ПРИМЕНЕНИЕ НОРМ ПРАВА ОРГАНАМИ ПРЕДВАРИТЕЛЬНОГО СЛЕДСТВИЯ И ДОЗНАНИЯ

THE LAW ENFORCEMENT BY THE BODIES OF PRELIMINARY INVESTIGATION AND INQUIRY

УДК 343.42
DOI 10.52468/2542-1514.2025.9(1).122-131

ОСОБЕННОСТИ КВАЛИФИКАЦИИ ПРЕСТУПЛЕНИЙ В СФЕРЕ КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ И ПРОТИВОДЕЙСТВИЯ ИМ*

И.А. Ефремова
Саратовская государственная юридическая академия, г. Саратов, Россия

Информация о статье
Дата поступления –
04 июня 2024 г.
Дата принятия в печать –
10 января 2025 г.
Дата онлайн-размещения –
20 марта 2025 г.

Ключевые слова
Преступления, противодействие, информационно-телекоммуникационные сети, сеть «Интернет», преступления в сфере компьютерной информации

Преступники взяли на вооружение новые информационно-телекоммуникационные технологии и переместили противоправную деятельность в онлайн-пространство. В последнее время наблюдается рост преступлений, совершаемых в сфере компьютерной информации и (или) с использованием информационно-телекоммуникационных сетей. Уровень их латентности варьируется от 80 до 90 %. С применением статистического метода, системно-структурного анализа в статье констатируется рост общественно опасных деяний, совершаемых в сфере компьютерной информации и (или) с использованием информационно-телекоммуникационных сетей. Утверждается необходимость выработать эффективные меры противодействия таким преступлениям, в том числе уголовно-правовые.

PECULIARITIES OF QUALIFICATION OF CRIMES IN THE FIELD OF COMPUTER INFORMATION AND COUNTERACTION TO THEM**

Irina A. Efremova
Saratov State Law Academy, Saratov, Russia

Article info
Received –
2024 June 04
Accepted –
2025 January 10
Available online –
2025 March 20

Keywords
Crimes, counteraction, information and telecommunication networks, the Internet, crimes in the field of computer information

The subject of the study is the specifics of the qualification of crimes in the field of computer information and measures to counter them. The purpose of the study is to examine the specifics of the qualification of crimes in the field of computer information and to develop effective measures to counter them. Research methodology. Along with the universal method of cognition, general scientific and private scientific methods were used: first of all, the statistical method, system-structural analysis, analytical research. This made it possible to comprehensively investigate the specifics of the qualification of crimes in the field of computer information and identify measures to counter them. Scientific results of the study. It has been established that recently there has been an increase in crimes committed in the field of computer information and (or) using information and telecommunication networks. In 2023, the share increased from 26.5% to 34.8% compared to the previous year. More than half of such crimes (50.6%) belong to the categories of grave and especially grave. It is determined that criminal liability for crimes committed in the field of computer information is established in Chapter 28 of the Criminal Code of the Russian Federation "Crimes in the field of computer information", for crimes committed using information and

* Исследование выполнено за счет гранта Российского научного фонда № 24-28-00312, https://rscf.ru/project/24-28-00312.
** The research was carried out at the expense of a grant from the Russian Science Foundation No. 24-28-00312, https://rscf.ru/project/24-28-00312/.

telecommunication networks - in art. 105; 110; 110.1; 110.2; 111; 112; 115; 116; 117; 119; 126; 127; 127.2; 128.1; 133; 137; 151.2; 159.6; 171.2; 185.3; 205.2; 222; 222.1; 228.1; 230; 238.1; 242; 242.1; 242.2; 245; 258.1; 260.1; 280; 280.1; 280.4; 282; 354.1 The Criminal Code of the Russian Federation, containing a qualifying The attribute is an information and telecommunication network. The classification of this feature as qualifying is based on the degree of public danger of the crime. But there is a varying degree of public danger of these acts. In some formations, the commission of a crime using information and telecommunication networks is a qualified type (art. 110, 110.2, 128.1, 151.2, 205.2, 228.1, 230, 242.1, 242.2, 245, 258.1, 260.1, 280, 280.1, 280.4 of the Criminal Code of the Russian Federation), in others – especially qualified (art. 110.1, 133, 137, 222, 222.1, 242 159.6, 171.2, 185.3, 238.1 of the Criminal Code of the Russian Federation). It is noted that this feature raises questions when qualifying, for example, when identifying an organized group that commits criminal acts using information and telecommunications networks, including the Internet; distinguishing from other crimes. As measures to counteract crimes committed in the field of computer information and (or) using information and telecommunication networks, including the Internet, it is proposed: to develop a concept of economic development to overcome poverty; to instill a culture of using digital technologies, to form positive value orientations; to develop a Concept of crime prevention, in which it is necessary to devote a separate section on these criminal acts; develop a national plan to counter these crimes; to increase the equipment of law enforcement agencies; to create specialized units for countering cybercrime in the structure of the Ministry of Internal Affairs of the Russian Federation, etc. Conclusions about the achievement of the purpose of this study. In the conducted research, the problems of qualification of crimes in the field of computer information are identified and counteraction measures are proposed.

