошенничество в сфере высоких технологий: дис. … канд. юрид. наук. / С. С. Медведев. – Краснодар, 2008. – С. 145–146.

118. Международная практика по организации эмиссии и борьбе с мошенничеством [Электронный ресурс] // Режим доступа: http://visa.com.ru/ru/ru–ru/personal/security/visacardsecurity.shtml

119. Мерзлов, Ю. А. Криминологический портрет лиц, совершающих преступления в сфере компьютерной информации / Ю. А. Мерзлов // Правопорядок: история, теория, практика. – 2015. – № 4 (7). – С. 56–61.

120. Минуллина, А. Ф. Исследование характеристик эмоционального интеллекта и показателей толерантности к неопределенности у мужчин и женщин / А. Ф. Минуллина, Э. И. Муртазина // Гуманитарные исследования в Восточной Сибири и на Дальнем Востоке. – 2014. – № 4 (30). – С. 125–130.

121. Мунькина, А. В. Виды мошенничества с банковскими пластиковыми картами и способы защиты от него / А. В. Мунькина // Информационная безопасность и вопросы профилактики киберэкстремизма среди молодежи. Материалы внутривузовской конференции. Под редакцией Г.Н. Чусавитиной, Е.В. Черновой, О.Л. Колобовой, 2015. – С. 340–350.

122. Нагорный, В. А. Криминологические особенности некоторых преступлений, совершаемых в сфере оборота платежных карт / В. А. Нагорный // Права и свободы человека и эффективные механизмы их реализации в мире, России и Татарстане: материалы международной научно–практической конференции, 28–29 ноября 2013 г. Казань: Познание, 2014. – С. 493–498.

123. Наличные деньги и электронные средства платежа: проблемы, тенденции // Деньги и кредит. – 2012. – № 7. – С. 3–23.

124. Народная Республика Йемен. Конституция и законодательные акты. // Сост. и пер. Сюкияйнена Л.Р. // Под ред. Юдина Ю.А. – М. 1985. – С. 413–421.

125. Никульцева, А. Н. Перспективы имплементации международно–правовых обязательств в сфере ответственности за преступления в сфере

компьютерной информации в российском законодательстве / А. Н. Никульцева // Актуальные проблемы права: материалы III Междунар. науч. конф. (г. Москва, ноябрь 2014 г.). – М.: Буки–Веди, 2014. – С. 99–104.

126. Номоконов, В. А. Киберпреступность: прогнозы и проблемы борьбы / В. А. Номоконов, Т. Л. Тропина // Библиотека криминалиста.− 2013.− № 5 (10). − С.148–159.

127. Носкова, Е. Убытки от мошенничества выросли в 10 раз // Российская газета, 2014. [Электронный ресурс] // Режим доступа: http://www.rg.ru/2014/08/19/moshennichestvo.html

128. Овчинский, В. С. Оперативно–розыскная аналитика в цифровом мире / В. С. Овчинский, А. С. Овчинский // Информатизация и информационная безопасность правоохранительных органов. Сборник трудов XXV Всероссийской научно–практической конференции. Академия управления МВД России, 2016. – С. 175–180.

129. Овчинский, В. С. Трамп, ФБР, искусственный интеллект / В. С. Овчинский [Электронный ресурс] // Режим доступа: http://zavtra.ru/blogs/tramp_fbr_iskusstvennij_intellekt

130. Огнев, В. О грустном юморе М. Светлова / В. Огнев // Литературная газета. – 2011. – № 2.

131. Орлова, Ю. Р. Криминологические особенности личности несовершеннолетних женского пола, совершивших корыстно–насильственные преступления / Ю. Р. Орлова, О. Н. Гусева // Юридическая психология. – 2008. – № 4. – С. 19–23.

132. Павлова, Е. В. Россия и современный мир: ключевые проблемы в экономической сфере / Е. В. Павлова, Т. Е. Снхчян // Молодой ученый. – 2014. – № 4. – С. 589–593.

133. Павлова, Е. В. Современное состояние рынка кредитования физических лиц в Российской Федерации / Е. В. Павлова, М. В. Ермакова // Вектор науки Тольяттинского государственного университета. Серия: Экономика и управление. – 2013. – № 4 (15). – С. 36–39.

134. Панов, С. Л. Принципы взаимодействия органов внутренних дел и общественных формирований по противодействию правонарушениям / С. Л. Панов, С. А. Тимко, В. П. Тимко // Психопедагогика в правоохранительных органах. – 2016. – № 4 (67). – С.53–56.

135. Письмо Банка России от 01.03.2013 №34–Т «О рекомендациях по повышению уровня безопасности при использовании банкоматов и платежных терминалов». [Электронный ресурс] // Режим доступа: :http://www.consultant.ru/document/cons_doc_LAW_143007/

136. Пластик свободной конвертации. [Электронный ресурс] // Режим доступа: http://www.prostobank.ua/layout/set/print/plastikovye_karty/stati/plastik_svobodnoy_konvertatsii.

137. Плюснина, О. А. Мошенничество с банковскими картами: акценты финансовой безопасности / О. А. Плюснина, Т. Г. Григорьева // Инновационная наука. – 2016. – № 4–2 (16). – С. 12–15.

138. Понявин, В. В. Развитие института ответственности за изготовление и сбыт поддельных ценных бумаг и платежных документов в российском праве / В. В. Понявин // Молодой ученый. – 2009. – № 10. – С. 252–256.

139. Пресс–служба Управления «К» МВД РФ. [Электронный ресурс] // Режим доступа: http://www.mvd.ru/news/show_104337/

140. Простосердов, М. А. К вопросу об оценке общественной опасности преступлений, совершаемых в сети Интернет / М.А. Простосердов // Актуальные проблемы уголовного права и криминологии: сборник научных трудов кафедры уголовного права. Выпуск № 3. Под ред. Ю.Е. Пудовочкина и А.В. Бриллиантова. – М.: РАП., 2013. – С. 198–209.

141. Простосердов, М. А. Проблемы квалификации компьютерных преступлений / М.А. Простосердов // Российское правосудие. – 2012. – № 6 (74). – С. 106 –108.

142. Простосердов, М. А. Экономические преступления, совершаемые в киберпространстве, и меры противодействия им / М.А. Простосердов // Су-

дебные известия. Информационный бюллетень Управления Судебного департамента в Тамбовской области. – 2014. − № 15(2) – С. 49–53.

143. Простосердов, М. А. Экономические преступления, совершаемые в киберпространстве, и меры противодействия им: дис. … канд. юрид. наук / М. А. Простосердов. – М., 2016.

144. Ревина, Н. В. Опыт зарубежных стран в развитии виктимологической профилактики мошенничества / Н. В. Ревина, А. В. Ростокинский // Бизнес в законе. – 2010. – № 1.

145. Репин, М. Е. Преступления в сфере компьютерной информации: проблемы выявления и раскрытия / М. Е. Репин А. Ю. Афанасьев // Молодой ученый. — 2015. – № 15. – С. 460–463.

146. Репин, М. Е. Характеристика преступлений мошеннического характера, совершаемых с использованием сотовой связи / М. Е. Репин // Молодой ученый. – 2016. – № 11. – С. 1335–1338.

147. Ривман, Д. В. Виктимология / Д. В. Ривман, В. С. Устинов. – СПб.: Юрид. центр Пресс, 2000.

148. Ривман, Д. В. Криминальная виктимология / Д. В. Ривман. – СПб.: Питер, 2002. – 304 с.

149. Сабадаш, В. П. Специальные подразделения и организации по борьбе с Интернет–мошенничеством в различных государствах мира / В. П. Сабадаш // Библиотека криминалиста.− 2013. − №5(10). – С.328–338.

150. Сабитов, Р. А. Понятие и признаки криминального обмана / Р. А. Сабитов // Уголовное право. – 2015. – № 5. – С. 86 – 89.

151. Салихова, Н. Р. Соотношение характеристик ценностно–смысловой сферы личности и стратегий совладающего поведения / Н. Р. Салихова, М. В. Клементьева // Известия ТГУ. – 2014. – № 4. – С. 224 – 235.

152. Сафонов, О. М. Уголовно–правовая оценка использования компьютерных технологий при совершении преступлений: состояние законода-

тельства и правоприменительной практики, перспективы совершенствования : дис. … канд. юрид. наук / О. М. Сафонов. – М., 2015.

153. Сбербанк с 1 июля откажется от выпуска карт с магнитной полосой. [Электронный ресурс] // Режим доступа: http://wwwinterfax.ru/ifx.asp?id=8f938919–675e–f24b–9e51–62f1e702b73a

154. Смирнов, А. А. Сеть «Интернет» в механизме криминологической детерминации / А.А. Смирнов // Библиотека криминалиста. − 2013. − № 5(10). – С.161–173.

155. Список стран с повышенным уровнем риска карточного мошенничества [Электронный ресурс] // Режим доступа: http://www.asiacreditbank.kz/upload/Cards/%D0%A1%D0%BF%D0%B8%D1%81%D0%BE%D0%BA%20%D1%81%D1%82%D1%80%D0%B0%D0%BD%20%D1%81%20%D0%BF%D0%BE%D0%B2%D1%8B%D1%88%D0%B5%D0%BD%D0%BD%D1%8B%D0%BC%20%D1%83%D1%80%D0%BE%D0%B2%D0%BD%D0%B5%D0%BC%20%D1%80%D0%B8%D1%81%D0%BA%D0%B0%20%D0%BA%D0%B0%D1%80%D1%82%D0%BE%D1%87%D0%BD%D0%BE%D0%B3%D0%BE%20%D0%BC%D0%BE%D1%88%D0%B5%D0%BD%D0%BD%D0%B8%D1%87%D0%B5%D1%81%D1%82%D0%B2%D0%B0.pdf

156. Степанов, М. В. Критический анализ нормы о мошенничестве в сфере компьютерной информации (ст. 1596 УК РФ) / М. В. Степанов // Юридическая наука и практика: Вестник Нижегородской академии МВД России. – 2016. – № 1 (33). – С. 173–178.

157. Степанов–Егиянц, В. Г. Методологическое и законодательное обеспечение безопасности компьютерной информации в Российской Федерации (уголовно–правовой аспект): автореф. дис. … д–ра юрид. наук / В. Г. Степанов–Егиянц. – М., 2016

158. Степанов–Егиянц, В. Г. Преступления сфере безопасности обращения компьютерной информации: сравнительный анализ: дис. …канд. юрид. наук / В. Г. Степанов–Егиянц. – М., 2005. − 168 с.

159. Степанов–Егиянц, В. Г. Совершение мошенничества с использованием компьютера или информационно–телекоммуникационных сетей / В. Г. Степанов–Егиянц // Финансовая жизнь. – 2013. – № 2. – С. 68–70.

160. Степанов–Егиянц, В. Г. Современная уголовная политика в сфере борьбы с компьютерными преступлениями / В. Г. Степанов–Егиянц // Российский следователь. – 2012. – № 24. – С. 43–46.

161. Сунчалиева, Л. Э. Мошенничество (Уголовно-правовой и криминологический аспект) : дис. ... канд. юрид. наук / Л. Э. Сунчалиева. – Ставрополь, 2004. – 187 с.

162. Суслопаров, А. В. Компьютерные преступления как разновидность преступлений информационого характера : дис. ... канд. юрид. наук / А.В. Суслопаров. – Красноярск, 2010.

