

Вестник Восточно-Сибирского института МВД России. 2026. № 2 (117). С. 129–137.
Vestnik of the East Siberian Institute of the Ministry of Internal Affairs of Russia. 2026,
vol. 117, no. 2, pp. 129-137.

5.1.4. Уголовно-правовые науки (юридические науки)

Научная статья
УДК 343.3/7

ОСВОБОЖДЕНИЕ ОТ УГОЛОВНОЙ ОТВЕТСТВЕННОСТИ ПРИ СОВЕРШЕНИИ ПРЕСТУПЛЕНИЙ В СФЕРЕ КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ

Гафурова Эльмира Равилевна

Ижевский государственный технический университет имени М. Т. Калашникова, Ижевск,
Российская Федерация, ely_1979@mail.ru

Введение. В статье рассмотрены проблемы и особенности применения института освобождения от уголовной ответственности (гл. 11 УК РФ) к преступлениям в сфере компьютерной информации (гл. 28 УК РФ). Актуальность темы обусловлена ростом общественной опасности киберпреступлений в условиях цифровизации и необходимостью поиска баланса между карательной и поощрительной функциями уголовного закона в этой специфической области. Требуется анализ эффективности общих оснований освобождения и выработка предложений по их адаптации или созданию специальных норм.

Материалы и методы. Нормативную основу исследования составляют положения глав 11 и 28 Уголовного кодекса Российской Федерации, а также разъяснения высших судов. Исследование основано на анализе конкретных примеров судебной практики, а также на трудах ученых в области уголовного права и информационной безопасности. Методологическую основу составили формально-юридический, сравнительно-правовой методы, методы анализа и синтеза.

Результаты исследования. Автор пришел к выводу, что прямое применение общих оснований освобождения от уголовной ответственности (деятельное раскаяние, примирение с потерпевшим, судебный штраф, истечение сроков давности) к преступлениям в сфере компьютерной информации сопряжено со значительными сложностями. Эти сложности обусловлены цифровой спецификой: латентностью и анонимностью преступлений, проблемами идентификации потерпевшего и оценки причиненного вреда, особенностями исчисления сроков давности. Установлено, что в отличие от ряда других составов, в гл. 28 Уголовного кодекса Российской Федерации отсутствуют специальные поощрительные нормы об освобождении от ответственности.

Выводы и заключения. Проведенное исследование позволило обосновать необходимость совершенствования правового регулирования. Для преодоления выявленных проблем и повышения эффективности противодействия киберпреступности предложено дополнить Уголовный кодекс Российской Федерации специальным примечанием об освобождении от ответственности к ст. 272 и 273 Уголовного кодекса Российской Федерации, а также детализировать условия его применения в разъяснениях Верховного Суда Российской Федерации. Данные меры направлены на стимулирование

виновных лиц к сотрудничеству, возмещению ущерба и обеспечению баланса между карательными и восстановительными механизмами в цифровой среде.

Ключевые слова: уголовная ответственность, освобождение от уголовной ответственности, преступления в сфере компьютерной информации, деятельное раскаяние, добровольность, своевременность

Для цитирования: Гафурова Э. Р. Освобождение от уголовной ответственности при совершении преступлений в сфере компьютерной информации // Вестник Восточно-Сибирского института МВД России. 2026. № 2 (117). С. 129–137.

5.1.4. Criminal Law Sciences (Legal Sciences)

Original article

EXEMPTION FROM CRIMINAL LIABILITY IN THE FIELD OF COMPUTER INFORMATION CRIMES

Elmira R. Gafurova

Izhevsk State Technical University named after M.T. Kalashnikov, Izhevsk, Russian Federation, ely_1979@mail.ru

Introduction. The article discusses the problems and features of applying the institution of exemption from criminal liability (Chapter 11 of the Criminal Code of the Russian Federation) to crimes in the field of computer information (Chapter 28 of the Criminal Code of the Russian Federation). The relevance of the topic is due to the growing public danger of cybercrimes in the context of digitalization and the need to find a balance between the punitive and incentive functions of criminal law in this specific area. It is necessary to analyze the effectiveness of general grounds for release and develop proposals for their adaptation or creation of special norms.

Materials and Methods. The study is based on the provisions of Chapters 11 and 28 of the Criminal Code of the Russian Federation, as well as the explanations of the highest courts. The study is based on the analysis of specific examples of judicial practice, as well as the works of scholars in the field of criminal law and information security. The study is based on formal legal and comparative legal methods, as well as analysis and synthesis.