1. Введение

Вступление Российской Федерации в эпоху информационного общества повлекло не только изменения в экономике, политике, способах коммуникации, но и в преступной сфере. Преступники взяли на вооружение новые информационно-телекоммуникационные технологии и переместили противоправную деятельность в онлайн-пространство, в связи с чем преступность приобрела новые характеристики. В последнее время наблюдается рост преступлений, совершаемых в сфере компьютерной информации и (или) с использованием информационно-телекоммуникационных сетей. С января по декабрь 2023 г. было зарегистрировано 677,0 тыс. указанных деяний. Темп прироста по отношению к предыдущему году составил 29,7 %. Удельный вес увеличился с 26,5 до 34,8 %. Больше половины таких преступлений (50,6 %) относится к категориям тяжких и особо тяжких (было зарегистрировано 342,6 тыс., темп прироста 25,9 %)[1]. И это не учитывая высокий уровень латентности обозначенных посягательств [1, с. 146; 2, p. 1601], который варьируется от 80 до 90 % [3, с. 37].

На дальнейший рост числа преступлений рассматриваемой группы окажет влияние увеличение количества пользователей сети «Интернет». Сегодня сетью «Интернет» пользуются 66 % домохозяйств, к 2030 г. планируется увеличить этот показатель до 97 %. Поэтому следует выработать эффективные меры противодействия обозначенным преступлениям, в том числе уголовно-правовые.

Выработке эффективных мер противодействия будут способствовать научные исследования. Изучению уголовно-правовой квалификации общественно опасных деяний, совершаемых в сфере компьютерной информации и (или) с использованием информационно-телекоммуникационных сетей, и противодействию им посвящены работы российских и зарубежных [4, p. 66; 5, p. 2517; 6, p. 85] исследователей, среди которых можно выделить В.А. Бессонова, Б.В. Вехова, Р.И. Дремлюгу, М.А. Ефремову Н.В. Летелкина, М.А. Простосердова, И.М. Рассолова, Е.А. Рускевича, Т.Л. Тропину и др. Но в настоящее время отсутствует комплексное исследование, которое было бы посвящено уголовно-правовой оценке указанных общественно опасных деяний, совершаемых в сфере компьютерной информации и (или) с использованием информационно-телекоммуникационных сетей, и противодействию им. Поэтому рассмотрим обозначенное, используя наряду с всеобщим методом познания, общенаучные и частнонауч-

[1] Характеристика состояния преступности в Российской Федерации за январь – декабрь 2023 года // МВД России: офиц. сайт. URL: https://мвд.рф/reports/item/47055751/ (дата обращения: 20.05.2024).

ISSN 2542-1514 (Print)

ные методы исследования, прежде всего статистический метод, системно-структурный анализ, аналитическое исследование.

2. Результаты исследования и обсуждения

Уголовная ответственность за преступления, совершаемые в сфере компьютерной информации, установлена в гл. 28 Уголовного кодекса (далее – УК) РФ «Преступления в сфере компьютерной информации», за преступления, совершаемые с использованием информационно-телекоммуникационных сетей, – в ст. 110, 110.1, 110.2, 128.1, 133, 137, 151.2, 159.6, 171.2, 185.3, 205.2, 222, 222.1, 228.1, 230, 238.1, 242, 242.1, 242.2, 245, 258.1, 260.1, 280, 280.1, 280.4, 282, 354.1 УК РФ, содержащих квалифицирующий признак – информационно-телекоммуникационная сеть. Но посредством использования информационно-телекоммуникационных сетей могут быть совершены и иные общественно опасные посягательства. Например, в Британии было впервые совершено изнасилование с помощью использования информационно-телекоммуникационной сети. Группа мужчин изнасиловали аватар несовершеннолетней во время игры, что оказало на несовершеннолетнюю девушку негативное эмоциональной и психологическое воздействие[2]. В Самаре было совершено мужеложство путем использования информационно-телекоммуникационной сети «Интернет»[3], но это не было отражено на уголовно-правовой оценке содеянного. Поэтому учеными предлагается дополнить ст. 63 УК РФ таким отягчающим обстоятельством, как совершение преступных посягательств с использованием средств массовой передачи информации [7, с. 15] или с использованием информационно-телекоммуникационных сетей [8, с. 10].

Обозначенное было поддержано государственными органами, в связи с чем было предложено дополнить ч. 1 ст. 63 УК РФ таким отягчающим обстоятельством, как публичная демонстрация, в том числе в средствах массовой информации или информационно-телекоммуникационных сетях (включая сеть «Интернет»), а ст. 111, 112, 115, 116, 117, 127 УК РФ – квалифицирующим признаком – совершение преступления, сопряженного с публичной демонстрацией процесса его осуществления с использованием средств массовой информации либо электронных или информационно-телекоммуникационных сетей (включая сеть «Интернет»)[4]. Но посредством использования информационно-телекоммуникационных сетей могут совершаться иные преступления, в связи с чем предлагаемый перечень составов преступлений является недостаточным.