163. Теплова, Д. О. Криминологическая характеристика и предупреждение организованного мошенничества: дис. ... канд. юрид. наук. / Д. О. Теплова. – М., 2014. – С. 248.

164. Теплова, Д. О. Криминологические основы противодействия организованному мошенничеству: Монография. / Д. О. Теплова. – М.: РГУП, 2017. – 220 с.

165. Тонков, Е. Е. Научные ведомости Белгородского государственного университета / Е. Е. Тонков, И. М. Комаров // Философия. Социология. Право. – 2011. – № 8 (103).

166. Тропина, Т. Л. Киберпреступность. Понятие, состояние, уголовно–правовые меры борьбы : дис. ... канд. юрид. наук / Т. Л. Тропина. – Владивосток, 2005.

167. Тропина, Т. Л. Криминализация киберпреступлений: достижение консенсуса / Т. Л. Тропина // Компьютерная преступность и кибертерроризм. Исследования, аналитика. – 2004. – № 2. – С. 49–56.

168. Тюнин, В. И. Некоторые вопросы толкования и применения норм о специальных видах мошенничества / В. И. Тюнин // Уголовное право. – 2015. – № 5. – С. 116–126.

169. Уголовный кодекс Австрии [Электронный ресурс] // Режим доступа: http://www.gesetze–im–internet.de/stgb/

170. Уголовный кодекс Белоруссии [Электронный ресурс] // Режим доступа: http://etalonline.by/?type=text&regnum=hk9900275#load_text_none_1

171. Уголовный кодекс Германии с изменениями от 28 декабря 2003 года. [Электронный ресурс] // Режим доступа: http://lexetius.com/StGB/263a

172. Уголовный кодекс Дании. [Электронный ресурс] // Режим доступа: https://www.retsinformation.dk/Forms/R0710.aspx?id=152827#Kap28

173. Уголовный кодекс Италии [Электронный ресурс] // Режим доступа: URL:http://www.altalex.com/?idnot=36653

174. Уголовный кодекс Китайской Народной Республики [Электронный ресурс] // Режим доступа: http://constitutions.ru/archives/403

175. Уголовный кодекс Нидерландов [Электронный ресурс] // Режим доступа: http://wetten.overheid.nl/BWBR0001854/TweedeBoek/TitelV/Artikel138ab/geldigheidsdatum

176. Уголовный кодекс Республики Корея [Электронный ресурс] // Режим доступа: http://www.crime.vl.ru/index.php?p=1324&more=1

177. Уголовный кодекс Украины [Электронный ресурс] // Режим доступа: http://zakon1.rada.gov.ua/cgi–bin/laws/main.cgi?nreg=2341–14&p=1214905443606898

178. Уголовный кодекс Финляндии [Электронный ресурс] // Режим доступа: http://www.finlex.fi/en/laki/kaannokset/1889/en18890039.pdf

179. Уголовный кодекс Швейцарии [Электронный ресурс] // Режим доступа: http://law.edu.ru/norm/norm.asp?normID=1241950&subID=100098712,100098714,100098872,100099140,100099172#text.

180. Уголовный кодекс Эстонии [Электронный ресурс] // Режим доступа: http://www.hot.ee/almanach/kriminaalseadustik.html

181. Уровень образования населения // Национальный исследовательский университет «Высшая школа экономики». [Электронный ресурс] // Режим доступа: https://memo.hse.ru/ind_w10_0_01

182. Фадина, Ю. П. Уголовно–правовая характеристика мошенничества в сети Интернет / Ю. П. Фадина // Вестник ЮГУ. – 2017. – № 1–2 (44). – С.117–121.

183. Фаргиев, И. А. Виктимология в системе научного знания / И. А. Фаргиев // Северо–кавказский юридический вестник. – 2014. – № 4. – С. 101–105.

184. Финагеев, В. А. Проблемы взаимодействия правоохранительных органов и подразделений банковской безопасности в выявлении и расследовании преступлений / В. А. Финагеев // Таможенное дело. – 2013. – № 2 (86). – С. 264–270.

185. Франк, Л. В. Потерпевшие от преступления и проблемы советской виктимологии / Л.В. Франк. – Душанбе: Ирфон, 1977. – 240 с.

186. Фролов, М.Д. Уголовно–правовое и криминологическое противодействие мошенничеству в сфере компьютерной информации: : автореф. дис. ... канд. юрид. наук. М., 2019.

187. Фурманов, Д. В. Усугубление проблемы безопасности при использовании пластиковых карт / Д. В. Фурманов, Е. Н. Смольянинова // Территория новых возможностей. – 2012. – № 1. – С.158–163.

188. Хазова, С. А. Эмоциональные ресурсы совладающего поведения / С. А. Хазова // Ярославский педагогический вестник. – 2014. – № 1. – С. 293–297.

189. Харламов, Д. Д. Критерии криминализации новых видов мошенничества в УК РФ / Д. Д. Харламов // АВБсП. – 2016. – № 1. – С. 44–46.

190. Хилюта, В. В. Идентификация признаков мошенничества, присвоения и растраты в судебной практике / В. В. Хилюта // Уголовное право. – 2015. – № 5. – С. 127–130.

191. Хисамова, З. И. Уголовно–правовые меры противодействия преступлениям, совершаемым в финансовой сфере с использованием информационно–телекоммуникационных технологий: дис. ... канд. юрид. наук / З. И. Хисамова. – Краснодар, 2016.

192. Центральный банк Российской Федерации. [Электронный ресурс] // Режим доступа: http://www.cbr.ru/statistics/p_sys/print.aspx?file=sheet007.htm&pid=psRF&sid=ITM_12859

193. Частная криминология: учебник / отв. ред. Д.А. Шестаков. СПб.: Юрид. центр Пресс, 2007. – 771 с.

194. Чекунов, И. Г. Киберпреступность: понятие и классификация / И. Г. Чекунов // Российский следователь. – 2012. – № 2. – С. 37–44.

195. Чекунов, И. Г. Некоторые особенности квалификации преступлений в сфере компьютерной информации / И. Г. Чекунов // Российский следователь. – 2012. – № 3. – С. 26–28.

196. Чупрова, А. Ю. Уголовно–правовые механизмы регулирования отношений в сфере электронной коммерции: дис. … д–ра юрид. наук. / А. Ю. Чупрова. – М., 2015. – С. 479.

197. Шагапов, И. Р. Мошенничество: проблемы применения законодательства / И. Р. Шагапов // Молодой ученый. – 2016. – № 7. – С. 538–540.

198. Шаламов, Г. А. Воровство в банковской сфере: монография / Г. А. Шаламов. – Иркутск: Изд–во ИрГТУ, 2012. – 140 с.

199. Широков, В. А. Киберпреступность: история уголовно–правового противодействия / В. А. Широков, Е. В. Беспалова // Информационное право. – 2006. – № 4. – С. 18–19.

200. Энгельгардт, А. А. Вопросы квалификации мошенничества в сфере компьютерной информации / А. А. Энгельгардт // Право. Журнал Высшей школы экономики. – 2016. – № 4. – С.86–95.

201. Якимова, Е. Д. Виктимологическая профилактика преступности: содержание и задачи / Е. Д. Якимова // Виктимология. – 2014. – № 1 (1). – С.55–58.

202. Яни, П. С. Законодательное определение потерпевшего от преступления / П. С. Яни // Российская юстиция. – 1995. – № 4. – С. 40.

203. Яни, П. С. Мошенничество и иные преступления против собственности: уголовная ответственность. Книга третья: монография / П.С. Яни. − М., Библиотека журнала «Уголовное право». 2007. − 136 с.

204. Ярочкин, В. И. Безопасность банковских систем / В. И. Ярочкин. – М.: Изд–во Ось–89, 2012. – 461 с.

205. Ясенев В. Н. Информационная безопасность в экономических системах / В. Н. Ясенев. – Н. Новгород: Изд–во ННГУ, 2006. –С. 58.

206. Ястребов, Д. А. Неправомерный доступ к компьютерной информации: уголовно–правовые и криминологические аспекты: дис.... канд. юрид. наук. / Д. А. Ястребов. – М., 2005. – С. 137–138.

Источники на иностранных языках

207. Goodchild J. Social Engineering: The Basics. / J. Goodchild // CSOonline. – 2010. – № 1.

208. Hentig H. Remarks on the Interaction of perpetrator and Victim // The of Criminal and Criminology. – 1941. – V. 31.

209. Lejins P.P. The Field of Prevention / Peter P. Lejins // Delinquency Prevention: Theory and Practice / William E. Amos, Charles F. Wellford (eds). – Englewood Cliffs, NJ : Prentice–Hall, 1967. – P. 2–21.

210. Mansfield–Devine S. «Darknets» / S. Mansfield–Devine // Computer Fraud & Security. – 2009 (12). – P. 4–6. [Электронный ресурс] // Режим доступа: doi:10.1016/S1361–3723(09)70150–2

211. Wood J. «The Darknet: A Digital Copyright Revolution» / J. Wood // Richmond Journal of Law and Technology. – 2011. – № 16 (4).

Приложение А
Тест Айзенка

На выполнение теста дается ровно *30 минут*. Не задерживайтесь слишком долго над одним заданием. Быть может, вы находитесь на ложном пути и лучше перейти к следующей задаче. Но и не сдавайтесь слишком легко; большинство заданий поддается решению, если вы проявите немного настойчивости. Продолжать размышлять над заданием или отказаться от попыток и перейти к следующему – подскажет здравый смысл. Помните при этом, что к концу серии задания становятся в общем труднее. Всякий человек в силах решить часть предлагаемых заданий, но никто не в состоянии справиться со всеми заданиями за полчаса.

Ответ на задание состоит из одного числа, буквы или слова. Иногда нужно произвести выбор из нескольких возможностей, иногда вы сами должны придумать ответ. Ответ напишите в указанном месте. Если вы не в состоянии решить задачу, не следует писать ответ наугад. Если же у вас есть идея, но вы не уверены в ней, то ответ все–таки проставьте.

Прежде чем приступить к решению, удостоверьтесь, что вы правильно поняли, что от вас требуется. Вы напрасно потеряете время, если возьметесь за решение, не уяснив, в чем состоит задача.

Примечания:

– Точки обозначают количество букв в пропущенном слове. Например, (**. . . .**) означает, что пропущенное слово состоит из четырех букв.

– Для решения некоторых заданий потребуется использовать последовательность букв русского алфавита без буквы «е».

Буквенный тест

1. Вставьте слово, которое означало бы то же, что и слова, стоящие вне скобок.

ТКАНЬ (...) СОСТОЯНИЕ ВЕЩЕСТВА

Ответ: газ

2. Вставьте слово, которое служило бы окончанием первого слова и началом второго.

ГО (...) КОТ

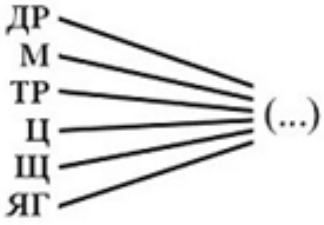
Ответ: бой

3. Решите анаграммы и исключите лишнее слово.

КОХЙЕК
СНИНЕТ
ОЖИВТ
ЛУФОБТ

Ответ: живот (остальные слова – виды спорта)

4. Найдите общее окончание для всех перечисленных слов.



5. Вставьте слово, которое означало бы то же, что и слова, стоящие вне скобок.