The Results of the Study. The author concludes that the direct application of the general grounds for exemption from criminal liability (active repentance, reconciliation with the victim, judicial fine, and expiration of the statute of limitations) to crimes in the field of computer information is fraught with significant difficulties. These difficulties are caused by the digital specifics: the latency and anonymity of crimes, the problems of identifying the victim and assessing the harm caused, and the peculiarities of calculating the statute of limitations. It has been established that, unlike in a number of other offenses, Chapter 28 of the Criminal Code of the Russian Federation does not contain special incentives for exemption from liability.

Findings and Conclusions. The conducted research substantiated the need to improve legal regulation. To overcome the identified problems and increase the effectiveness of countering cybercrime, it was proposed to supplement the Criminal Code of the Russian Federation with a special note on exemption from liability under Articles 272 and 273 of the Criminal Code of the Russian Federation, as well as to detail the conditions for its application in the explanations of

the Supreme Court of the Russian Federation. These measures are aimed at encouraging perpetrators to cooperate, compensate for damages, and ensure a balance between punitive and restorative mechanisms in the digital environment.

Keywords: criminal liability, exemption from criminal liability, crimes in the field of computer information, active repentance, voluntariness, and timeliness

For citation: Gafurova E. R. Osvobozhdenie ot ugolovnoj otvetstvennosti pri sovershenii prestuplenij v sfere komp'yuternoj informacii [Exemption from Criminal Liability in the Field of Computer Information Crimes]. Vestnik Vostochno-Sibirskogo institute MVD Rossii – Vestnik of the East Siberian Institute of the Ministry of Internal Affairs of Russia. 2026, vol. 117, no. 2, pp. 129-137. (In Russ.).

Современный этап развития общества, характеризующийся повсеместной цифровизацией, объективно обуславливает рост общественной опасности преступных посягательств в сфере компьютерной информации (далее – КИ). Составы преступлений, сосредоточенные в главе 28 Уголовного кодекса Российской Федерации¹ (далее – УК РФ), криминализируют нарушения целостности, конфиденциальности и доступности КИ, что создает угрозу для нормального функционирования критической инфраструктуры, экономики и прав граждан [1, с. 57].

В части обеспечения общественного порядка и общественной безопасности рассматриваемая глава уголовного законодательства предусматривает девять составов преступлений, посягающих на КИ, а также нормальную работу электронных вычислительных машин, их систем и сетей (ст. 272, 272.1, 273, 274, 274.1, 274.2, 274.3, 274.4, 274.5). Динамика изменений, а именно введение ст. 274.1-274.5 УК РФ, свидетельствует о стремлении законодателя оперативно реагировать на новые вызовы, такие как создание и использование вредоносных программ для целей криптоджекинга или нарушения работы критической информационной инфраструктуры [2, с. 103].

Борьба с указанными видами преступлений имеет особое значение, так как преследует следующие важные государственные цели:

- обеспечение информационной безопасности государства. В период глобализации, интеграции и повсеместной информатизации уголовно-правовая охрана КИ становится важным инструментом защиты государства от различных угроз;

- защита общественных отношений, связанных с использованием КИ. Глава 28 УК РФ охватывает сферу, в которой важно обеспечивать конфиденциальность, целостность и доступность КИ, а также сохранность средств, используемых для ее обработки;

- борьба с растущим количеством преступлений в сфере КИ. С каждым годом совершенствуются технические устройства и информационные технологии, появляются новые способы совершения таких преступлений;

- противодействие скрытому характеру компьютерной преступности. Преступления в этой сфере часто носят анонимный, удаленный и сложный характер, что затрудняет их предотвращение и пресечение традиционными способами. Кроме того, существует проблема «цифрового следа» и его процессуального закрепления: данные

¹ Уголовный кодекс Российской Федерации : УК : принят Гос. Думой 24 мая 1996 г. : одобрен Советом Федерации 5 июня 1996 г. : послед. ред. // Собрание законодательства РФ. 17.06.1996. № 25. Ст. 2954.

легко изменяемы и требуют специальных познаний для изъятия и исследования, что создает риски утраты доказательств [1, с. 57];

– борьба с трансграничным характером компьютерной преступности. Преступник может находиться в одной стране, совершать преступление в другой, а последствия могут наступать в третьей, что усложняет противодействие компьютерной преступности в рамках одного государства [3, с. 89].