В основе отнесения обозначенного к квалифицирующим признакам лежит степень общественной опасности, являющаяся количественным признаком общественной опасности [9, с. 319–321]. Степень общественной опасности – основанная на характере общественной опасности, обстоятельствах, смягчающих и отягчающих наказание, других факторах, характеризующих личность, готовность лица к совершению нового посягательства на объекты уголовно-правовой охраны. Определяющим в степени общественной опасности является уровень готовности лица к совершению нового преступления. Состояние готовности базируется на характере причиненного вреда соответствующему объекту преступления (объективный показатель) и получении лицом полного или неполного удовлетворения от совершенного им посягательства (субъективный показатель) [10, с. 545]. Преступления, совершаемые с использованием информационно-телекоммуникационных сетей, посягают на различные объекты уголовной охраны (жизнь, здоровье, общественную безопасность и т. д.), и виновные не получают должного удовлетворения от совершенного деяния, что подтверждается тем, что преступниками продолжительное время совершаются указанные деяния. Так, Е., С. и Д. более года совершали хищение с банковских счетов различных физических лиц[5].

На длительность совершения анализируемых деяний в целях удовлетворения своих потребностей сказывается их трансграничный характер, причинение значительного ущерба и их слабая раскрываемость. В 2023 г. раскрываемость преступлений, совершенных с использованием информационно-те-

[2] Комолов А. Полиция Британии расследует первое изнасилование в виртуальной реальности // Российская газета. 2024. 3 янв. URL: https://rg.ru/2024/01/03/policiia-britanii-rassleduet-pervoe-iznasilovanie-v-virtualnoj-realnosti.html (дата обращения: 27.05.2024).

[3] Справка по результатам проведенного анализа судебной практики рассмотрения уголовных дел о совершении преступлений в сфере компьютерных технологий (подготовлена Самарским областным судом 26 сентября 2022 г.) // СПС «КонсультантПлюс».

[4] Письмо Верховного Суда РФ от 13 сентября 2023 г. № 4-ВС-4557/23 «Официальный отзыв на проект федерального закона № 506240-8 “О внесении изменений в Уголовный кодекс Российской Федерации”».

[5] Уголовное дело № 1-54/2019, находящееся в архиве Центрального районного суда г. Читы Забайкальского края.

ISSN 2658-4050 (Online)

лекоммуникационных сетей или в сфере компьютерной информации, составила 26,6 %[6].

Но установление в большинстве составов преступлений обозначенного квалифицирующего признака породит проблемы при квалификации, поскольку в настоящее время при уголовно-правовой оценке возникает немало вопросов, в связи с чем Пленум Верховного Суда РФ разработал и принял постановление, посвященное вопросам судебной практики по уголовным делам о преступлениях в сфере компьютерной информации, а также иным преступлениям, совершенным с использованием электронных или информационно-телекоммуникационных сетей, включая сеть «Интернет». В нем представлено толкование компьютерной информации, компьютерных устройств, охраняемой законом компьютерной информации, компьютерной программы, уничтожения, блокирования, модификации, копирования компьютерной информации, нейтрализации средств защиты компьютерной информации, неправомерного доступа компьютерной информации, информационно-телекоммуникационной сети, сайта в сети «Интернет»; обозначен момент окончания преступлений, совершаемых в сфере компьютерной информации, и преступлений, совершаемых с использованием информационно-телекоммуникационных сетей, включая сеть «Интернет»; указаны правила квалификации этих деяний и т. д. Но это не устранило всех возникающих на практике вопросов. Например, Верховный Суд РФ признал необоснованной квалификацию содеянного по п. «б» ч. 2 ст. 228.1 УК РФ. Из материалов уголовного дела следует, что для производства и сбыта наркотических средств лицо приобрело через информационно-телекоммуникационную сеть «Интернет» всё необходимое оборудование. С его помощью он долгое время производит наркотические средства. Но Верховный Суд РФ указал, что квалифицирующий признак «с использованием информационно-телекоммуникационных сетей (включая сеть “Интернет”)» используется применительно к сбыту наркотических средств, психотропных веществ[7]. В рассматриваемом случае сбыт виновным, как установлено, не производился.

Возникают вопросы и при установлении организованной группы, которая совершает преступление с использованием информационно-телекоммуникационных сетей, в том числе сети «Интернет». Правоприменительная практика в указанной части разнится даже в одних и тех же судах. Неверная уголовно-правовая квалификация содеянного повлечет назначение уголовного наказания, которое не позволит достичь его цели и задач уголовного закона, в связи с чем данный вопрос сегодня является одним из актуальных. Так, суд исключил квалифицирующий признак – организованную группу, переквалифицировав на то, что деяние было совершено группой лиц по предварительному сговору с использованием информационно-телекоммуникационной сети «Интернет». Из материалов уголовного дела следует, что Е., С. и Д. совершали хищение с банковских счетов физических лиц. На телефоны потерпевших были установлены вредоносные программы, что позволило виновным беспрепятственно осуществлять хищение. Исключив организованную группу, суд указал, что в процессе расследования не был установлен такой ее признак, как объединение для совершения уголовно-наказуемого посягательства, поскольку в основе их объединения была заложена не целенаправленная деятельность, а дружба, а также такой признак, как устойчивость организованной группы (обосновав тем, что виновные могли из нее выйти)[8].

