Научная статья
УДК 342.23
DOI: 10.35854/2219-6242-2023-4-565-577

Особенности преступлений, совершаемых с использованием информационно-телекоммуникационных технологий или в сфере компьютерной информации в современных условиях

Ольга Викторовна Аникаева[1], Игорь Николаевич Бобровничий[2]✉
[1] АО «Альфа банк», Барнаул, Россия
[2] Северный институт — филиал Всероссийского государственного университета юстиции (РПА Минюста России), Петрозаводск, Россия
[1] olenka_anikaeva@mail.ru
[2] bobrovnichyin@mail.ru✉

Аннотация. В статье исследованы особенности преступлений, совершаемых с использованием информационно-телекоммуникационных технологий или в сфере компьютерной информации в современных условиях, а также определены ведущие направления и меры противодействия таким преступлениям. Проанализированы виды преступлений и их статистика. Особое внимание уделено личности преступников, их классификации. Изучены основные причины преступлений и их связь с поведением жертвы.

Ключевые слова: преступления, совершаемые с использованием информационно-телекоммуникационных технологий или в сфере компьютерной информации; хакер, киберпреступник, киберпреступность, мошенничество, IT-мошенничества, IT-преступления, кибертерроризм, кибербуллинг, кибербезопасность, причины преступлений, личность преступника, жертва преступления, направления и меры противодействия преступлениям

Для цитирования: Аникаева О. В., Бобровничий И. Н. Особенности преступлений, совершаемых с использованием информационно-телекоммуникационных технологий или в сфере компьютерной информации в современных условиях // Социология и право. 2023. Т. 15. № 4. С. 565–577. https://doi.org/10.35854/2219-6242-2023-4-565-577

Original article

Characteristics of crimes committed with the use of information and telecommunication technologies or in the sphere of computer information in modern conditions

Olga V. Anikayeva[1], Igor N. Bobrovnichiy[2]✉
[1] "Alfa Bank" JSC, Barnaul, Russia
[2] Northern Institute — a branch of the All-Russian State University of Justice (RLA of the Ministry of Justice of Russia), Petrozavodsk, Russia
[1] olenka_anikaeva@mail.ru
[2] bobrovnichyin@mail.ru✉

Abstract. The article studies the features of crimes committed with the use of information and telecommunication technologies or in the sphere of computer information in modern conditions, as well as identifies the leading directions and measures to counteract such crimes.

Types of crimes and their statistics are analyzed. Special attention is paid to the personality of criminals, their classification. The main causes of crimes and their connection with the behavior of the victim are studied.

Keywords: crimes committed with the use of information and telecommunication technologies or in the sphere of computer information; hacker, cybercriminal, cybercrime, fraud, IT-fraud, IT-crime, cyberterrorism, cyberbullying, cybersecurity, causes of crimes, personality of the criminal, victim of crime, directions and measures of counteraction to crimes

For citation: Anikayeva O.V., Bobrovnichiy I.N. Characteristics of crimes committed with the use of information and telecommunication technologies or in the sphere of computer information in modern conditions. *Sociology and Law.* 2023;15(4):565-577. https://doi.org/10.35854/2219-6242-2023-4-565-577

Введение

Как известно, развитие компьютерных технологий порождает развитие компьютерной преступности. Важнейшей частью национальной безопасности России является обеспечение безопасности неотъемлемых инфраструктурных, коммуникационных и информационных систем, а также усиление защиты корпоративных и персональных сетей данных [1].

Согласно официальным данным Главного информационного аналитического центра Министерства внутренних дел Российской Федерации (ГИАЦ МВД России), в 2019 г. зарегистрировано 90 587 преступлений, совершаемых с использованием компьютерных и информационно-телекоммуникационных технологий, в 2020 г. — 174 674, в 2021 — 294 409. Показатели преступлений, совершенных с использованием информационно-телекоммуникационных технологий или в сфере компьютерной информации, значительно возросли: с 14,5 % в 2019 г. до 25,0 % в 2020 г. Из общего числа таких преступлений 52,4 % относятся к категории тяжких и особо тяжких, что составляет 267 600 (+87,5 %); 58,8 % совершены через интернет (300 300; +91,3%), а 42,9 % — с использованием средств мобильной связи (218 700; +88,3 %). В январе — феврале 2021 г. количество выявленных IT-преступлений увеличилось на 29,4 % по сравнению с предыдущим годом, в том числе совершенных через интернет — на 48,3 %, а через мобильные устройства — на 32,6 %. Если в январе — феврале 2020 г. удельный вес преступлений в IT-сфере составлял 19,3 %, то в первые два месяца текущего года он увеличился до 26,3 %. Рост преступности произошел в основном за счет телефонного и интернет-мошенничества. Телефонные онлайн-мошенники похитили у граждан более 150 млрд руб. [2].