С развитием преступных способов при посягательствах на компьютерную и иную цифровую информацию законодателями вводятся новые нормы, изменяются и дополняются существующие, а также ужесточаются санкции за совершение подобного рода преступлений. Этот процесс, однако, носит асимметричный характер: ужесточение санкций опережает разработку гибких механизмов освобождения от ответственности, учитывающих специфику киберпространства. Несмотря на это, в таких условиях законодатель, наряду с ужесточением санкций за отдельные виды киберпреступлений, не исключает и применения в данных случаях особого поощрительного института уголовного права – освобождения от уголовной ответственности.

Так, в свете сложившейся судебной-следственной практики и тенденции на дифференциацию уголовной ответственности к преступлениям в сфере КИ (гл. 28 УК РФ) подлежат применению общие нормы об освобождении от уголовной ответственности (гл. 11 УК РФ). При этом правоприменитель уделяет особое внимание наиболее распространенным в практической деятельности основаниям освобождения от ответственности: деятельное раскаяние (ст. 75 УК РФ), примирение с потерпевшим (ст. 76 УК РФ), возмещение ущерба (ст. 76.1 УК РФ).

Рассмотрим положительные и отрицательные характеристики применения вышеперечисленных оснований освобождения от уголовной ответственности за совершение преступлений гл. 28 УК РФ.

Во-первых, специфика компьютерных преступлений требует особого подхода к оценке условий освобождения.

Условиями применения деятельного раскаяния к преступлениям гл. 28 УК РФ являются:

- совершение преступления впервые;
- категория преступления небольшой или средней тяжести;
- добровольная явка с повинной;
- способствование раскрытию и расследованию преступлений;
- возмещение причиненного ущерба или заглаживание вреда;
- утрата общественной опасности [4, с. 154].

Положительными аспектами применения деятельного раскаяния выступают: стимулирующая функция, компенсационный потенциал и процессуальная экономия. Иными словами, лицо, совершившее подобного рода преступления, сотрудничает с правоохранительными органами, тем самым более быстро обеспечивается восстановление нарушенных прав и интересов. Однако в данном случае возможны сложности в определении добровольности явки с повинной ввиду условий анонимности сетевого пространства [5, с. 27], например, в случаях, когда лицо было идентифицировано в результате оперативно-розыскных мероприятий. К тому же в законодательстве отсутствуют конкретные критерии оценки вклада способствованию раскрытию и расследованию преступлений. Особую сложность представляет проблема определения

размера вреда в цифровой среде, который подлежит возмещению, поскольку при определении размера ущерба следует учитывать не только прямые материальные потери, но и затраты на восстановление безопасности информационных систем, если ее целостность была нарушена. Кроме того, остается открытым вопрос о возможности освобождения лица, которое разработало, но не распространяло вредоносное программное обеспечение, однако добровольно передало его исходный код и информацию об уязвимостях правоохранительным органам.

Специфика применения ст. 76 УК РФ обусловлена особенностями объекта преступного посягательства и характером причиняемого вреда, в связи с чем возможны ограничения применения из-за проблемы идентификации потерпевшего, так как высока вероятность возникновения трудности определения круга потерпевших при массовых компьютерных атаках. Вместе с тем необходимо сказать о сложности заглаживания вреда, особенно в случае необходимости восстановления цифровой информации, и ограниченности действия, когда отсутствует возможность применения к преступлениям, посягающим на публичные интересы [2, с. 103].

Инновационный характер освобождения от уголовной ответственности с назначением судебного штрафа также представляет значительный интерес для правового регулирования ответственности за компьютерные преступления. На сегодняшний день имеются сложности определения размера штрафа ввиду установления тяжести наступивших последствий от киберпреступлений.

Освобождение от уголовной ответственности в связи с истечением сроков давности (ст. 78 УК РФ) при совершении компьютерных преступлений отличается значительными особенностями исчисления сроков давности:

- латентный характер компьютерных преступлений;
- сложность установления момента окончания преступления;
- проблемы определения момента обнаружения преступления.

В соответствии с положением части 2 ст. 78 УК РФ сроки давности исчисляются со дня совершения преступления. Однако при компьютерных преступлениях возникают сложности в определении этого момента.