ЖИВОТНОЕ (...) МОНАХ

6. Вставьте слово, которое служило бы окончанием первого слова и началом второго.

СНА (...) ОВОЙ

7. Решите анаграммы и исключите лишнее слово.

ОЗУКРА
НИШПАЯЛ
НИБОВОС
НИШКУП

8. Найдите общее начало для трех следующих слов.

(.....) = БУРКА, ГОРЕЦ, КНИЖНИК

9. Вставьте слово, которое означало бы то же, что и слова, стоящие вне скобок.

РОДНИК (...) ОТМЫЧКА

10. Вставьте слово, которое служило бы окончанием первого слова и началом второго.

ПЕ (...) ОЛ

11. Решите анаграммы и исключите лишнее слово.

АЧТПО
АИДРО
ФАГРЕЛТЕ
КТЕВПНЦ

12. Найдите общее начало для трех следующих слов.

(....) = ВОЗ, НОС, РАЗДЕЛ

13. Вставьте слово, которое служило бы окончанием первого слова и началом второго.

ТА (...) АТ

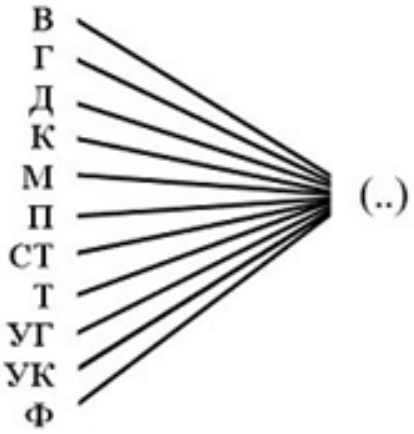
14. Вставьте слово, которое означало бы то же, что и слова, стоящие вне скобок.

БИТВА (.....) РУГАНЬ

15. Решите анаграммы и исключите лишнее слово.

АПНИСЕЛЬ
ЯШВИН
ТАСУПАК
АКАЧКБО
ШУРГА

16. Найдите общее окончание для следующих слов.



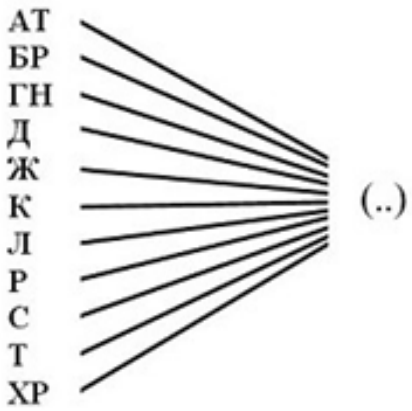
17. Вставьте слово, которое служило бы окончанием первого слова и началом второго.

БАЛ (...) ЕДА

18. Решите анаграммы и исключите лишнее слово.

ЮКИЛТ
ЛЮТАНЬП
АЛИФАК
ОЗАР
ЛОТУ

19. Найдите общее окончание для всех перечисленных слов.



20. Вставьте слово, которое означало бы то же, что и слова, стоящие вне скобок.

РЫБА (....) НАКЛОННАЯ ПОВЕРХНОСТЬ

21. Вставьте слово, которое служило бы окончанием первого слова и началом второго.

ДИК (.....) ЕЦ

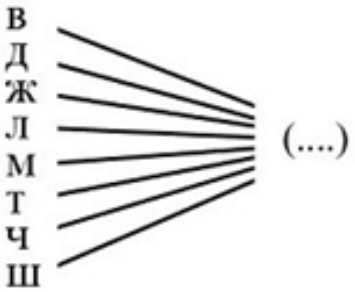
22. Решите анаграммы и исключите лишнее слово.

РАКОЧВА
ЛЬБГДОУ
ЕХРО
ЛУПЕДЬ

23. Вставьте слово, которое означало бы то же, что и слова, стоящие вне скобок.

НАСЫПЬ (...) ВРАЩАЮЩИЙСЯ СТЕРЖЕНЬ

24. Найдите общее окончание для всех последующих слов.



25. Вставьте слово, которое служило бы окончанием первого слова и началом второго.

СА (...) ОН

26. Решите анаграммы и исключите лишнее слово.

ЗМАТЕ
РАЖПИ
АГОВЛ
ИНЕРГ

27. Вставьте слово, которое означало бы то же, что и слова, стоящие вне скобок.

ЧАСТЬ ОДЕЖДЫ (.....) ГРУЗОПОДЪЕМНЫЙ МЕХАНИЗМ

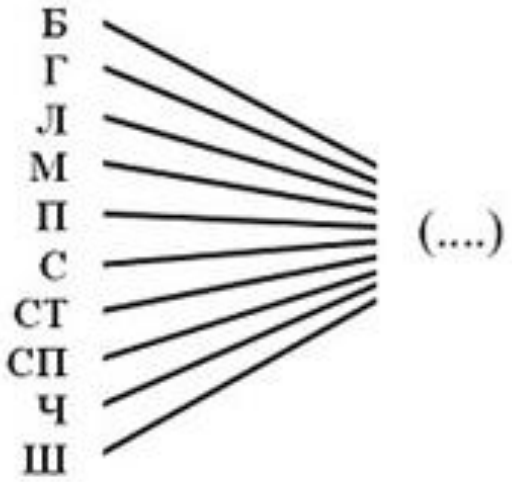
28. Вставьте слово, которое служило бы окончанием первого слова и началом второго.

У (....) Ь

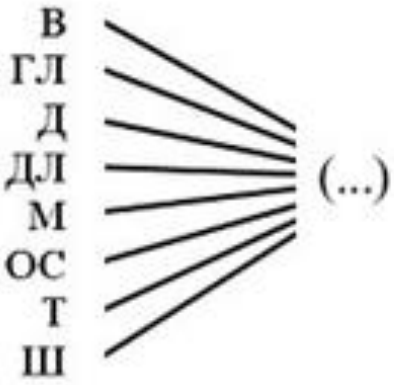
29. Решите анаграммы и исключите лишнее слово.

СЛОО
ОКОТИ
ООТРОНТ
РЕБЛАГД

30. Найдите общее окончание для всех последующих слов.



31. Найдите общее окончание для всех последующих слов.



32. Вставьте слово, которое означало бы то же, что и слова, стоящие вне скобок.

ЖИВОТНОЕ (.....) НЕЖНОСТЬ

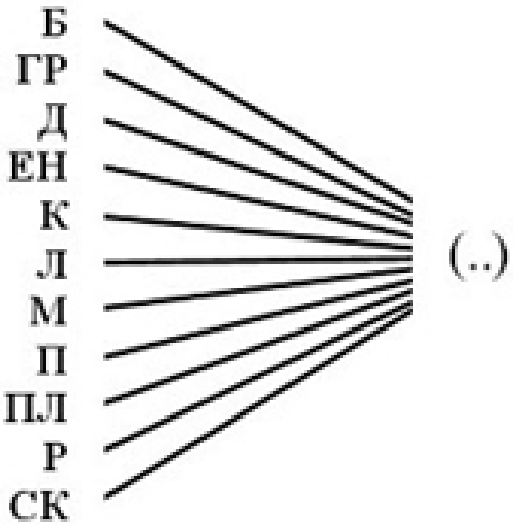
33. Вставьте слово, которое служило бы окончанием первого слова и началом второго.

КОВЕР (...) ЛЕТА

34. Решите анаграммы и исключите лишнее слово.

ЛЕОР
БЕОРОЙВ
КОВАОРЖОН
ФЕЛИНДЬ

35. Найдите общее окончание для всех последующих слов.



36. Вставьте слово, которое служило бы окончанием первого слова и началом второго.

КАБ (...) ОШКО

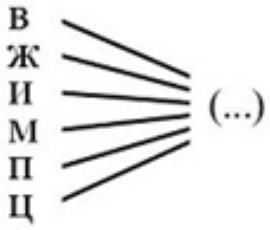
37. Решите анаграммы и исключите лишнее слово.

НЙЕНЙЭШТ
КИНСЕКД
ВЕХЧО
КЗААЛЬБ
СЙТООТЛ

38. Вставьте слово, которое означало бы то же, что и слова, стоящие вне скобок.

САМОВОЛЬНЫЙ УХОД (.....) МОЛОДАЯ ВЕТКА

39. Найдите общее окончание для всех последующих слов.



40. Вставьте слово, которое означало бы то же, что и слова, стоящие вне скобок.

ПРЕДЛОГ (.....) РЕМЕНЬ УЗДЫ

41. Вставьте слово, которое служило бы окончанием первого слова и началом второго.

С (...) ОКНО

42. Решите анаграммы и исключите лишнее слово.

ЛИОРЗТЕВЕ
ОИКСМТ
РКМОА
МИТТЕР

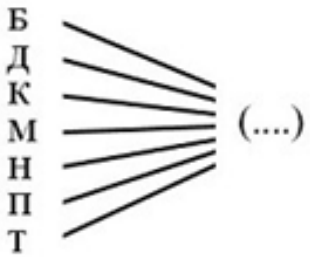
43. Вставьте слово, которое означало бы то же, что и слова, стоящие вне скобок.

КОСТОЧКА ПАЛЬЦА (.....) ПАУКООБРАЗНОЕ

44. Вставьте слово, которое служило бы окончанием первого слова и началом второго.

ГА (...) РЕЛЬ

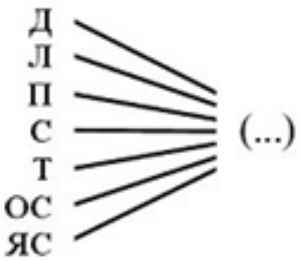
45. Найдите общее окончание для всех последующих слов.



46. Решите анаграммы и исключите лишнее слово.

ЗОАК
РЕОББ
СФОМАРЕ
ШАДОЛЬ

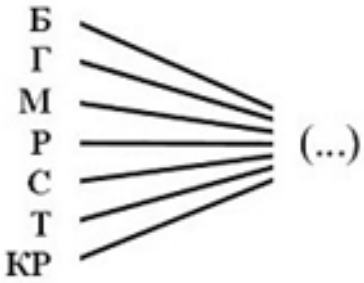
47. Найдите общее окончание для всех последующих слов.



48. Вставьте слово, которое служило бы окончанием первого слова и началом второго.

Г (...) ОЖА

49. Найдите общее окончание для всех последующих слов.

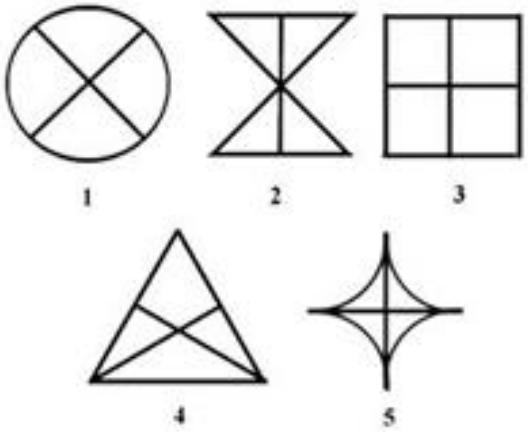


50. Решите анаграммы и исключите лишнее слово.