В процессе рассмотрения другого уголовного дела указанный суд согласился с уголовно-правовой оценкой содеянного и признал, что преступление было совершено организованной группой с использованием информационно-телекоммуникационной сети «Интернет». Из материалов уголовного дела следовало, что участники организованной группы были друзьями[9]. Вызывает проблемы при квалификации и территориальная рассредоточенность, анонимность участников организованной группы, совершающей изучаемые общественно опасные деяния, в связи с чем органами предварительного расследования не устанавливается, что деяние было совершено организованной группой. Следовательно, это сказывается и на достижении целей уголовного наказания.

[6] Характеристика состояния преступности в Российской Федерации за январь – декабрь 2023 года.

[7] ВС указал квалифицирующий признак, не используемый по делам о производстве наркотиков // Российское агентство правовой и судебной статистики. URL: https://rapsinews.ru/publications/20221103/308440464.html (дата обращения: 27.05.2024).

[8] Уголовное дело № 1-54/2019, находящееся в архиве Центрального районного суда г. Читы Забайкальского края.

[9] Уголовное дело № 1-949/2018, находящееся в архиве Центрального районного суда г. Читы Забайкальского края.

ISSN 2542-1514 (Print)

Но, к сожалению, учеными не рассматривается обозначенная проблема. Отсутствуют и разъяснения Пленума Верховного Суда РФ в указанной части.

В настоящее время прослеживается различное влияние рассматриваемого способа совершения преступления на степень общественной опасности. В одних составах совершение преступления с использованием информационно-телекоммуникационных сетей является квалифицированным видом (ст. 110, 110.2, 128.1, 151.2, 205.2, 228.1, 230, 242.1, 242.2, 245, 258.1, 260.1, 280, 280.1, 280.4 УК РФ), в других – особо квалифицированным (ст. 110.1, 133, 137, 222, 222.1, 242 УК РФ), в третьих – криминообразующим признаком основного состава уголовно наказуемого деяния (ст. 159.6, 171.2, 185.3, 238.1 УК РФ). Квалифицированный состав и особо квалифицированный состав преступления разнятся степенью общественной опасности: уровнем готовности лица к совершению нового посягательства и получением виновным полного или неполного удовлетворения от совершенного им деяния. В силу обозначенных критериев представленное можно отнести к особо квалифицированному виду состава.

Привлечение виновных к уголовной ответственности и назначение им наказания, соответствующего степени и характеру общественной опасности совершенного деяния[10], – осуществление противодействия общественно опасным деяниям, совершаемым в сфере компьютерной информации и (или) с использованием информационно-телекоммуникационных сетей, уголовно-правовыми средствами. Но для эффективного противодействия изучаемым преступным посягательствам следует разработать целый комплекс мер противодействия.

Термин «противодействие» означает действие, препятствующее другому действию[11], направленное против него[12]. Применительно к юридической теории противодействие преступности наличествует тогда, когда деятельность государственных органов, общества и отдельных лиц противонаправлена деятельности по совершению или подготовке к совершению общественно опасных посягательств [11, с. 159]. Противодействие общественно опасным деяниям, совершаемым в сфере компьютерной информации и (или) с использованием информационно-телекоммуникационных сетей, осуществляется по двум направлениям: общесоциальное (выявление и устранение экономических, социальных, правовых и культурно-нравственных причин и условий изучаемой преступности) и специально-криминологическое противодействие (выявление и устранение специальных детерминант посредством профилактики (общей, индивидуальной, виктимологической) и пресечения преступлений рассматриваемой группы). Только благодаря обнаружению и воздействию на детерминанты можно добиться снижения указанных деяний.

В целях противодействия анализируемых уголовно-наказуемых посягательств необходимо снижать уровень бедности населения, поскольку бедность – локомотив преступности. Лица, совершающие преступления в сфере компьютерной информации или с использованием информационно-телекоммуникационных технологий, в большинстве случаев преследуют цель обогатиться.

Для преодоления бедности сегодня в стране предпринимается немало мер: например, осуществляются ежемесячные выплаты полным семьям с низкими доходами, ежемесячные пособия на детей от 3 до 8 лет, двухэтапная индексация основных социальных выплат и т. д.[13] Не углубляясь в изучение данных мер противодействия, поскольку они лежат в иной плоскости исследования, укажем, что следует разработать концепцию экономического развития по преодолению бедности, которая бы включала краткосрочные и долгосрочные меры. Это позволит снизить уровень бедности в России и положительно скажется на снижении количественных и качественных показателей изучаемых преступных посягательств.

Оказывает влияние на совершение общественно опасных деяний, совершаемых в сфере компьютерной информации и (или) с использованием информационно-телекоммуникационных сетей, падение рубля и высокий уровень инфляции. Поэтому целесообразно разработать и внедрить комплекс мер, направленных на предотвращение падения рубля и роста инфля-

[10] Это обеспечивает верная уголовно-правовая оценка содеянного.