Приведем пример судебной практики. По приговору Октябрьского районного суда г. Липецка от 20 декабря 2021 г. К.П.И., несудимый, осужден по: ч. 2 ст. 272 УК РФ к 1 году ограничения свободы; по ч. 2 ст. 273 УК РФ - к 1 году 6 месяцам ограничения свободы; по ч. 1 ст. 272 УК РФ - к штрафу в размере 20 000 рублей в доход государства; по ч. 1 ст. 273 УК РФ - к 1 году ограничения свободы; по ч. 1 ст. 272 УК РФ - к штрафу в размере 20 000 рублей в доход государства; по ч. 1 ст. 273 УК РФ - к 1 году ограничения свободы; по ч. 1 ст. 272 УК РФ - к штрафу в размере 20 000 рублей в доход государства; по ч. 1 ст. 273 УК РФ - к 1 году ограничения свободы; на основании ч. 2 ст. 69 УК РФ по совокупности преступлений путем частичного сложения наказаний окончательно назначено два года ограничения свободы со штрафом в размере 25 000 рублей в доход государства с возложением ограничений и обязанности, указанных в приговоре. Апелляционным постановлением Липецкого областного суда от 3 марта 2022 г. приговор в отношении К.П.И. изменен: он освобожден от наказания в виде штрафа в размере 20 000 рублей в доход государства, назначенного ему за каждое из трех преступлений, предусмотренных ч. 1 ст. 272 УК РФ, на основании п. «а» ч. 1 ст. 78 УК РФ в связи с истечением сроков давности уголовного преследования; наказание в виде штрафа в

размере 25 000 рублей в доход государства постановлено исключить из окончательного наказания, назначенного К.П.И. на основании ч. 2 ст. 69 УК РФ по совокупности преступлений; из резолютивной части приговора исключено указание о реквизитах для уплаты штрафа. Таким образом, К.П.И. был освобожден от уголовной ответственности и от наказания по ч. 1 ст. 272 УК РФ на основании п. «а» ч. 1 ст. 78 УК РФ в связи с истечением сроков давности².

По нашему мнению, применение гл. 11 УК РФ к преступлениям в сфере КИ требуют учета особого цифровой специфики. Уровень сформировавшейся судебной практики по данной категории преступлений ограничен отсутствием специальных критериев оценки условий освобождения.

Во-вторых, в уголовном законодательстве имеется перечень поощрительных норм об освобождении от уголовной ответственности за совершение отдельного вида преступлений, предусмотренных Особенной частью УК РФ. По преступлениям гл. 28 УК РФ такие нормы отсутствуют, что свидетельствует о применении только общих оснований освобождения, закрепленных в гл. 11 УК РФ.

Их отсутствие объясняется тем, что формирование главы 28 УК РФ происходило в период становления отечественного законодательства в сфере информационной безопасности. Первоначальная редакция (1996 г.) включала лишь два основных состава, что отражало недостаточную изученность феномена компьютерной преступности. Законодатель исходил из применимости общих институтов уголовного права без учета специфики цифровых технологий.

До настоящего времени в законодательстве и научной литературе отсутствует единый подход к определению критериев освобождения от ответственности за компьютерные преступления. Дискуссионными остаются вопросы спецификации деятельного раскаяния при киберпреступлениях, определение момента «добровольности» сообщения о преступлении, критерии возмещения ущерба в цифровой среде. Компьютерные преступления, как правило, относятся к категории преступлений небольшой и средней тяжести (за исключением квалифицированных составов), что изначально ориентировало на применение общих норм об освобождении.

Отсутствие единообразной судебной практики, а также ее отсутствие ввиду высокой латентности совершения рассматриваемых преступлений по вопросам освобождения от ответственности также затрудняет формулирование специальных норм.

По нашему мнению, внедрение специальных оснований освобождения от уголовной ответственности за преступления в сфере КИ возможно, так как виды и категории преступлений значительно изменяются в связи с развитием информационных технологий. Целью такой специальной нормы должно стать создание эффективного «золотого моста» для киберпреступника, побуждающего его к явке с повинной и оказанию технической помощи в обмен на освобождение от уголовной ответственности за преступления небольшой и средней тяжести при соблюдении ряда строгих условий.

Стоит предусмотреть специальное основание для статей 272, 273 УК РФ следующего содержания:

² Кассационное определение от 4 апреля 2024 г. по делу № 77-УД23-10-К1 // Верховный Суд Российской Федерации : офиц. сайт. URL: https://vsrf.ru/lk/practice/stor_pdf/2353844 (дата обращения: 09.02.2026).

«Примечание. Лицо, совершившее преступление, предусмотренное статьей 272 или 273 настоящего Кодекса, освобождается от уголовной ответственности, если оно добровольно и своевременно сообщило о совершенном преступлении в правоохранительные органы, способствовало раскрытию этого преступления, устранило последствия противоправного доступа или распространения вредоносных программ и возместило причиненный ущерб».