ТРБА
КПИРАКС
ТРСАЕС
АТМЬ
НКВЧУА

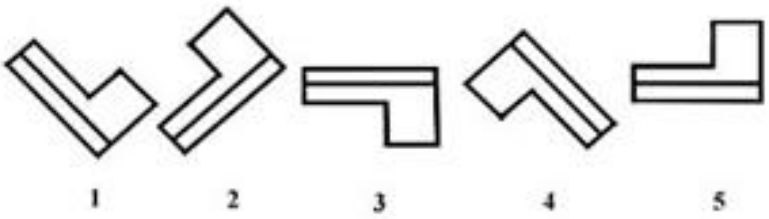
Наглядно–образный тест

1. Исключите лишнюю фигуру.



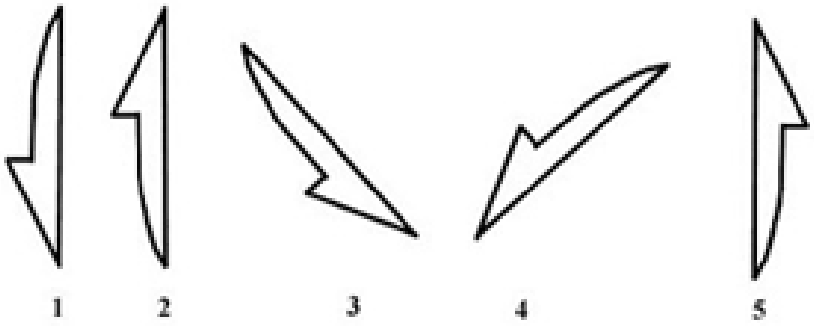
Ответ: 3

2. Исключите лишнюю фигуру.



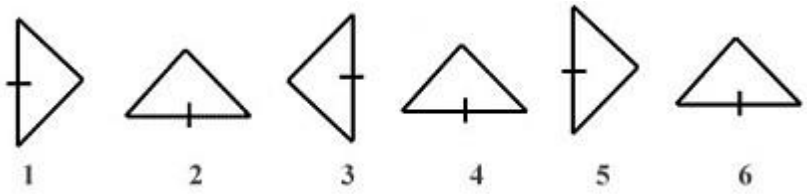
Ответ: 4

3. Исключите лишнюю фигуру.

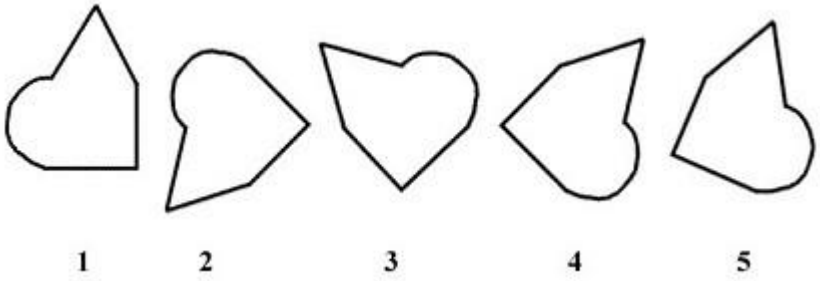


Ответ: 2

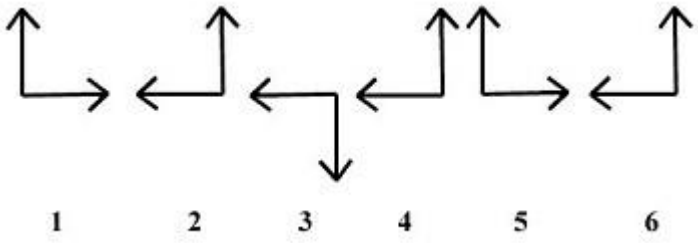
4. Исключите лишнюю фигуру.



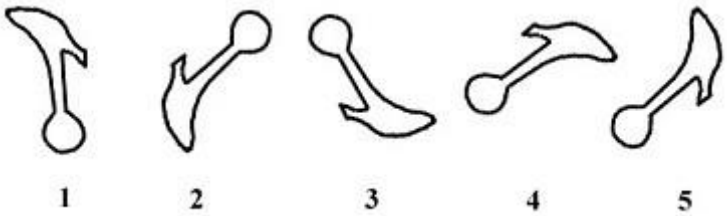
5. Исключите лишнюю фигуру.



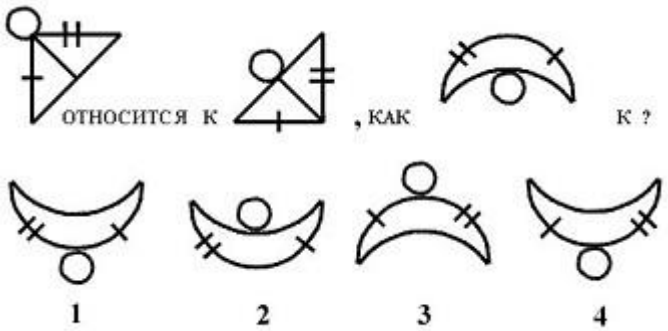
6. Исключите лишнюю фигуру.



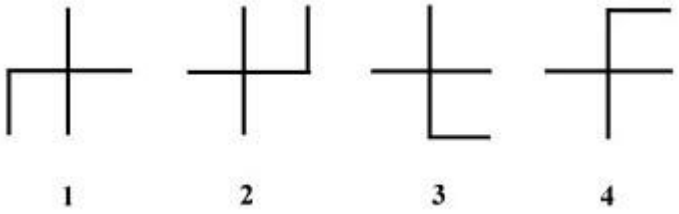
7. Исключите лишнюю фигуру.



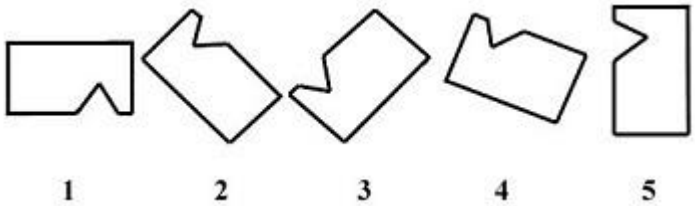
8. Вставьте пропущенную фигуру, выбрав ее из четырех пронумерованных.



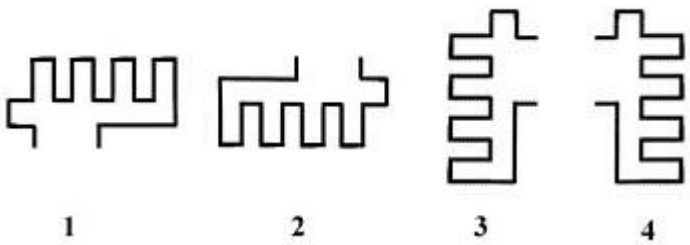
9. Исключите лишнюю фигуру.



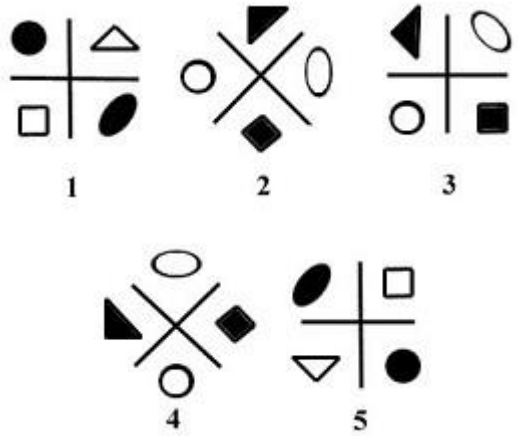
10. Исключите лишнюю фигуру.



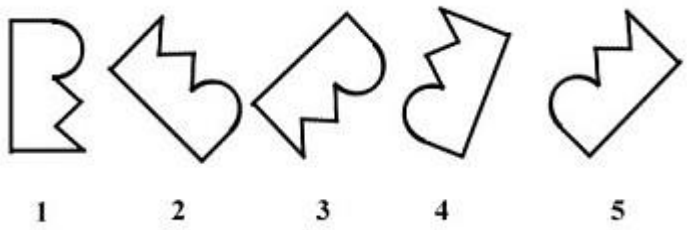
11. Исключите лишнюю фигуру.



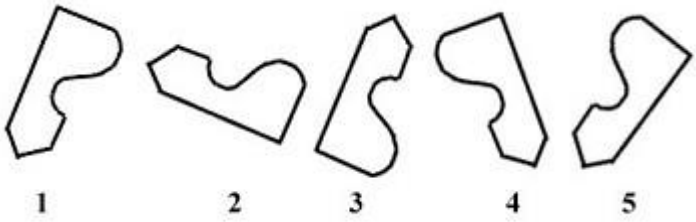
12. Исключите лишнюю фигуру.



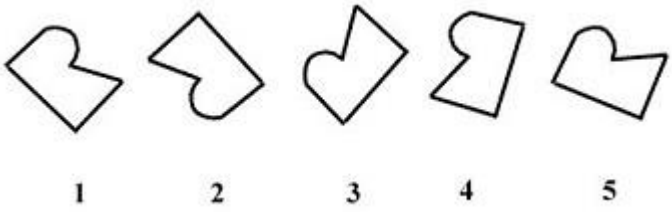
13. Исключите лишнюю фигуру.



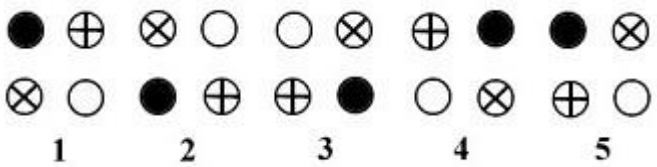
14. Исключите лишнюю фигуру.



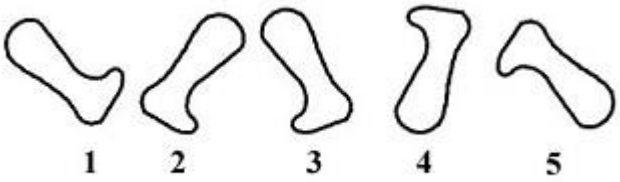
15. Исключите лишнюю фигуру.



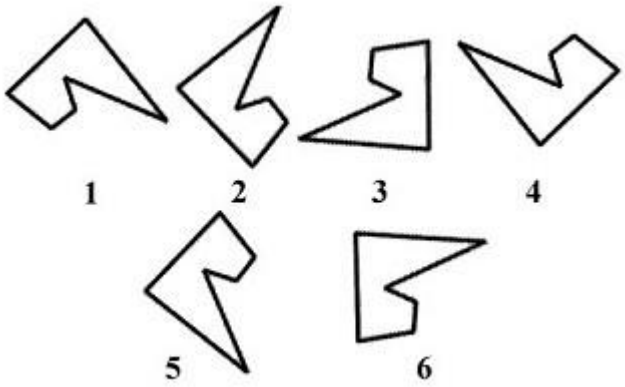
16. Исключите лишнюю фигуру.



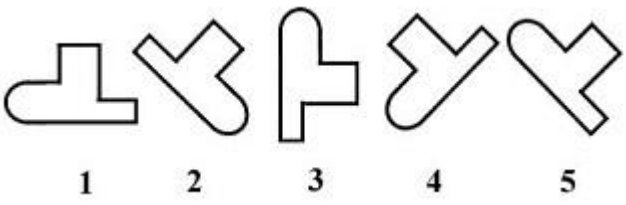
17. Исключите лишнюю фигуру.