[11] Ожегов С.И., Шведова Н.Ю. Толковый словарь русского языка: 72 500 сл. и 7 500 фразеол. выражений. М.: Азъ, 1994. С. 204.

[12] Ефремова Т.Ф. Толковый словарь словообразовательных единиц русского языка: ок. 1900 словообразоват. единиц. М.: Астрель, 2005. С. 234.

[13] Эксперт: поддержка семей с детьми способствовала снижению уровня бедности в России // ТАСС. 2023. 10 марта. URL: https://tass.ru/obschestvo/17240199 (дата обращения: 23.05.2024).

ISSN 2658-4050 (Online)

ции[14]. Указанные меры необходимо вводить постепенно, поскольку резкое уменьшение уровня инфляции может негативно сказаться на экономике страны, на что обращают внимание руководители крупнейших банков Российской Федерации[15].

Также положительно на противодействии преступлениям рассматриваемой группы скажется и надлежащее воспитание и образование подрастающего поколения. Приобщение человека к благам цифрового мира начинается с самого детства. Ребенок ежедневно видит, как родители и окружающие пользуются различными цифровыми технологиями, поэтому он привыкает к их постоянному присутствию. В связи с чем детям необходимо прививать культуру использования цифровых технологий, формировать положительные ценностные ориентации. На ценностные ориентации личности возможно воздействовать и посредством воспитания, образования, культуры [12, с. 37], религии и т. д. Совокупность данных мер может положительно сказаться на ценностных ориентациях личности.

В целях определения деятельности государства по противодействию изучаемым общественно опасным посягательствам следует разработать и принять Концепцию предупреждения преступности, в которой необходимо посвятить отдельный раздел указанным уголовно наказуемым деяниям. Концепция предупреждения преступности – это разработка государственной программы, определяющей основополагающие начала предупреждения данных преступлений, цели, задачи государства, которые будут ставиться им в целях противодействия. Концепция позволяет определить основания данной деятельности.

Для ее эффективной реализации будет целесообразно разработать национальный план противодействия изучаемым преступлениям, в котором будут содержаться конкретные меры, которые необходимо предпринять для противодействия деяниям анализируемой группы, поскольку они, во-первых, довольно распространены в стране, а также посягают на различные объекты уголовно-правовой охраны, во-вторых, обладают повышенной общественной опасностью.

Больше всего учеными для противодействия общественно опасным деяниям, совершаемым в сфере компьютерной информации и (или) с использованием информационно-телекоммуникационных сетей, предлагается повысить оснащенность правоохранительных органов, осуществляющих предварительное расследование этих деяний. В структуре информационных технологий особое место занимают большие данные (*big data*) [13, с. 152; 14, p. 7032]. Использование технологий *big data* может оказывать содействие в решении различных задач, связанных со сбором данных о преступниках, фиксацией преступного поведения, связей, формированием «электронного личного дела»; контролем группировок отрицательной направленности. Искусственный интеллект позволит прогнозировать преступное поведение на основании имеющих данных о личности, причинах и условиях совершенного преступления, характере его совершения и т. д., что позволит повысить эффективность деятельности по противодействию рассматриваемым преступным деяниям [15, с. 763–764; 16, p. 14]. При этом следует непрерывно развивать цифровые технологии, которые бы способствовали выявлению и раскрытию правоохранительными органами изучаемых уголовно-наказуемых деяний [17–23].

Скажется на повышении эффективности противодействия анализируемых деяний посредством их раскрытия создание специализированных подразделений по противодействию киберпреступлениям в структуре МВД РФ, на что указывал В.А. Колокольцев[16], поскольку они наиболее распространены и имеют особенности, которыми также должны обладать лица, осуществляющие их расследование. Также предлагается создать составы судов, рассматривающих дела, касающиеся общественно опасных деяний, совершаемых в сфере компьютерной информации и (или) с использованием информационно-телекоммуникационных сетей[17].

[14] В силу того, что разработка данных мер должна осуществляться учеными другой специальности – 08 00 00 «Экономические науки», – в настоящем исследовании мы их не будем детализировать и останавливаться на них подробно. Это не исключает важности их разработки, в том числе для снижения изучаемой преступности в Российской Федерации.

[15] Смирнова К. В чем опасность резкого снижения инфляции? Объясняют Греф и экономисты // Forbes. 2017. 30 мая. URL: https://www.forbes.ru/finansy-i-investicii/345293-v-chem-opasnost-rezkogo-snizheniya-inflyacii-obyasnyayut-gref-i (дата обращения: 20.05.2024).

[16] Колокольцев призвал усилить работу по противодействию IT-преступности и киберхищениям // ТАСС. 2021. 20 июля. URL: https://tass.ru/obschestvo/11943461 (дата обращения: 27.05.2024).