Сегодня насчитывается много видов компьютерных преступлений: производство и распространение компьютерных вирусов и вредоносных программ, разглашение конфиденциальной информации, коммерческой тайны, личной информации, взлом чужого доменного имени и ряд других. Глава 28 «Преступления в сфере компьютерной информации» дополнена в Уголовный кодекс (УК) РФ 1996 г. Она содержит четыре состава преступления (ст. 272–274.1). Глава 21 УК РФ также дополнена ст. 159.6 «Мошенничество в сфере компьютерной информации». Комплексная оценка понятия «компьютерная информация» требует знаний в области коммуникации и киберпреступности, понимания их диапазона.

Следует отметить, что около половины из зарегистрированных преступлений, совершенных с использованием информационно-телекоммуникационных технологий или в сфере компьютерной информации (48,14 %, то есть 249 249 из 517 722), составляют мошенничества, предусмотренные ст. 159, 159.3, 159.6 УК РФ. 95,71 % (238 560) из них — это мошенничества, совершенные с использо-

ванием информационно-телекоммуникационных технологий или в сфере компьютерной информации (ст. 159 УК РФ); 4,11 % (10 258) — мошенничества с использованием электронных средств платежа (ст. 159.3 УК РФ). Из 311 211 мошенничеств по ст. 159 УК РФ более 80 % (80,27 % — 249 822) зарегистрированы по ч. 2–7 ст. 159 УК РФ, свыше 60 % из которых совершены по ч. 2 и ч. 4 ст. 159 УК РФ.

Краткая характеристика состояния преступности в России за январь — декабрь 2021 г. свидетельствует о существенном увеличении ущерба от преступлений (по оконченным и приостановленным уголовным делам), то есть +62,7 % (834,5 млрд руб.), росте регистрируемых мошенничеств (+1,2 % — 339,6 тыс. из 2 004 404) и существенных их изменениях (увеличении тяжести, росте количества преступлений, совершенных с использованием информационно-телекоммуникационных технологий или в сфере компьютерной информации, групповом характере, появлении новых способов обмана и злоупотреблении доверием и т. д.).

Практически 40 % (38,58 %) раскрытых мошенничеств, совершенных организованной группой либо преступным сообществом (преступной организацией), — это преступления с применением информационно-телекоммуникационных технологий (3 012) [3]. Меры криминалистической превенции и иной профилактики в современных условиях эпидемиологических рисков и угроз существенно сократили количество (–97,1 %) зарегистрированных мошенничеств с использованием платежных карт (ст. 159.3 УК РФ).

Президент РФ В. В. Путин на расширенном заседании коллегии МВД России справедливо говорил «о новых вызовах, связанных с проникновением криминала в сферу информационных технологий и телекоммуникаций. Количество преступлений в этой сфере ежегодно растет. В результате действий кибермошенников урон несут отечественные компании. И, что вызывает особую остроту общественной реакции, с потерями средств и накоплений, с невосполнимым моральным ущербом сталкиваются наши граждане во все большем и большем количестве. Жертвами преступников становятся пенсионеры, многодетные семьи, люди с ограниченными возможностями по здоровью» [4].

По статистике, в январе — марте 2022 г. количество IT-преступлений возросло на 83,9 %, что связано с последствиями введенных ограничительных мер из-за массового распространения новой коронавирусной инфекции COVID-19. Всего в этот период зарегистрировано 101 537 преступлений данного вида. По состоянию на январь 2023 г. также сохраняются тенденции роста числа IT-мошенничеств (рост на 12 %) [5].

Теория

Компьютерные преступления вызывают все большую тревогу в современном цифровом мире, с постоянно расширяющимся разнообразием вредоносных действий — от кибербуллинга и кражи личных данных до взлома и манипулирования последними. Кроме того, компьютерные преступления могут включать в себя и более традиционные формы преступной деятельности, такие как мошенничество, эксплуатация детей и терроризм. С распространением новых технологий и устройств преступники смогли найти новые способы использования уязвимых систем для получения финансовой выгоды или других вредоносных целей. Сегодня особенно важно, чтобы организации предпринимали упреждающие шаги для защиты от этих все более изощренных угроз.

Для совершения таких преступлений существует много способов, чтобы избежать ответственности. Например, сеть Интернет позволяет преступнику оста-

ваться незамеченным. Благодаря своей способности действовать удаленно, преступники используют различия в правовых системах разных стран, что может дать возможность остаться безнаказанным. Свои обороты набирает и кибертерроризм. Вышеперечисленное преступник может осуществить, используя лишь интернет и компьютер жертвы.

Предполагается, что компьютерные преступления относятся к действиям, нарушающим безопасность данных и систем в виртуальном мире. Тем не менее доказано, что это влияет на реальные социальные связи. Компьютерные преступления представляют собой существенную угрозу безопасности данных и систем в виртуальном мире. По мере роста нашей зависимости от технологий растет и риск злонамеренных атак на наши цифровые сети, которые могут привести к значительным сбоям в работе и финансовым потерям. К сожалению, киберпреступники становятся все более изощренными. Поэтому важно, чтобы частные лица и организации принимали соответствующие меры для защиты от потенциальных угроз. Инвестируя в надежные стратегии кибербезопасности, они могут обеспечить сохранность своих данных и их защиту от злоумышленников.