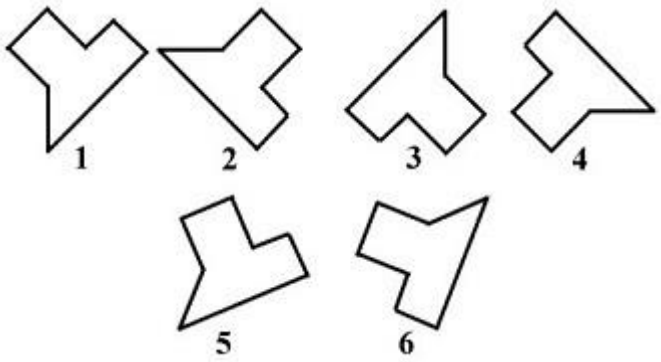
18. Исключите лишнюю фигуру.



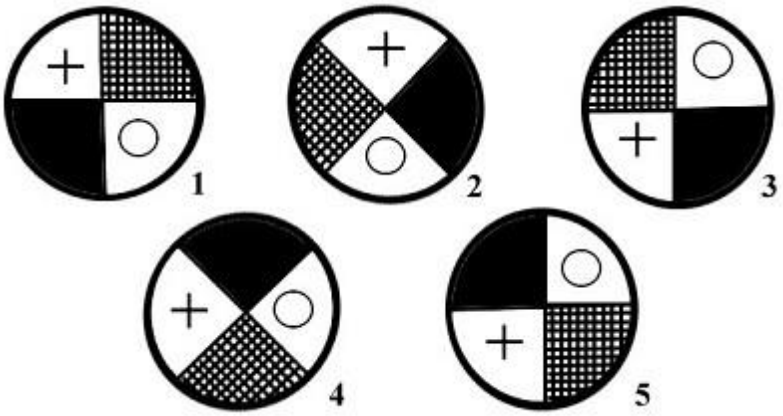
19. Исключите лишнюю фигуру.



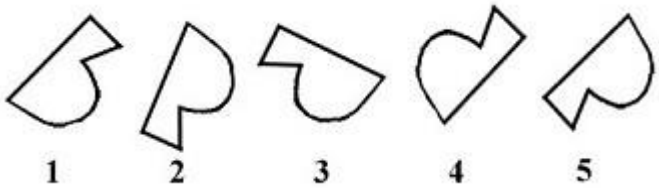
20. Исключите лишнюю фигуру.



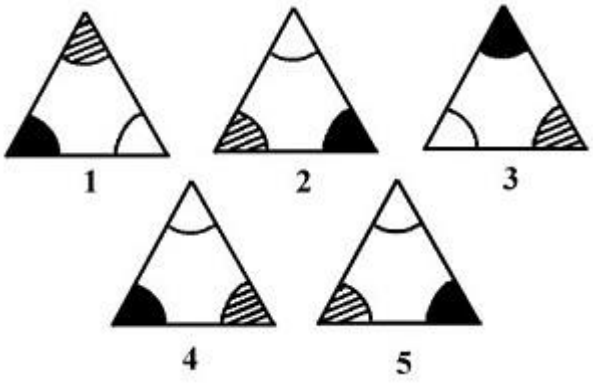
21. Исключите лишнюю фигуру.



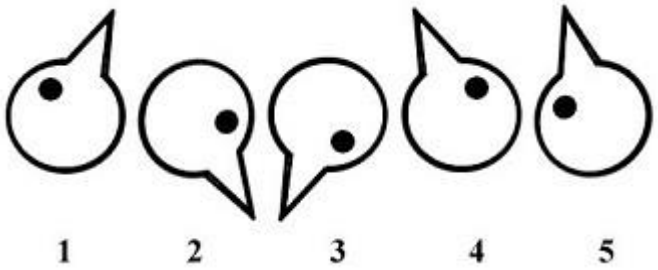
22. Исключите лишнюю фигуру.



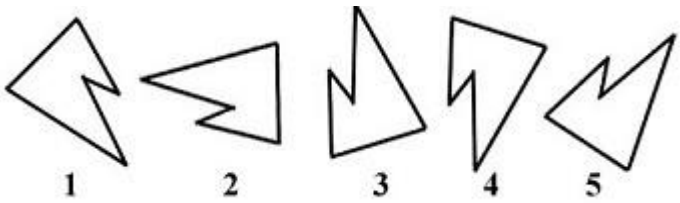
23. Исключите лишнюю фигуру.



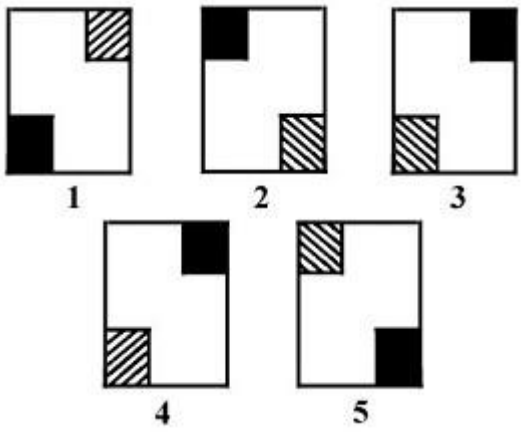
24. Исключите лишнюю фигуру.



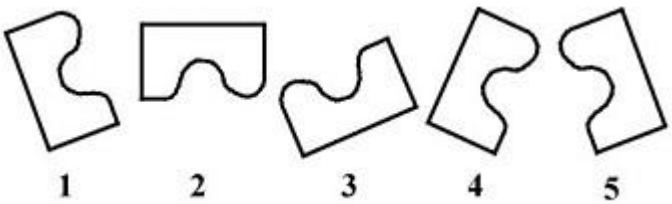
25. Исключите лишнюю фигуру.



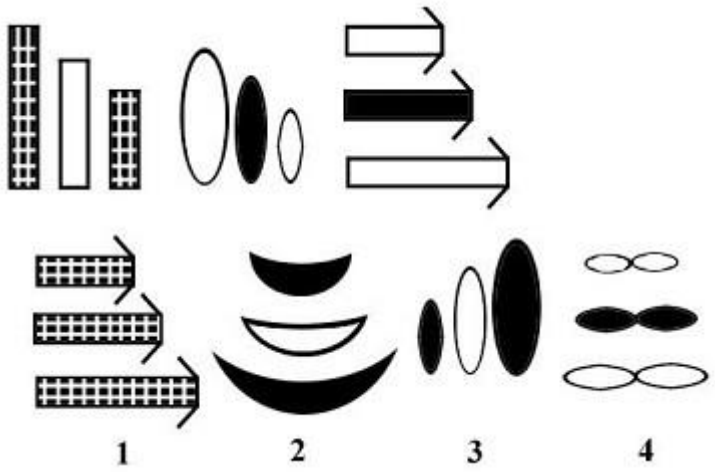
26. Исключите лишнюю фигуру.



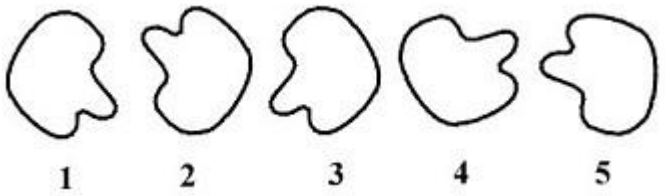
27. Исключите лишнюю фигуру.



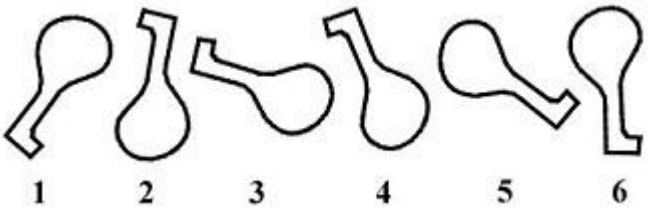
28. Вставьте пропущенную фигуру из четырех пронумерованных, имея в виду, что в верхнем ряду первая фигура относится ко второй так же, как третья к пропущенной.



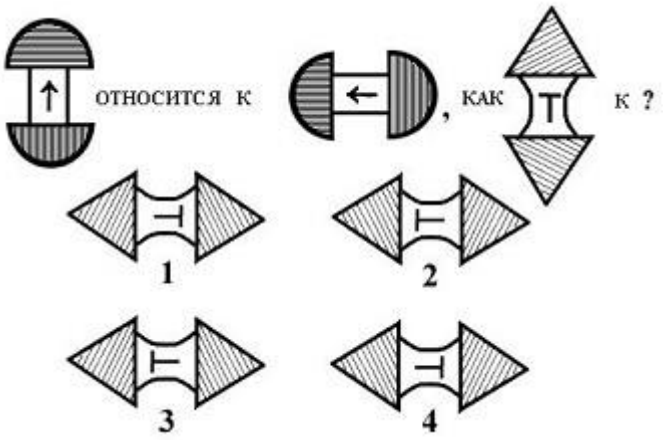
29. Исключите лишнюю фигуру.



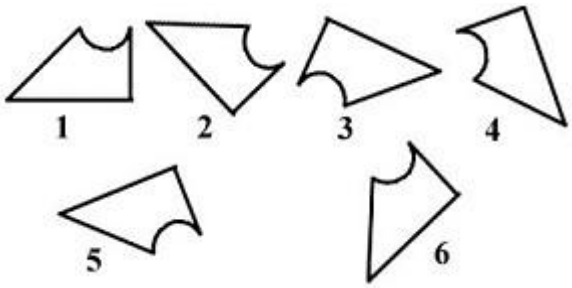
30. Исключите лишнюю фигуру.



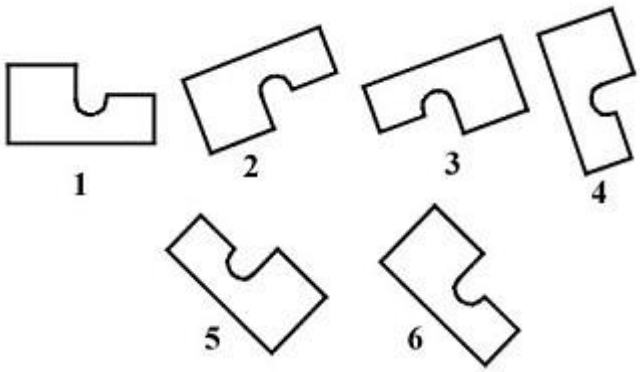
31. Вставьте пропущенную фигуру, выбрав ее из четырех пронумерованных.



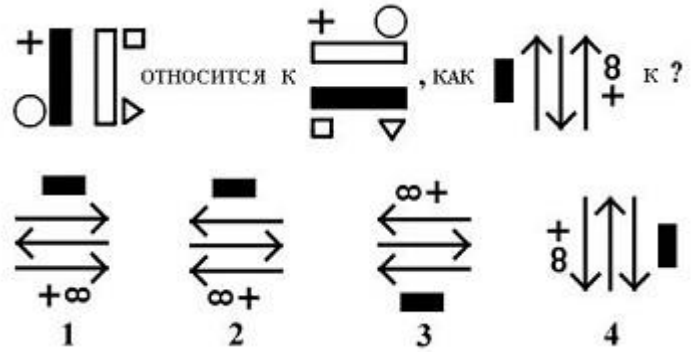
32. Исключите лишнюю фигуру.