[17] В РФ могут создать спецсоставы по киберпреступности, но не новый суд – ВС // Российское агентство правовой и судебной статистики. 2023. 7 июня. URL: https://

ISSN 2542-1514 (Print)

3. Заключение

Таким образом, наблюдается рост числа общественно опасных деяний, совершаемых в сфере компьютерной информации и (или) с использованием информационно-телекоммуникационных сетей. Они посягают на различные объекты уголовной охраны (жизнь, здоровье, общественную безопасность и т. д.), и виновные не получают должного удовлетворения от совершенного деяния. Поэтому следует выработать эффективные меры противодействия преступлениям (к числу таких мер можно отнести разработку концепции экономического развития по преодолении бедности, которая бы включала краткосрочные и долгосрочные меры, и концепции предупреждения преступности; оснащение правоохранительных органов современными технологиями расследования; создание специальных отделов, занимающихся расследованием изучаемых преступлений), в том числе уголовно-правовые. Последние заключаются в совершенствовании уголовного закона и практики его применения.

СПИСОК ЛИТЕРАТУРЫ

1. Поляков В. В. Латентность высокотехнологичных преступлений: понятие, структура, методы оценки уровня / В. В. Поляков // Всероссийский криминологический журнал. – 2023. – Т. 17, № 2. – С. 146–155.

2. Yussuph T. T. Data protection and privacy as a tool to reduce financial loss from cybercrimes / T. T. Yussuph, J. W. Muhammed, D. M. Olalekan, B. Yusuf, A. Unuriode, B. H. Matti // Global Scientific Journal. – 2023. – Vol. 11, iss. 11. – P. 1596–1606.

3. Сухаренко А. Н. Современные криминальные вызовы и угрозы информационной безопасности России / А. Н. Сухаренко // Противодействие терроризму. Проблемы XXI века. – 2012. – № 2. – С. 36–41.

4. Caneppele S. Crime Drop or Police Recording Flop? On the Relationship between the Decrease of Offline Crime and the Increase of Online and Hybrid Crimes / S. Caneppele, M. F. Aebi // Policing: A Journal of Policy and Practice. – 2019. –Vol. 13, iss. 1. – P. 66–79. – DOI: 10.1093/police/pax055.

5. Mmbodi R. Cybercrimes in Social Networking / R. Mmbodi, N. Hlongwane // International Journal of Social Science and Human Research. – 2024. – Vol. 7, iss. 4. – P. 2517–2522. – DOI: 10.47191/ijsshr/v7-i04-38.

6. Aldoghmi H. S. The Role of International Efforts in Combating Cybercrimes / H. S. Aldoghmi // The International Journal of Humanities & Social Studies. – 2024. – Vol. 11, iss. 11. – P. 85–92. – DOI: 10.24940/theijhss/2023/v11/i11/HS2311-019.

7. Антипов А. И. Уголовно-правовое значение использование средств массовой информации и информационно-телекоммуникационных сетей интернет при совершении преступлений с признаками призывов, склонения незаконного оборота предметов и материалов : дис. … канд. юрид. наук / А. И. Антипов. – СПб., 2022. – 248 с.

8. Шутова А. А. Уголовно-правовое противодействие информационным преступлениям в сфере экономической деятельности: теоретические и прикладные аспекты : дис. … канд. юрид. наук / А. А. Шутова. – Н. Новгород, 2017. – 264 с.

9. Уголовное право. Общая часть. Преступление : акад. курс : в 10 т. / под ред. Н. А. Лопашенко. – М. : Юрлитинформ, 2016. – Т. 3 : Уголовная политика. Уголовная ответственность. – 507 с.

10. Разгильдиев Б. Т. Фундаментальные аспекты уголовного наказания / Б. Т. Разгильдиев // Всероссийский криминологический журнал. – 2017. – Т. 11, № 3. – С. 542–550.

11. Майоров А. В. Виктимологическая модель противодействия преступности : моногр. / А. В. Майоров. – М. : Юрлитинформ, 2014. – 223 с.

12. Тупичкина Е. А. Влияние социокультурных факторов на трансформацию ценностных ориентаций у российской молодежи / Е. А. Тупичкина, С. И. Семенака // Научно-педагогическое обозрение. – 2022. – № 4 (44). – С. 37–47.

13. Овчинский В. С. Криминология цифрового мира : учеб. / В. С. Овчинский. – М. : Норма : ИНФРА-М, 2018. – 351 с.

rapsinews.ru/judicial_news/20230607/308981899.html (дата обращения: 27.05.2024).

14. Subashka Ramesh S. S. Using Big Data, An Extensible System for Forecasting and Analyzing Relations Among Crimes / S. S. Subashka Ramesh, A. Anshu, V. Kumar, H. Kumar // Turkish Journal of Computer and Mathematics Education. – 2021. – Vol. 12, no. 10. – P. 7032–7040. – DOI: 10.17762/turcomat.v12i10.5577.

15. Суходолов А. П. Искусственный интеллект в противодействии преступности, ее прогнозировании, предупреждении и эволюции / А. П. Суходолов, А. М. Бычкова // Всероссийский криминологический журнал. – 2018. – Т. 12, № 6. – С. 753–766. – (На англ. яз.).