Кроме того, для совершения преступления необходима сеть, а с появлением интернета люди в разных уголках мира получили возможность обмениваться информацией на различных платформах. Однако это не только дает множество преимуществ человечеству, но и открывает возможности для преступников совершать преступления с гораздо большей легкостью [6].

Всемирный рост обмена информацией через сети увеличил вероятность того, что граждане, компании и правительства станут мишенью для киберпреступников. Граждане особенно уязвимы к атакам на их персональные компьютеры или мобильные устройства, посредством которых хакеры собирают личные данные и распространяют незаконные материалы. Предприятия могут подвергаться вредоносным атакам на свои банковские системы, веб-сайты или платформы электронной коммерции. Правительства могут пострадать от кибератак на ключевые системы государственного управления и взлома оборудования критически значимой инфраструктуры государственных учреждений.

Результаты и обсуждение

Следует помнить о том, что компьютерные преступления характеризуются исключительно высокой степенью латентности, которая может быть как искусственной, так и естественной. Тем не менее она служит важным фактором, способствующим совершению этих преступлений.

Если речь идет о естественной латентности, о ней знают лишь участвующие в преступной деятельности. Часто в случаях, связанных с кражей компьютерной информации и данных на компьютерах и компьютерных носителях, жертвы не знают о том, что произошло нечто противозаконное. В качестве типичного приведем следующий пример. Так, согласно распределенным ролям, неустановленное лицо (лица), действуя в составе группы лиц по предварительному сговору с Ж., приобрели вредоносную программу и оборудование для ее распространения. Ж., согласно своей преступной роли, с целью совершения преступления в группе лиц по предварительному сговору, приобрел у граждан, которые не подозревали о преступных намерениях преступной группы, банковские карты, а затем предоставил информацию о реквизитах счетов указанных банковских карт неустановленному лицу. После получения реквизитов счетов банковских карт, используя указанную информацию, неустановленное лицо (лица) стало рассылать на абонентские номера телефонов неограниченного числа граждан SMS-сообщения,

содержащие ссылку на вредоносную программу. В дальнейшем неустановленным способом денежные средства потерпевших переводили на счета банковских карт, приобретенных Ж. у различных граждан, неосведомленных о преступных намерениях указанной преступной группы. Иными словами, посредством сети Интернет путем ввода, модификации компьютерной информации либо иного вмешательства в функционирование средств хранения, обработки или передачи компьютерной информации либо информационно-телекоммуникационных сетей, помимо воли владельца счета, тайно и умышленно, из корыстных побуждений, похищали денежные средства путем незаконного их перевода со счетов банковских карт потерпевших на подконтрольные Ж. счета банковских карт [7].

В целях выявления рассматриваемых преступлений и их профилактики следует определить, какие черты личности приводят к преступному поведению в интернете [8]. В основном авторы классифицируют криминальные группы населения в зависимости от уровня владения компьютером:

1. Хакеры. Лица с развитыми техническими способностями для совершения данного вида преступлений, такие как программисты, операторы терминалов, эксперты по безопасности компьютерных систем, системные администраторы и другие лица, обладающие значительным опытом в использовании компьютерных технологий. Хакеров часто воспринимают как людей с развитыми техническими способностями, но они привносят в работу гораздо больше, чем умение работать с компьютером. Они используют свой опыт, чтобы мыслить творчески и решать проблемы новыми и инновационными способами, расширяя границы возможного. Их присутствие может быть особенно ценным во многих отраслях, от кибербезопасности до онлайн-торговли, помогая компаниям опережать события и принимать более обоснованные решения. В итоге хакеры дают колоссальные знания, которые помогают приблизить светлое будущее для всех.

2. Пользователи. Правонарушители, которые не обладают значительными знаниями, но все-таки совершают мошенничество, используя поверхностные знания и приобретенные программные средства, электронные устройства [9].

Изучение судебных решений показало, что большинство лиц, совершивших экономические киберпреступления, не имеют постоянной работы, 51 % из них оказываются в этой категории. Как правило, их признают виновными в мошенничестве (по ст. 159.3 и 159.6 УК РФ). Остальные 49 % — это в основном работники низшего и среднего звена (продавцы как в обычных, так и в интернет-магазинах), иногда чиновники (бухгалтеры) и IT-специалисты (персонал компьютерных кафе, инженеры-программисты, старшие техники-программисты).

По мнению В. В. Коломинова, интернет-мошенников можно разделить на три группы, в зависимости от их квалификации: представители обычного типа действуют в поверхностном интернете (например, через каналы мобильной связи или сайты социальных сетей); продвинутых мошенников можно найти в «даркнете», они исследуют утечку данных для вымогательства денег; наконец, такие, которые специализируется на схемах fly-by-night или букмекерских конторах [10].

Профессионалы — это мошенники, занимающие теневую сферу и работающие в одиночку, их возраст неизвестен, поскольку информация отсутствует. У них много свободного времени, и их метод работы — обманывать себе подобных, распространяя мошеннические планы. Их атаки целенаправленны, и они ищут бреши в системе безопасности финансовых учреждений для осуществления противоправной деятельности, повышая уровень латентной преступности.