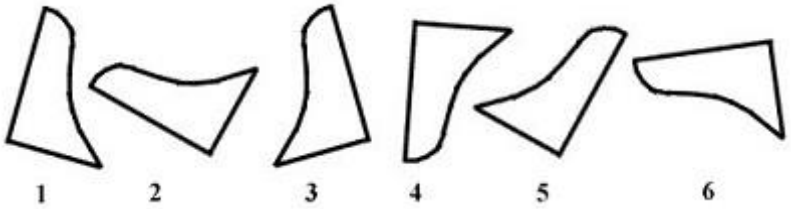
33. Укажите лишние фигуры.



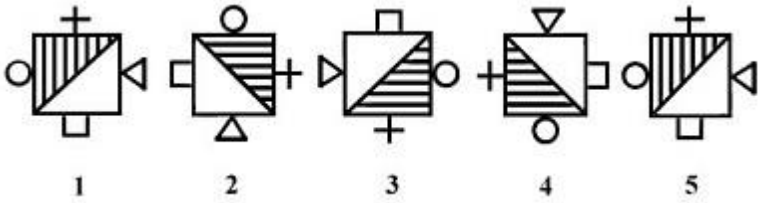
34. Вставьте пропущенную фигуру, выбрав ее из четырех пронумерованных.



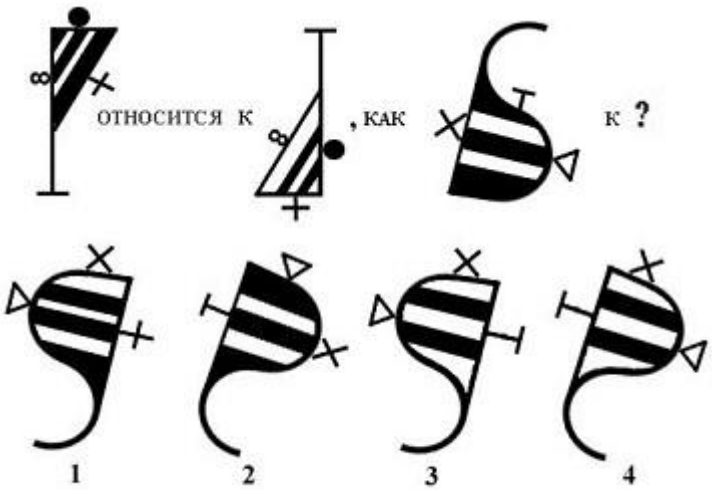
35. Укажите лишние фигуры.



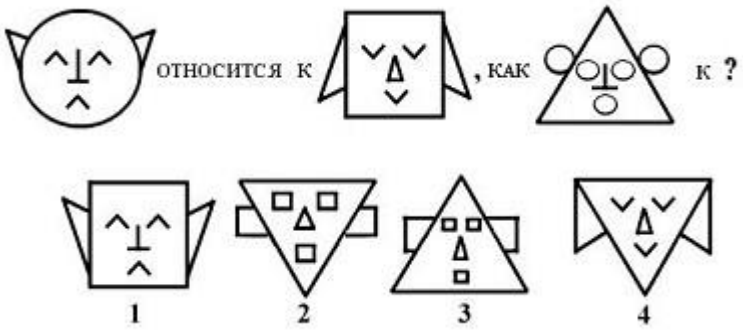
36. Исключите лишнюю фигуру.



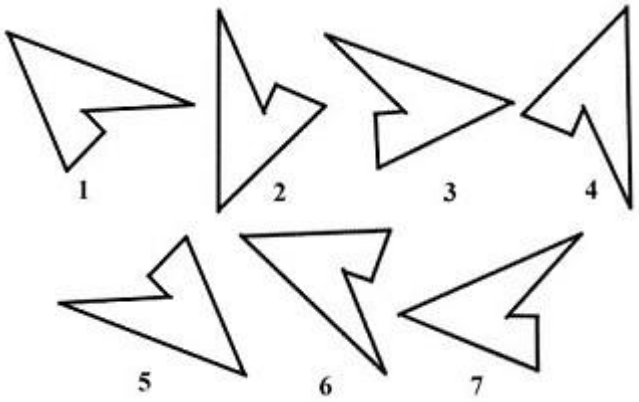
37. Вставьте пропущенную фигуру, выбрав ее из четырех пронумерованных.



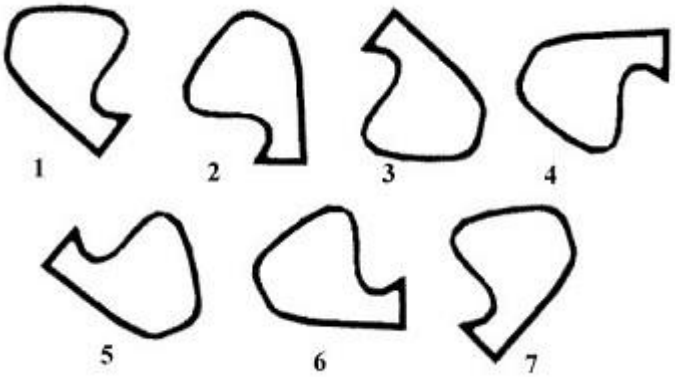
38. Вставьте пропущенную фигуру, выбрав ее из четырех пронумерованных.



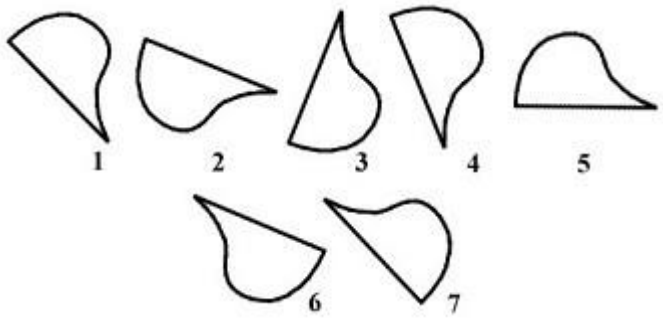
39. Укажите две лишние фигуры.



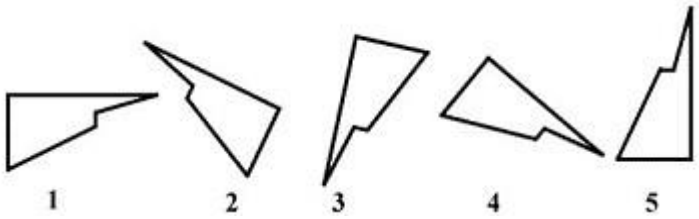
40. Найдите три лишние фигуры.



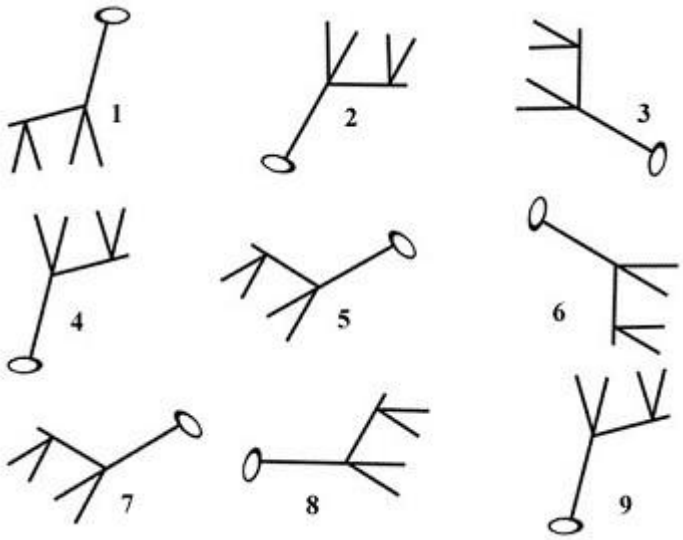
41. Найдите три лишние фигуры.



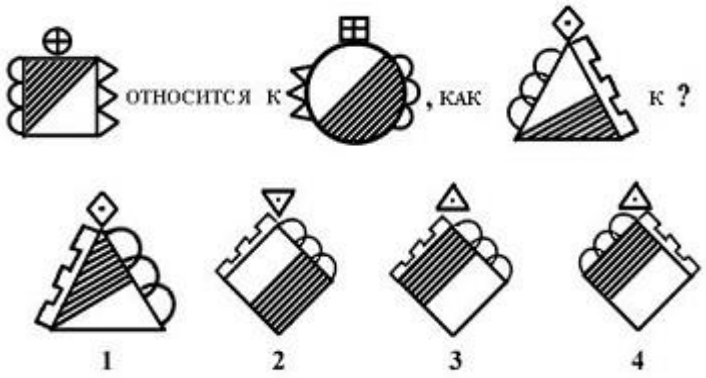
42. Укажите две лишние фигуры.



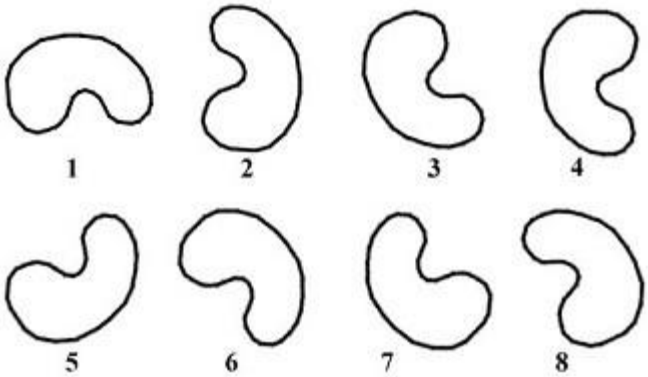
43. Исключите лишнюю фигурку.



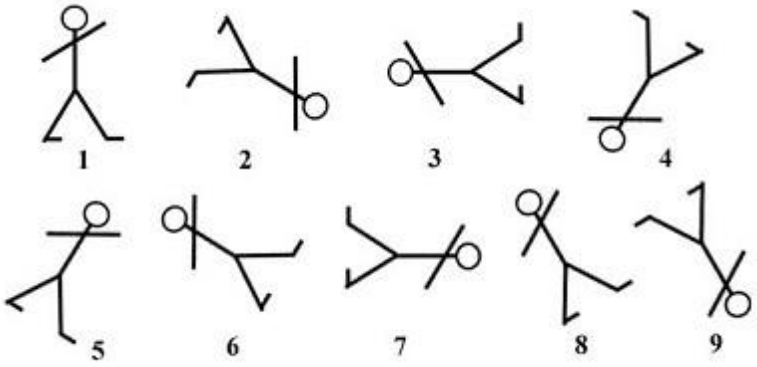
44. Вставьте пропущенную фигуру, выбрав ее из четырех пронумерованных.



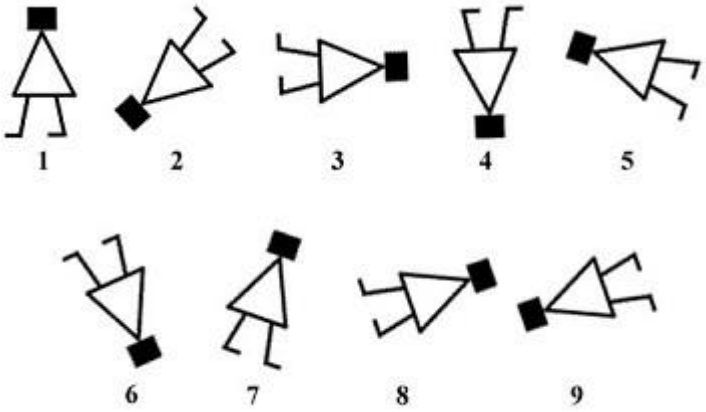
45. Найдите три лишние фигуры.