16. Cybercrime: The Investigation, Prosecution and Defense of a Computer-Related Crime / ed. by R. Clifford. – 3rd ed. – Carolina Academic Press, 2011. – 312 p.

17. Кириленко В. П. Гармонизация Российского уголовного законодательства о противодействии киберпреступности с правовыми стандартами Европы / В. П. Кириленко, Г. В. Алексеев // Всероссийский криминологический журнал. – 2020. – Т. 14, № 6. – С. 898–913.

18. Осипенко А. Л. Основные направления развититя криминологической науки и практики предупреждения преступлений в условиях цифровизации общества / А. Л. Осипенко, В. С. Соловьев // Всероссийский криминологический журнал. – 2021. – Т. 15, № 6. – С. 681–691.

19. Дремлюга Р. И. Уголовно-правовая политика в сфере противодействия платформизации преступной деятельности / Р. И. Дремлюга, А. И. Коробеев // Всероссийский криминологический журнал. – 2022. – Т. 16, № 1. – С. 47–56. – DOI: 10.17150/2500-4255.2022.16(1).47-56.

20. Лантух Э. В. Использование специальных знаний при расследовании преступлений в сфере компьютерной информации / Э. В. Лантух, В. С. Ишигеев, О. П. Грибунов // Всероссийский криминологический журнал. – 2020. – Т. 14, № 6. – С. 882–890.

21. Мкртчян С. М. Преступления против собственности, совершаемые в сфере функционирования блокчейна: новые преступные схемы и их уголовно-правовая оценка / С. М. Мкртчян // Всероссийский криминологический журнал. – 2020. – Т. 14, № 6. – С. 845–854.

22. Вершинина И. А. Данные в цифровом мире: новые возможности или дополнительные риски? / И. А. Вершинина, А. В. Лядова // Вестник Российского университета дружбы народов. Серия: Социология. – 2020. – Т. 20, № 4. – С. 977–984. – DOI: 10.22363/2313-2272-2020-20-4-977-984.

23. Серебренникова А. В. Криминологические проблемы цифрового мира (цифровая криминология) / А. В. Серебренникова // Всероссийский криминологический журнал. – 2020. – Т. 14, № 3. – С. 423–430.

REFERENCES

1. Polyakov V.V. Latency of high-tech crimes: concept, structure and methods of assessing its level. *Vserossiiskii kriminologicheskii zhurnal = Russian journal of criminology*, 2023, vol. 17, no. 2, pp. 146–155. (In Russ.).

2. Yussuph T.T., Muhammed J.W., Olalekan D.M., Yusuf B., Unuriode A., Matti B.H. Data protection and privacy as a tool to reduce financial loss from cybercrimes. *Global Scientific Journal*, 2023, vol. 11, iss. 11, pp. 1596–1606.

3. Sukharenko A. Modern criminal threats and challenges to information security of Russia. *Protivodeistvie terrorizmu. Problemy XXI veka = Counter-terrorism*, 2012, no. 2, pp. 36–41. (In Russ.).

4. Caneppele S., Aebi M.F. Crime Drop or Police Recording Flop? On the Relationship between the Decrease of Offline Crime and the Increase of Online and Hybrid Crimes. *Policing: A Journal of Policy and Practice*, 2019, vol. 13, iss. 1, pp. 66–79. DOI: 10.1093/police/pax055.

5. Mmbodi R., Hlongwane N. Cybercrimes in Social Networking. *International Journal of Social Science and Human Research*, 2024, vol. 7, iss. 4, pp. 2517–2522. DOI: 10.47191/ijsshr/v7-i04-38.

6. Aldoghmi H.S. The Role of International Efforts in Combating Cybercrimes. *The International Journal of Humanities & Social Studies*, 2024, vol. 11, iss. 11, pp. 85–92. DOI: 10.24940/theijhss/2023/v11/i11/HS2311-019.

7. Antipov A.I. *Criminal and legal significance of the use of mass media and information and telecommunication networks of the Internet in the commission of crimes with signs of appeals, inducement of illegal trafficking of objects and materials*, Cand. Diss. St. Petersburg, 2022. 248 p. (In Russ.).

8. Shutova A.A. *Criminal law counteraction to information crimes in the field of economic activity: theoretical and applied aspects*, Cand. Diss. Nizhny Novgorod, 2017. 264 p. (In Russ.).

9. Lopashenko N.A. (ed.). *Criminal law. The general part. Crime*, Academic course, in 10 volumes. Moscow, Yurlitinform Publ., 2016. Vol. 3: Criminal policy. Criminal liability. 507 p. (In Russ.).

10. Razgildiyev B.T. Fundamental aspects of criminal punishment. *Vserossiiskii kriminologicheskii zhurnal = Russian journal of criminology*, 2017, vol. 11, no. 3, pp. 542–550. (In Russ.).

11. Maiorov A.V. *Victimological model of crime prevention*, Monograph. Moscow, Yurlitinform Publ., 2014. 223 p. (In Russ.).