При изучении различных типов киберпреступников можно выделить две отдельные группы: хакеры и корыстные преступники. Указанные категории

не являются взаимоисключающими: среди корыстных киберпреступников — и хакеры, и обычные мошенники. Аналогично среди хакеров можно встретить как корыстных, так и бескорыстных (например, таких, которые действуют с учетом мотива вандализма).

Исходя из места совершения преступления, людей можно в целом определить как принадлежащих к трем различным классам преступников. Одни активны только в виртуальном пространстве: их преступные наклонности сформировались в крайне нелегальной среде киберпространства, поэтому, устранив плохие элементы, возможно, они не представляют существенной опасности для общества по сравнению с реальными преступниками.

Преступное поведение других разделено между физической и цифровой сферами: такие преступники обычно имеют более укоренившуюся преступную психологию, на которую не оказывает сильного влияния их киберсреда. Наконец, третьи — преступники, ранее совершавшие преступления в некибернетической сфере, но в настоящее время занимающиеся киберпреступностью. Данная категория преступников появилась благодаря технологическому прогрессу, позволяющему им получать доступ к различным видам информационных ресурсов. Поскольку многие из них обладают эффективными организационными возможностями, они привлекают специализированную помощь, концентрируя свои усилия на увеличении прибыли и укреплении собственной власти [11].

Нельзя не обратить внимание на психологическую составляющую онлайн-преступлений. Поскольку жертва не может видеть преступника или взаимодействовать с ним лично, невозможно определить его возраст. Таким преступником может быть несовершеннолетний или даже студент, но в качестве преступника может выступать и пожилой человек. Специалисты в области криминалистики подразделяют тех, кто совершает подобные преступления с помощью кибертехнологий, на определенные категории: компьютерные преступники, «белые воротнички», компьютерные шпионы и хакеры/программисты по принуждению [12]. Разнообразие мотивов и целей, стоящих за преступлениями этой категории, очень велико, и чаще всего ими движет корысть. Иными причинами могут быть возмездие, вражда, вандализм, желание нанести ущерб деловой репутации конкурента, розыгрыш или сокрытие другого правонарушения.

Н. Н. Фетодов предлагает при формировании образа преступника, использующего компьютерные технологии, исходить из того, что его понимание методов и приемов является осознанным и высоким. Таких преступников он называет «хакерами», «инсайдерами», «белыми воротничками», «электронными бизнесменами», а тех, чьей мотивацией служит антисоциальная психопатия — «антисоциальным типом».

С точки зрения криминологической типологии лица с профессиональным опытом или привычкой составляют большинство преступников, а неустойчивый тип появляется редко; халатные или случайные типы практически не встречаются. Если речь идет о личности правонарушителя, необходимо учитывать и внутренние, и внешние факторы. Внутренняя сторона проявляется через социально-психологические черты и атрибуты человека в его взаимодействии с социальным миром. Внешние элементы проявляются через антисоциальное поведение индивида.

Таким образом, указанные два аспекта тесно переплетены между собой. Чтобы составить полное представление о личности преступника, мы должны рассмотреть тип преступления, совершенного с применением современных технологий. Для совершения такого рода преступлений необходимо не только обладать определенными знаниями и навыками, но и уметь их использовать, совершенствовать,

оставаясь в курсе достижений информационных технологий; такие возможности, как правило, существуют лишь в крупных городах или региональных столицах, в которых внедрены современные достижения.

В крупных, развитых городах страны компьютерные преступления совершают в основном представители IT-персонала (59,3 %). Зачастую эти люди имеют достойное материальное положение, перспективную карьеру и не испытывают материальных трудностей. Тем не менее они решают участвовать в преступной деятельности, которая приводит к потерям для тех, кто происходит из более бедных слоев населения. Безработные и студенты составляют меньший процент киберпреступников — 28,3 % и 11,4 % соответственно. Такие преступники обычно имеют высокий уровень образования (у многих из них высшее или неоконченное высшее образование), что говорит об их потребности в специальных знаниях и навыках программирования. Это значительно больше, чем у других типов преступников, что говорит об их технической «подкованности».

Как известно, большинство преступных действий совершают мужчины. Тем не менее наблюдается стремительный рост количества женщин в определенных профессиях (речь идет о секретарской работе, бухгалтерских и канцелярских задачах). Это можно объяснить отсутствием «компьютеризации» среди пожилых людей, а также тем, что компьютерную грамотность прививают детям с ранних лет. К наиболее плодотворным возрастным группам для преступной деятельности отнесены лица в возрасте от 16 до 25 лет и от 26 до 35 лет соответственно. Современные исследователи активно изучают личности тех, кто совершает так называемые традиционные преступления с применением современных технологий.

Р. И. Дремлюга исследует личности совершающих интернет-преступления. Он обнаружил, что большинство преступников — мужчины 18–24 лет. Кроме того, 80 % среди них не имели судимостей, и они сопротивляются обнаружению правоохранительными органами. Основной мотивация этих преступлений — денежная выгода, хотя месть, озорство и самоутверждение также сыграли свою роль в 22 % случаев. Большинство из таких людей не получили образования в области современных компьютерных технологий; а вместо этого они обучаются на интернет-ресурсах [13].