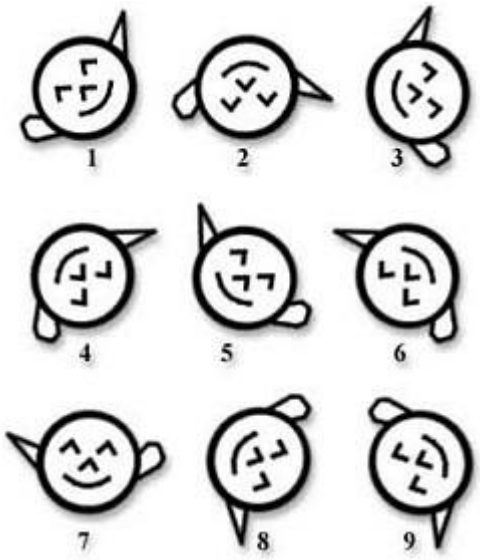
46. Исключите лишнюю фигурку.



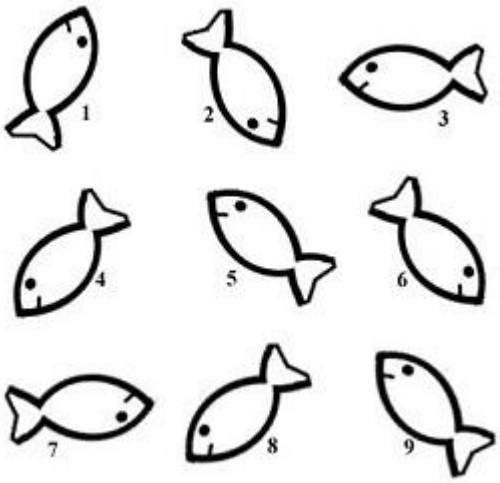
47. Найдите три лишние фигурки.



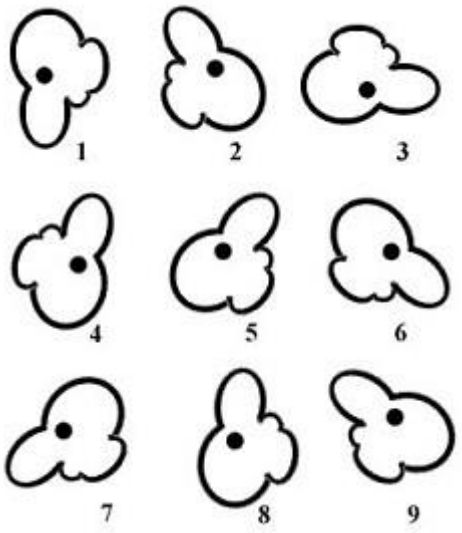
48. Найдите три лишние фигурки.



49. Исключите лишнюю фигурку.



50. Найдите три лишние фигурки.



Приложение Б

Перечень материалов дел, проанализированных автором

1. Приговор Невельского городского суда Сахалинской области от 14.10.2014 по делу № 1–95/2014.
2. Приговор Ванинского районного суда Хабаровского края от 07.11.2014 по делу № 1–194/14.
3. Приговор Кировского районного суда города Хабаровска от 07.09.2012 по делу № 1–58/2012.
4. Приговор Центрального районного суда города Комсомольска–на–Амуре от 21.05.2012 по делу № 1–625.
5. Приговор Якутского городского суда Республики Саха (Якутия) от 24.11.2011 по делу № 1–1598–11.
6. Приговор Фрунзенского районного суда города Владивостока от 05.04.2011 по делу № 1–96/2011.
7. Приговор Димитровградского городского суда Ульяновской области от 19.12.2014 по делу № 1–433/2014.
8. Приговор Ульяновского районного суда Ульяновской области от 27.08.2014 по делу № 1–2079/14.
9. Приговор Медведевского районного суда Республики Марий Эл от 10.07.2014 по делу № 1–2–27/2014.
10. Приговор Советского районного суда города Казани от 27.06.2014 № 1–393/14.
11. Приговор Медведевского районного суда Республики Марий Эл от 13.01.2014 по делу № 1–16/2014(1–229/2013).
12. Приговор Благовещенского районного суда Республики Башкортостан от 22.10.2013 по делу № 1–104/2013.
13. Приговор Ленинского районного суда города Нижний Новгород от 20.08.2013 по делу № 1–246/2013.

14. Приговор Ленинского районного суда города Пензы от 13.08.2012 по делу № 1–131/12.

15. Приговор Автозаводского районного суда города Тольятти от 03.07.2012

16. Приговор Фрунзенского районного суда города Саратова от 29.02.2012

17. Приговор Печорского городского суда Республики Коми от 06.06.2014 по делу № 1–194/2014.

18. Приговор Вологодского городского суда Вологодской области от 02.09.2013 по делу № 1–471/2013.

19. Приговор Череповецкого городского суда Вологодской области от 21.01.2013 по делу № 1–98/2013(1–1375/2012).

20. Приговор Московского районного суда города Санкт–Петербурга от 22.08.2011 по делу № 1–472/2011.

21. Приговор Изобильненского районного суда Ставропольского края от 21.05.2013 по делу № 1–156/2013.

22. Приговор Кисловодского городского суда Ставропольского края от 09.11.2012 по делу № 1–397/12.

23. Приговор Кировского районного суда города Омска от 02.12.2014 по делу № 1–759/2014.

24. Приговор Ленинского районного суда города Новосибирска от 28.05.2014 по делу № 1–403/2014.

25. Приговор Ленинского районного суда города Барнаула от 26.05.2014 по делу № 1–235/2014.

26. Приговор Советского районного суда города Красноярска от 13.11.2012

27. Приговор Ленинского районного суда города Нижнего Тагила от 16.01.2014 по делу № 1–93/2014(1–573/2013).

28. Приговор Елецкого районного суда Липецкой области от 15.08.2014 по делу № 1–77/2014.

29. Приговор Железнодорожного городского суда Московской области от 21.05.2014 по делу № 1–142/14.

30. Приговор Октябрьского районного суда города Тамбова от 14.02.2014 по делу № 1–85/14.

31. Приговор Орехово–Зуевского городского суда Московской области от 06.09.2013 по делу № 1–500/2013.

32. Приговор Гусь–Хрустального городского суда Владимирской области от 23.05.2013 № 1–40/2013.

33. Приговор Ленинского районного суда города Костромы от 10.04.2012 по делу № 1–58/2012.

34. Приговор Пушкинского городского суда Московской области от 27.12.2010 по делу № 1–524/10.

35. Приговор Ленинского районного суда города Владимира от 15.10.2010 по делу № 1–337/2010.

36. Приговор Волжского городского суда Волгоградской области от 23.09.2014 по делу № 1–941/2014.

37. Приговор Темрюкского районного суда Краснодарского края от 08.04.2014 по делу № 1–128/2014.

38. Приговор Октябрьского районного суда города Краснодара от 27.06.2013 по делу № 1–256/2013.

39. Приговор Центрального районного суда города Волгограда от 22.06.2011 по делу № 1–199/2011.

40. Апелляционное определение Московского городского суда от 06.05.2013 по уголовному делу № 10–2076

41. Апелляционное определение Московского городского суда от 23.09.2013 по уголовному делу № 10–8391

42. Приговор Железнодорожного районного суда города Красноярска от 24.06.2014 по делу № 1–12/2014(1–190/2013).

43. Приговор Пресненского районного суда города Москвы от 29.04.2014 по делу № 1–43/2014.

44. Приговор Хамовнического районного суда города Москвы от 01.08.2013 по делу № 1–100/2013.

45. Приговор Кировского районного суда города Курска от 15.05.2014 № 1–64/9–2014.

46. Приговор Савеловского районного суда города Москвы от 03.06.2013 № 1–226/13.

47. Приговор Димитровградского городского суда Ульяновской области от 19.12.2014 по делу № 1–433/2014.

48. Приговор Октябрьского районного суда города Самары от 10.06.2014 № 1–141/14.

49. Приговор Советского районного суда города Уфы от 05.05.2014 по делу № 1–209/2014.

50. Приговор Самарского районного суда города Самары от 18.04.2014 по делу № 1–34/2014.

51. Приговор Комсомольского районного суда города Тольятти от 18.03.2014 по делу № 1–125/2014.

52. Приговор Красноглинского районного суда города Самары от 06.03.2014 по делу № 1–76/2014.

53. Приговор Промышленного районного суда города Самары от 21.02.2014 по делу № 1–122/2014.

54. Приговор Ленинского районного суда города Самары от 12.04.2013 по делу № 1–73/2013.

55. Приговор Зеленодольского городского суда Республики Татарстан от 04.06.2013 по делу № 1–218/2013.

56. Приговор Благодарненского районного суда Ставропольского края от 15.12.2014 по делу № 1–183/14.

57. Приговор Андроповского районного суда Ставропольского края от 31.10.2014 по делу № 1–97/14.

58. Приговор Апанасенковского районного суда Ставропольского края от 28.08.2014 по делу № 1–78/2014.

59. Приговор Апанасенковского районного суда Ставропольского края от 11.08.2014 по делу № 1–72/2014.

60. Приговор Благодарненского районного суда Ставропольского края от 28.07.2014 по делу № 1–108/2014.

61. Приговор Кизилюртовского городского суда Республики Дагестан от 11.06.2014 по делу № 1–49/2014.

62. Приговор Братского городского суда Иркутской области от 12.11.2014 по делу № 1–549/2014.

63. Приговор Сургутского городского суда Ханты–Мансийского автономного округа – Югры от 16.12.2014 по делу № 1–1286/2014.

64. Приговор Златоустовского городского суда Челябинской области от 23.06.2014 по делу № 1–260/2014.

65. Приговор Талицкого районного суда Свердловской области от 19.06.2014 по делу № 1–92/2014.

66. Приговор Талицкого районного суда Свердловской области от 18.02.2014 по делу № 1–30/2014.

67. Приговор Зареченского районного суда города Тулы от 16.12.2014 по делу № 1–125/2014.

68. Приговор Железногорского городского суда Курской области от 21.10.2014 по делу № 1–243/2014.

69. Приговор Конаковского городского суда Тверской области от 24.07.2014 по делу № 1–171/2014.

70. Приговор Кировского районного суда города Курска от 15.05.2014

71. Приговор Хамовнического районного суда города Москвы от 15.05.2014 по делу № 1–49/2014.

72. Приговор Пресненского районного суда города Москвы от 16.05.2013 по делу № 1–176/2013.

73. Приговор Подольского городского суда Московской области от 23.04.2013 по делу № 1–232/13(78648).

74. Приговор Индустриального районного суда города Хабаровска от 18.07.2014 по делу № 1–726/2014.

75. Приговор Октябрьского районного суда города Пензы от 14.06.2012 по делу № 1–166/2012.

76. Приговор Выборгского гарнизонного военного суда от 19.02.2010 по делу № 14/10.

77. Приговор Курского районного суда Ставропольского края от 08.08.2013 по делу № 1–132/2013.

78. Приговор Мончегорского городского суда Мурманской области от 09.07.2010 по делу № 118–2010.

79. Приговор Советского районного суда города Челябинска от 24.12.2013 по делу № 1–588/2013.

80. Приговор Советского районного суда города Брянска от 14.10.2014 по делу № 1–162(14).

81. Приговор Хорошевского районного суда города Москвы от 01.12.2014 по делу № 1–587/2014.