12. Tupichkina E.A., Semenaka S.I. The influence of socio-cultural factors on the transformation of value orientations of Russian youth. *Nauchno-pedagogicheskoe obozrenie = Pedagogical Review*, 2022, no. 4 (44), pp. 37–47. (In Russ.).

13. Ovchinskii V.S. *Criminology of the digital world*, Textbook. Moscow, Norma Publ., INFRA-M Publ., 2018. 351 p. (In Russ.).

14. Subashka Ramesh S.S., Anshu A., Kumar V., Kumar H. Using Big Data, An Extensible System for Forecasting and Analyzing Relations Among Crimes. *Turkish Journal of Computer and Mathematics Education*, 2021, Vol. 12, no. 10, pp. 7032–7040. DOI: 10.17762/turcomat.v12i10.5577.

15. Sukhodolov A.P., Bychkova A.M. Artificial Intelligence in Crime Counteraction, Prediction, Prevention and Evolution. *Vserossiiskii kriminologicheskii zhurnal = Russian journal of criminology*, 2018, vol. 12, no. 6, pp. 753–766.

16. Clifford R. (ed.). *Cybercrime: The Investigation, Prosecution and Defense of a Computer-Related Crime*, 3rd ed. Carolina Academic Press, 2011. 312 p.

17. Kirilenko V.P., Alekseev G.V. The harmonization of Russian criminal legislation on counteracting cybercrime with the legal standards of the Council of Europe. *Vserossiiskii kriminologicheskii zhurnal = Russian journal of criminology*, 2020, vol. 14, no. 6, pp. 898–913. (In Russ.).

18. Osipenko A.L., Solovev V.S. Main trends in the development of criminological theory and crime prevention practice in the context of the digitalization of society. *Vserossiiskii kriminologicheskii zhurnal = Russian journal of criminology*, 2021, vol. 15, no. 6, pp. 681–691. (In Russ.).

19. Dremliuga R.I., Korobeev A.I. Criminal law policy in counteracting the use of networking platforms for criminal activity. *Vserossiiskii kriminologicheskii zhurnal = Russian journal of criminology*, 2022, vol. 16, no. 1, pp. 47–56. (In Russ.).

20. Lantukh E.V., Ishigeev V.S., Gribunov O.P. The use of special knowledge in the investigation of computer crimes. *Vserossiiskii kriminologicheskii zhurnal = Russian journal of criminology*, 2020, vol. 14, no. 6, pp. 882–890. (In Russ.).

21. Mkrtchian S.M. Property crimes in the blockchain sphere: new criminal schemes and their criminal law assessment. *Vserossiiskii kriminologicheskii zhurnal = Russian journal of criminology*, 2020, vol. 14, no. 6, pp. 845–854. (In Russ.).

22. Vershinina I.A., Liadova A.V. Data in the digital world: New opportunities or additional risks?. *Vestnik Rossiiskogo universiteta druzhby narodov. Seriya: Sotsiologiya = RUDN Journal of Sociology*, 2020, vol. 20, no. 4, pp. 977–984. DOI: 10.22363/2313-2272-2020-20-4-977-984. (In Russ.).

23. Serebrennikova A.V. Criminological problems of the digital world (digital criminology). *Vserossiiskii kriminologicheskii zhurnal = Russian journal of criminology*, 2020, vol. 14, no. 3, pp. 423–430. (In Russ.).

ИНФОРМАЦИЯ ОБ АВТОРЕ

Ефремова Ирина Алексеевна – доктор юридических наук, доцент, профессор кафедры уголовного и уголовно-исполнительного права, профессор кафедры прокурорского надзора и криминологии
Саратовская государственная юридическая академия
410056, Россия, г. Саратов, ул. Вольская, 1
E-mail: efremova005@yandex.ru
ORCID: 0000-0003-0071-1999
ResearcherID: HJY-8774-2023
SPIN-код РИНЦ: 3413-7425; AuthorID: 320387

INFORMATION ABOUT AUTHOR

Irina A. Efremova – Doctor of Law, Associate Professor; Professor, Department of Criminal and Penal Enforcement Law; Professor, Department of Prosecutorial Supervision and Criminology
Saratov State Law Academy
1, Vol'skaya ul., Saratov, 410056, Russia
E-mail: efremova005@yandex.ru
ORCID: 0000-0003-0071-1999
ResearcherID: HJY-8774-2023
RSCI SPIN-code: 3413-7425; AuthorID: 320387

ISSN 2658-4050 (Online)

БИБЛИОГРАФИЧЕСКОЕ ОПИСАНИЕ СТАТЬИ

Ефремова И.А. Особенности квалификации преступлений в сфере компьютерной информации и противодействия им / И.А. Ефремова // Правоприменение. – 2025. – Т. 9, № 1. – С. 122–131. – DOI: 10.52468/2542-1514.2025.9(1).122-131.

BIBLIOGRAPHIC DESCRIPTION

Efremova I.A. Peculiarities of qualification of crimes in the field of computer information and counteraction to them. *Pravoprimenenie = Law Enforcement Review*, 2025, vol. 9, no. 1, pp. 122–131. DOI: 10.52468/2542-1514.2025.9(1).122-131. (In Russ.).