Как правило, они не имеют криминального прошлого и охотно принимают на себя ответственность за свои действия. Несмотря на признание своей вины, такие люди часто не осознают преступность допущенных поступков. Это качество представлено как вероятностная модель, а не как абсолютная истина. В современных условиях данные виды преступлений совершают лица из разных слоев общества в разных регионах России, что затрудняет формирование точного «словесного портрета» преступника.

Ю. Р Орлова и О. Н. Гусева утверждают, что любое преступление в итоге определяется прошлым опытом человека, который формирует его взгляды и поведение в определенных конфликтных ситуациях, что впоследствии приводит его к опасным решениям. Наконец, исследование А. Х. Боташевой показало, что типичные преступники — мужчины (79 %) 35–40 лет (30 %), которые женаты (66 %) и имеют высшее образование (52 %) [14].

Упомянутые выше качества направлены на лиц, разбирающихся в новейших информационных технологиях. Преступники в данной сфере используют сложные и комбинированные стратегии, специализируются на вопросах из области финансов и экономики, понимают нюансы банковского рынка, знают банковские скоринговые системы, а также инструменты оценки кредитоспособности заемщика. Все это говорит о том, что преступники либо имеют опыт работы в банковском секторе, либо интенсивно изучали его. Это свидетельствует и о высокой

степени интеллекта, проницательности преступника, что подтверждается исследованиями [15].

Анализ данных уголовных дел и приговоров позволяет предположить, что существует общий профиль для данного типа преступников. Мужчины чаще вовлечены в эту деятельность, чем женщины, а их возраст обычно колеблется между 20 и 40 годами. Интеллектуальные способности этих преступников обычно умеренны или низки, о чем свидетельствуют их методы, используемые для планирования, осуществления и сокрытия преступлений.

Их знания в области компьютерного оборудования и программного обеспечения, как правило, ограничены. Они часто являются самоучками. Основным мотивом таких действий обычно служит жадность, к тому же значительную долю из них составляют люди, ранее совершавшие традиционные преступления. Этот вид незаконной деятельности связан с использованием компьютеров, компьютерных сетей или сетевых устройств в незаконных целях. Она может быть организована бандами или может осуществляться отдельными лицами, находящимися в местах лишения свободы.

Приведем пример. В период нахождения Г. в Исправительной колонии Управления Федеральной службы исполнения наказаний (УФСИН) России у него возник умысел, направленный на мошенничество. Г. получил доступ к мобильному устройству сотовой связи (смартфону с сим-картой мобильного оператора) и осуществлял при помощи данного устройства выход в сеть Интернет, посредством которой при помощи неустановленного стороннего вредоносного программного обеспечения для операционной системы «Андроид», путем ввода, модификации компьютерной информации и иного вмешательства в функционирование средств хранения, обработки компьютерной информации, получил удаленный доступ к отдельным функциям указанной операционной системы и, соответственно, доступ к мобильному устройству сотовой связи — смартфону, принадлежащему потерпевшему Ф. Тем самым Г. совершил несанкционированный перевод, то есть хищение денежных средств, с банковского счета банковской карты, открытого на имя Ф. в отделении Центрально-Черноземного банка ОАО «Сбербанк России», на банковский счет банковской карты, открытый на имя Ж. в структурном подразделении Сибирского банка ОАО «Сбербанк России», не посвящая последнюю в свой преступный умысел. Продолжая реализацию преступного умысла, направленного на хищение чужого имущества, находясь в Исправительной колонии, Г. в дневное время, используя неустановленное стороннее вредоносное программное обеспечение для операционной системы «Андроид», получил удаленный доступ к отдельным функциям указанной операционной системы и, соответственно, доступ к мобильному устройству сотовой связи, принадлежащему Ж.; совершил несанкционированный перевод денежных средств с банковского счета на банковский счет банковской карты, открытый на имя Д. в Среднерусском банке ОАО «Сбербанк России», не посвящая последнюю в свой преступный умысел.

С целью незаконного распоряжения похищенными денежными средствами Г., находясь в вышеуказанной колонии, используя мобильную связь, обратился к Д. с просьбой снять со своего банковского счета перечисленные при указанных выше обстоятельствах наличные денежные средства и потратить их в корыстных целях Г. При этом Д., которая не была посвящена в преступный умысел Г., по просьбе последнего, через банкомат осуществила снятие наличных денежных средств, поступивших на вышеуказанный банковский счет и распорядилась ими в корыстных целях Г. Тем самым Г. похитил принадлежащие гражданину Ф. денежные средства путем ввода, модификации компьютерной информации

и иного вмешательства в функционирование средств хранения, обработки компьютерной информации, причинив гражданину Ф. значительный ущерб [16].