82. Приговор Октябрьского районного суда города Тамбова от 29.05.2009 по уголовному делу № 1–324/09.

83. Приговор Мичуринского городского суда Тамбовской области по уголовному делу № 1–563/2004.

84. Приговор Новотроицкого городского суда Оренбургской области от 02.02.2012 по делу № 1–09/2012.

85. Приговор Бузулукского районного суда Оренбургской области от 03.12.2010 № 1(1)–208/2010.

86. Приговор Воткинского районного суда Удмуртской Республики от 05.10.2010 № 1–368(03/1423).

87. Приговор Волгодонского районного суда Ростовской области от 28.01.2010.

88. Приговор Куйбышевского районного суда города Омска от 05.02.2014 по делу № 1–53/2014(1–476/2013).

89. Приговор Приволжского районного суда города Казани от 28.02.2014 по делу № 1–13 2013;1–86 2012.

90. Приговор Первореченского районного суда города Владивостока от 28.04.2011 по делу № 1–240/11.

91. Постановление Московского городского суда от 05.12.2013 № 4у/2–9352.

92. Приговор Автозаводского районного суда города Тольятти по уголовному делу № 1–828/2004.

93. Приговор Сарапульского городского суда Удмуртской Республики от 05.08.2014 по делу № 1–139/14.

94. Приговор Юрьянского районного суда Кировской области от 21.04.2011 по делу № 1–52(21333).

95. Приговор Новгородского районного суда Новгородской области от 22.03.2011 по делу № 1–13/11.

96. Приговор Новозыбковского городского суда Брянской области от 18.07.2011.

97. Приговор Гусь–Хрустального городского суда Владимирской области по делу № 1–90/11.

98. Приговор Преображенского районного суда города Москвы от 10.02.2011.

99. Приговор Калужского районного суда Калужской области от 17.05.2010.

100. Приговор Кировского районного суда города Самары от 05.08.2010.

101. Приговор Советского районного суда города Томска от 10.03.2011.

102. Приговор Ленинского районного суда города Пензы от 25.05.2011.

103. Приговор мирового судьи судебного участка № 48 Самарской области от 06.06.2011.

104. Приговор Захаровского районного суда Рязанской области от 10.06.2011.

105. Приговор Егорьевского городского суда Московской области от 26.10.2011.

106. Приговор Октябрьского районного суда города Белгорода от 12.11.2012.

107. Приговор Новгородского районного суда Новгородской области от 21.02.2013.

108. Приговор Лысьвенского городского суда Пермского края от 14.03.2013.

109. Приговор Железнодорожного районного суда города Ульяновска от 09.04.2013.

110. Приговор Чертановского районного суда города Москвы от 19.07.2013.

111. Приговор мирового судьи судебного участка Ковдорского района Мурманской области от 26.08.2013.

112. Приговор Белгородского районного суда от 16.09.2013.

113. Приговор Октябрьского районного суда города Кирова от 11.12.2013.

114. Приговор Октябрьского районного суда города Кирова от 24.12.2013.

115. Приговор мирового судьи судебного участка Ковдорского района Мурманской области от 26.12.2013.

116. Решение по уголовному делу мирового судьи судебного участка № 1 Богдановичского судебного района Свердловской области 15.01.2014.

117. Постановление и.о. мирового судьи судебного участка № 49 города Находки от 16.01.2014.

118. Приговор Подольского городского суда Московской области

119. Приговор Индустриального районного суда города Барнаула от 28.03.2013.

120. Приговор Когалымского городского суда Ханты–Мансийского автономного округа от 24.01.2011.

121. Приговор Клинского городского суда Московской области от 18.10.2013.

122. Приговор Октябрьского районного суда города Кирова от 30.11.2012.

123. Приговор Чистопольского городского суда от 12.09.2013.

124. Приговор Московского районного суда города Чебоксары по делу №1–313/12.

125. Приговор Козульского районного суда красноярского края от 30.01.2014.

126. Приговор Центрального районного суда города Хабаровска от 18.10.2010.

127. Приговор Калининского районного суда Саратовской области от 16.07.2013.

128. Приговор Ленинского районного суда города Санкт–Петербурга от 07.07.2011.

129. Приговор Гагаринского районного суда города Москвы от 10.06.2013.

130. Приговор мирового судьи судебного участка № 7 по Ленинскому району города Уфы от 07.07.2011.

131. Приговор Никулинского районного суда города Москвы от 03.04.2013.

132. Приговор Ангарского городского суда Иркутской области от 30.05.2011.

133. Приговор Видновского городского суда Московской области от 30.10.2013.

134. Приговор Жирновского районного суда Волгоградской области от 18.07.2011. по делу № 1–105/2011.

135. Приговор Куединского районного суда Пермского края от 22.04.2013г. по делу № 1–34/2013.

136. Приговор Люблинского районного суда города Москвы от 14.11.2011.

137. Приговор Зареченского районного суда города Тулы от 25.12.2012.

138. Приговор Морозовского районного суда Ростовской области по делу № 1–3/11.

139. Приговор мирового судьи судебного участка № 280 района Вешняки города Москвы от 25.04.2012.

140. Приговор Ужурского районного суда Красноярского края от 22.08.2014.

141. Приговор Тобольского городского суда Тюменской области от 27.11.2013.

142. Приговор Железнодорожного районного суда города Самары от 14.06.2012.

143. Приговор Курганского городского суда по делу № 1–593/2012.

144. Приговор Коломенского городского суда Московской области от 24.05.2011.

145. Приговор Дальнереченского городского суда Приморского края от 17.06.2011.

146. Приговор Октябрьского районного суда города Уфы от 10.11.2010.

Приложение В
Словарь терминов

Мошенничество, совершаемое с использованием телекоммуникационного оборудования – категория противоправных действий, объединяющая в себе конкретные эпизоды мошенничества, в ходе совершения которого злоумышленником использовались: технические средства и оборудование, предоставляющее доступ к сетям мобильной связи, сети Интернет; компьютеры; программируемые технические устройства и т. д. Объединяет в себе такие виды мошенничества, как кардинг, фишинг, телефонное мошенничество, мошенничество в системах ДБО, мошенничество с платежными терминалами и т. п.

Эмиссия банковских карт – деятельность по выпуску банковских карт, открытию счетов и расчетно–кассовому обслуживанию клиентов при совершении операций с использованием выданных им банковских карт.

Эмбоссирование – процесс механического выдавливания на лицевой стороне пластиковой карты (или другом листовом материале) различной информации. Например, для банковских карт это номер карты, срок действия, имя и фамилия клиента, название компании (для корпоративных клиентов).

Повторное эмбоссирование – использование уже существующей банковской карты для создания на ее основе «дубликата» другой банковской карты.

Карта с магнитной полосой – тип карт, отличающийся наличием магнитной полосы. Магнитная полоса предназначена для хранения какой–либо информации. Запись информации выполняется путем намагничивания крошечных частиц, находящихся на поверхности полоски и содержащих железо (магнитный материал). Чтение информации выполняется путем проведения полосы по магнитной головке.

Процессинговые центры – юридическое лицо или его структурное подразделение, обеспечивающее информационное и технологическое взаимодействие между участниками расчетов.

Социальная инженерия – совокупность приемов, методов и технологий создания такого пространства, условий и обстоятельств, которые максимально эффективно приводят к конкретному необходимому результату, с использованием социологии и психологии. Для России это явление достаточно новое, оно ранее рассматривалось как метод управления действиями человека без использования технических средств, который основан на использовании слабостей человеческого фактора и считается очень разрушительным. Зачастую социальную инженерию рассматривают как незаконный метод получения информации, однако это не совсем так. Если рассматривать современную профессиональную социальную инженерию, то область ее применения вполне законна – например, она помогает достичь изначально недостижимый результат или «программировать» для совершения позитивных и полезных действий конкретного человека. Конечно, сегодня социальную инженерию зачастую используют в интернете для получения закрытой информации или информации, которая представляет большую ценность. Но современные соц–инженеры используют свои навыки для повышения результатов в бизнесе и жизни.

Кардинг (англ. *carding*) – вид мошенничества, при котором производится операция с использованием платежной карты или ее реквизитов, не инициированная или не подтвержденная ее держателем. Реквизиты платежных карт, как правило, берут со взломанных серверов интернет–магазинов, платежных и расчетных систем, а также с персональных компьютеров (либо непосредственно, либо через программы удаленного доступа, «трояны», «боты» с функцией формграббера). Кроме того, наиболее распространенным методом похищения номеров платежных карт на сегодня является фишинг (англ. *phishing*, искаженное «*fishing*» – рыбалка) – создание мошенниками сайта, который будет пользоваться доверием у пользователя,

например – сайт, похожий на сайт банка пользователя, через который и происходит похищение реквизитов платежных карт. Частным случаем кардинга является скимминг (от англ. *skim* – снимать сливки), при котором используется скиммер – инструмент злоумышленника для считывания, например, магнитной дорожки платежной карты.

Даркнет (англ. *DarkNet*) – частная сеть, соединения которой устанавливаются только между доверенными пирами, иногда именующимися как «друзья», с использованием нестандартных протоколов и портов.

Одноранговые сети – однора́нговая, децентрализо́ванная, или пи́ринговая (англ. peer–to–peer, P2P – равный к равному) сеть – это оверлейная компьютерная сеть, основанная на равноправии участников. Часто в такой сети отсутствуют выделенные серверы, а каждый узел (peer) является как клиентом, так выполняет и функции сервера.

Скоринговые системы – это система оперативной оценки клиента (потенциального заемщика), которой преимущественно пользуются розничные банки и микрофинансовые компании.

CNP–фрод (англ. *Card Not Present*) – мошенничество, совершаемое путем платежной транзакции без предъявления карты, то есть в условиях, когда в точке совершения транзакции отсутствует не только сама платежная карта, но и ее держатель.

EMV (Europay + MasterCard + VISA) – международный стандарт для операций по банковским картам с чипом. Этот стандарт разработан совместными усилиями компаниями Europay, MasterCard и Visa, чтобы повысить уровень безопасности финансовых операций.

Основное отличие для пользователя карты стандарта EMV – преимущественное требование ввода ПИН–кода при проведении любого платежа через терминал (например, в магазинах, ресторанах). Тем не менее данное требование не является обязательным: при желании банк–эмитент может настроить CVM–лист чип–карты так, что в первую очередь она будет запрашивать подпись.

Стандарт EMV определяет физическое, электронное и информационное взаимодействие между банковской картой и платежным терминалом для финансовых операций. Существуют стандарты, основанные на ISO/IEC 7816 для контактных карт, и стандарты ISO/IEC 14443 для бесконтактных карт.

Кей–шарк – объединенное название для устройств и программ, запоминающих последовательность (в некоторых случаях также: время, частоту) нажатия клавиш на клавиатуре компьютера.

Страта социальная (от лат. *Stratum* – слой, пласт) – элемент социальной структуры (социальный слой или группа), объединенный неким общим общественным признаком (имущественным, профессиональным или иным).

Страты конструируются на основании многомерной классификации и часто организуются в иерархический порядок.

Критерии конструирования страт зависят от целей исследования и от того, что считается важным в данном определенном исследовании и данной определенной модели. Это может быть один признак: пол, возраст, уровень дохода, уровень образования, область интересов, место проживания и т. п., или сочетание нескольких признаков (характеристик).