Процент преступников-рецидивистов в категории имущественных преступлений ниже 7 %, но наблюдается рост на 0,7 %. Необходимо обратить внимание на эту социальную группу, поскольку сложность борьбы с рецидивной преступностью заключается в том, что такие правонарушения, как правило, имеют высокую степень латентности, часто из-за жертв, которые нарушают существующие законы. Этим в итоге могут воспользоваться преступники.

Характеристики лиц, совершающих преступления с использованием современных информационно-коммуникационных технологий, значительно расширят вероятностную модель такой преступной деятельности. Это особенно важно для криминалистики, поскольку личность преступника приобретает уникальное значение по сравнению с другими областями.

Знания о мотивах и целях преступника, его попытках скрыть улики, поведении до и после совершения преступления могут быть использованы для совершенствования методов расследования, если речь идет о мошенничестве с применением цифровых средств. Сложно угнаться за темпом развития информационных технологий. Именно благодаря этому возникают особенности преступлений в сфере информационной безопасности: трудоемкое доказательство вины того или иного лица, усложненный поиск улик, отсутствие свидетелей позволяют киберпреступникам часто оставаться в тени [17].

Для эффективного противодействия компьютерной преступности необходимо определить ее причины. К. Н. Евдокимов выделяет следующие причины киберпреступности в России [18].

Социальные:

— широкое использование технологий в России, включая расширение компьютерных систем, информационных сетей, услуг и электронного документооборота;
— необходимость доступа населения к информационным услугам по легальным каналам в связи с более низким уровнем жизни.

Экономические:

— недобросовестная конкуренция среди производителей программного обеспечения и антивирусов;
— быстрая и легкая прибыль для преступников за счет манипуляций с ресурсами компьютеров и корпоративных сетей.

Политические:

— недостаточный государственный контроль над киберпространством и цифровыми медиа;
— использование кибероружия между враждующими странами (геополитическая причина).

Правовые:

— несовершенство российского законодательства в сфере борьбы с компьютерными преступлениями;
— несовершенство судебной практики (например, отсутствие разъяснений Пленума Верховного Суда РФ по вопросам квалификации и наказания за преступления в сфере компьютерной преступности);
— недостатки в работе следственных органов (по статистике, значительное количество уголовных дел прекращают на стадии предварительного следствия);
— недостатки в деятельности органов и должностных лиц, осуществляющих оперативно-розыскную деятельность.

Причины преступной деятельности не могут быть реализованы или установлены без определенных условий. В контексте изложенного выше выявлены следующие обстоятельства, способствующие совершению киберпреступлений:

— недостаточная грамотность в области информационных технологий;
— отсутствие комплексной государственной политики в отношении информационной безопасности;
— отсутствие лиц, ответственных за безопасность данных и их защиты от несанкционированного доступа.

Хотя это далеко не полный список потенциальных причин киберпреступности, все-таки существует необходимость в их лучшем понимании. Очевидно, что для надлежащего решения и предотвращения киберпреступлений в России целесообразно активно развивать международное сотрудничество и участвовать в соответствующих конвенциях относительно преступлений в сфере компьютерной информации.

Конвенции должны регулировать противодействие незаконному доступу к электронной информации, незаконному вмешательству, производству/распространению вредоносного программного обеспечения, контрабанде устройств и их краже. Кроме того, с развитием технологий изменяется и законодательство, а значит, его необходимо ежегодно пересматривать. На наш взгляд, очевиден тот факт, что наиболее значимыми причинами и обстоятельствами рассматриваемых преступлений являются социальные и правовые.

Выводы

В целом исследование показало, что с ростом нашей зависимости от технологий растет и количество преступлений в сфере информационных технологий, создавая значительные последствия как для предприятий, так и для частных лиц. Сегодня особенно важно, чтобы все предпринимали шаги по обеспечению своей цифровой безопасности, используя надежные пароли и обновляя свои компьютеры последними обновлениями безопасности. Принятие таких превентивных мер снизит риск, исходящий от преступлений, совершаемых с использованием информационно-телекоммуникационных технологий или в сфере компьютерной информации. Как показывают результаты исследования, в структуре таких преступлений наиболее распространены мошенничества. Важнейшими факторами, влияющими на распространение таких преступлений, служат личностные особенности преступников и их жертв. Недостаток информационно-коммуникативной компетенции, правовая безграмотность, излишняя доверчивость, корысть и другие особенности личности могут сделать человека жертвой рассмотренных преступлений.

В современных условиях очень важно, на наш взгляд, изучать не только способы совершения преступлений с применением информационно-телекоммуникационных технологий или в сфере компьютерной информации, но и их причины, личность преступников, прежде всего особенности жертв преступлений. Безусловно, активная работа с потенциальными жертвами может предотвратить многие преступления. Необходимо в связи с этим разрабатывать и проводить разнообразные мероприятия просветительского характера, используя опыт сотрудников правопорядка, а также достижения психологии и педагогики. Населению в профилактических целях нужно рассказывать о рисках стать жертвой, используя разнообразные источники информации, учитывая психологические особенности определенных категорий людей, связанных с возрастом, образованием и видом их деятельности. Очевидно, что это существенно повысит эффективность противодействия исследованным нами в статье преступлениям и будет способствовать их предупреждению.

Список источников

1. О Стратегии национальной безопасности Российской Федерации: указ Президента РФ от 31 декабря 2015 г. № 683 // Справ.-правовая система «КонсультантПлюс». URL: https://www.consultant.ru/document/cons_doc_LAW_191669/ (дата обращения: 21.03.2023).
2. Состояние преступности в России // МВД России: офиц. сайт. URL: https://xn--b1aew.xn--p1ai/folder/101762 (дата обращения: 21.03.2023).
3. Состояние преступности в России за январь — декабрь 2021 г. М.: ФКУ «Главный информационно-аналитический центр» МВД России, 2022. 66 с.
4. Расширенное заседание коллегии МВД России. Выступление Президента РФ В. В. Путина // Администрация Президента России: офиц. сайт. 2022. 17 февраля. URL: http://www.kremlin.ru/events/president/news/67795 (дата обращения: 28.03.2023).
5. Краткая характеристика состояния преступности в Российской Федерации за январь 2023 г. // МВД России: офиц. сайт. 2023. 20 февраля. URL: https://xn--b1aew.xn--p1ai/reports/item/35919430/ (дата обращения: 28.03.2023).
6. *Летелкин Н. В.* К вопросу об определении понятия преступлений, совершаемых с использованием информационно-телекоммуникационных сетей (включая сеть Интернет) // Уголовное право: стратегия развития в XXI веке: сб. ст. по материалам XV Междунар. науч.-практ. конф. (Москва, 25–26 января 2018 г.). М.: Проспект, 2018. С. 617–619.
7. Приговор Сыктывдинского районного суда Республики Коми от 5 мая 2016 г. по делу № 1-66/2016 // Правосудие: госуд. автоматизированная система РФ. URL: https://bsr.sudrf.ru/bigs/portal.html (дата обращения: 15.04.2023).
8. Наказание в системе уголовно-правовых средств противодействия преступности: взаимодействие правовых систем в условиях глобализации международной жизни / В. А. Авдеев, О. А. Авдеева, О. П. Грибунов, В. А. Сергевнин // Криминологический журнал Байкальского государственного университета экономики и права. 2016. Т. 10. № 2. С. 301–312. DOI: 10.17150/1996-7756.2016.10(2).301-312
9. *Косенко А. Н., Черный Г. А.* Общая характеристика психологии киберпреступника // Криминологический журнал Байкальского государственного университета экономики и права. 2012. № 3. С. 87–94.
10. *Коломинов В. В.* Мошенничество в сфере компьютерной информации как объект криминалистического познания // Сибирские уголовно-процессуальные и криминалистические чтения. 2015. № 2. С. 153–160.
11. *Юрова К. И., Гаврилина В.* Виды мошенничества в сети Интернет // Современные технологии: актуальные вопросы, достижения и инновации: сб. ст. III Междунар. науч.-практ. конф. (Пенза, 23 ноября 2016 г.) / отв. ред. Г. Ю. Гуляев. Пенза: Наука и Просвещение, 2016. С. 55–57.
12. *Крылов В. В.* Информационные компьютерные преступления: учеб. и практ. пособие. М.: Инфра-М: Норма, 1997. 276 с.
13. *Дремлюга Р. И.* Интернет-преступность: монография. Владивосток: Изд-во Дальневосточного ун-та, 2008. 240 с.
14. *Боташева А. Х.* К вопросу о личности преступника, совершающего мошенничество в банковской сфере // Общество и право. 2009. № 2. С. 96–100.
15. *Рогова Н. Г.* Отграничение мошенничества от преступлений в сфере экономической деятельности // Вектор науки Тольяттинского государственного университета. 2010. № 2. С. 98–99.
16. Приговор Коломенского городского суда Московской области от 28 апреля 2016 г. по делу № 1-7 В/16 г. // Правосудие: госуд. автоматизированная система РФ. URL: https://bsr.sudrf.ru/bigs/portal.html (дата обращения: 15.04.2023).
17. *Шапошников А. А.* Криминологическая характеристика личности киберпреступника // Вестник юридического факультета Южного федерального университета. 2018. Т. 5. № 3-4. С. 58–63.
18. *Евдокимов К. Н.* Причины компьютерной преступности в современной России // Российский следователь. 2015. № 3. С. 33–37.

References

1. On the National Security Strategy of the Russian Federation. Decree of the President of the Russian Federation of December 31, 2015 No. 683. Konsul'tantPlyus. URL: https://www.consultant.ru/document/cons_doc_LAW_191669/ (accessed on 21.03.2023). (In Russ.).
2. The state of crime in Russia. Official website of the Ministry of Internal Affairs of Russia. URL: https://xn--b1aew.xn--p1ai/folder/101762 (accessed on 21.03.2023). (In Russ.).
3. State of crime in Russia for January-December 2021. Moscow: Main Information and Analytical Center of the Ministry of Internal Affairs of Russia; 2022. 66 p. (In Russ.).
4. Extended meeting of the board of the Ministry of Internal Affairs of Russia. Speech by the President of the Russian Federation V.V. Putin. Official website of the Administration of the President of Russia. Feb. 17, 2022. URL: http://www.kremlin.ru/events/president/news/67795 (accessed on 28.03.2023). (In Russ.).
5. Brief description of the state of crime in the Russian Federation for January 2023. Official website of the Ministry of Internal Affairs of Russia. Feb. 20, 2023. URL: https://xn--b1aew.xn--p1ai/reports/item/35919430/ (accessed on 28.03.2023). (In Russ.).
6. Letelkin N.V. On the issue of defining the concept of crimes committed using information and telecommunication networks (including the Internet). In: Criminal law: Development strategy in the 21st century. Proc. 15th Int. sci.-pract. conf. (Moscow, January 25-26, 2018). Moscow: Prospekt; 2018:617-619. (In Russ.).
7. Verdict of the Syktyvdinsk District Court of the Komi Republic dated May 5, 2016 in case No. 1-66/2016. Pravosudie. URL: https://bsr.sudrf.ru/bigs/portal.html (accessed on 15.04.2023). (In Russ.).
8. Avdeev V.A., Avdeeva O.A., Gribunov O.P., Sergevnin V.A. Punishment in the system of criminal law measures of counteracting corruption: Interaction of legal systems in the conditions of international life's globalization. *Kriminologicheskii zhurnal Baikal'skogo gosudarstvennogo universiteta ekonomiki i prava = Criminology Journal of Baikal National University of Economics and Law.* 2016;10(2):301-312. (In Russ.). DOI: 10.17150/1996-7756.2016.10(2).301-312
9. Kosenko A.N., Cherniy G.A. General characteristic of a cybercriminal's personality. *Kriminologicheskii zhurnal Baikal'skogo gosudarstvennogo universiteta ekonomiki i prava = Criminology Journal of Baikal National University of Economics and Law.* 2012;(3):87-94. (In Russ.).
10. Kolominov V.V. Swindle in the field of computer information as object of criminalistics cognition. *Sibirskie ugolovno-protsessual'nye i kriminalisticheskie chteniya = Siberian Criminal Process and Criminalistic Readings.* 2015;(2):153-160. (In Russ.).
11. Yurova K.I., Gavrilina V. Types of fraud on the Internet. In: Modern technologies: Current issues, achievements and innovations. Proc. 3rd Int. sci.-pract. conf. (Penza, November 23, 2016). Penza: Nauka i Prosveshchenie; 2016:55-57. (In Russ.).
12. Krylov V.V. Information computer crimes. Moscow: Infra-M; Norma; 1997. 276 p. (In Russ.).
13. Dremlyuga R.I. Internet crime. Vladivostok: Far Eastern University Publishing; 2008. 240 p. (In Russ.).
14. Botasheva A.Kh. On the issue of the identity of the criminal who commits fraud in the banking sector. *Obshchestvo i pravo = Society and Law.* 2009;(2):96-100. (In Russ.).
15. Rogova N.G. Differentiation of swindle from crimes in economic activities sphere. *Vektor nauki Tol'yattinskogo gosudarstvennogo universiteta = Vector of Science of Togliatti State University.* 2010;(2):98-99. (In Russ.).
16. Verdict of the Kolomna City Court of the Moscow Region dated April 28, 2016 in case No. 1-7 B/16. Pravosudie. URL: https://bsr.sudrf.ru/bigs/portal.html (accessed on 15.04.2023). (In Russ.).
17. Shaposhnikov A.A. Criminological profile of a cybercriminal. *Vestnik yuridicheskogo fakul'teta Yuzhnogo federal'nogo universiteta = Bulletin of the Law Faculty, Southern Federal University.* 2018;5(3-4):58-63. (In Russ.).
18. Evdokimov K.N. Causes of cyber crime in modern Russia. *Rossiiskii sledovatel' = Russian Investigator.* 2015;(3):33-37. (In Russ.).

Информация об авторах

О. В. Аникаева — главный специалист; 656011, Алтайский край, Барнаул, Ленина пр., д. 106;

И. Н. Бобровничий — кандидат педагогических наук, доцент, заведующий кафедрой социально-экономических, гуманитарных и специальных дисциплин; 185005, Республика Карелия, Петрозаводск, Онежской флотилии ул., д. 51.

Information about the authors

O. V. Anikayeva — chief specialist; 106 Lenina Ave., Barnaul, Altai Territory, 656011, Russia;

I. N. Bobrovnichiy — PhD in Pedagogy, Associate Professor, Head of the Department of Socio-Economic, Humanitarian and Special Disciplines; 51 Onega flotilla st., Petrozavodsk, Republic of Karelia, 185005, Russia.

Конфликт интересов: авторы декларируют отсутствие конфликта интересов, связанных с публикацией данной статьи.

Conflict of interest: the authors declare no conflict of interest related to the publication of this article.

Статья поступила в редакцию 22.06.2023; одобрена после рецензирования 23.08.2023; принята к публикации 20.12.2023.

The article was submitted 22.06.2023; approved after reviewing 23.08.2023; accepted for publication 20.12.2023.