На основании этого внести дополнения в постановление Пленума Верховного Суда Российской Федерации от 15 декабря 2022 г. № 37 «О некоторых вопросах судебной практики по делам о преступлениях в сфере КИ, а также иных преступлениях, совершенных с использованием электронных или информационно-телекоммуникационных сетей, включая сеть «Интернет»»³, где определить, что для применения специального основания к ст. 272 и ст. 273 УК РФ необходимо понимать:

1. Своевременность сообщения – должна быть до наступления существенных вредных последствий или до момента, когда предотвратить эти последствия силами правоохранительных органов или потерпевшего стало невозможно.

2. Характер способствования раскрытию и расследованию преступления – предоставление информации об уязвимостях, алгоритмах вредоносных программ, механизмах несанкционированного доступа и т. д.

3. Специфику заглаживания вреда – восстановление защищенности КИ, устранение уязвимостей. Под устранением последствий должно пониматься не только техническое восстановление, но и предоставление потерпевшему полного отчета о произошедшем и рекомендаций по недопущению подобного в будущем.

Для эффективной реализации специальных оснований освобождения необходимо:

- установить порядок документального подтверждения устранения последствий;
- определить механизм оценки эффективности способствования раскрытию преступления;
- четко ограничить сферу применения специального основания, исключив из него случаи совершения преступлений в составе организованной группы, а также преступления, повлекшие тяжкие последствия или посягающие на информационную безопасность.

Данные меры будут способствовать повышению эффективности противодействия компьютерной преступности и обеспечению баланса цифровой безопасности.

Таким образом, совершенствование института освобождения от уголовной ответственности за преступления в сфере КИ представляет собой комплексную задачу, требующую системного подхода и учета национальных особенностей правового регулирования. Предлагаемые меры будут способствовать оптимизации уголовной репрессии, обеспечению баланса публичных и частных интересов, а также повышению эффективности противодействия компьютерной преступности в условиях цифровой трансформации общества. Перспективы противодействия преступлениям гл. 28 УК РФ

³ О некоторых вопросах судебной практики по уголовным делам о преступлениях в сфере компьютерной информации, а также иных преступлениях, совершенных с использованием электронных или информационно-телекоммуникационных сетей, включая сеть «Интернет»: постановление Пленума Верховного Суда Российской Федерации от 15 декабря 2022 г. № 37 // Бюллетень Верховного Суда РФ. № 3. Март. 2023.

должны быть направлены на разработку и внедрение предлагаемой нами концепции специальных оснований освобождения от уголовной ответственности.

СПИСОК ИСТОЧНИКОВ

1. Петрова И. А., Лобачев И. А. Преступления в сфере компьютерной (цифровой) информации: дискуссионные вопросы определения понятия, объекта уголовно-правовой охраны и предмета посягательств // Журнал прикладных исследований. 2020. № 1. С. 52–62.

2. Жаркова А. А. Об эффективности изменений, вносимых в гл. 28 Уголовного кодекса Российской Федерации // Вестник ЮГУ. 2015. № 1 (36). С. 102–104.

3. Ефремова М. А. Уголовная ответственность за неправомерное воздействие на критическую информационную инфраструктуру Российской Федерации // Вестник Казанского юридического института МВД России. 2022. Т. 13. № 4 (50). С. 86–92.

4. Сайтбеков А. М. Освобождение от уголовной ответственности в связи с деятельным раскаянием: теоретические и практические аспекты // Вестник Московского университета МВД России. 2025. № 2. С. 152–156.

5. Мосечкин И. Н. Проблемы уголовно-правовой охраны критической информационной инфраструктуры Российской Федерации // Всероссийский криминологический журнал. 2023. № 17 (1). С. 22–34.

REFERENCES

1. Petrova I. A., Lobachev I. A. Prestupleniya v sfere komp'yuternoj (cifrovoy) informacii: diskussionnye voprosy opredeleniya ponyatiya, ob'ekta ugolovno-pravovoj ohrany i predmeta posyagatel'stv [Crimes in the field of computer (digital) information: debatable issues of defining the concept, object of criminal law protection and subject of encroachments]. ZHurnal prikladnyh issledovanij - Journal of Applied Research. 2020, no. 1, pp. 52-62. (In Russ.).

2. Zharkova A. A. Ob effektivnosti izmenenij, vnosimyh v gl. 28 Ugolovnogo kodeksa Rossijskoj Federacii [On the Effectiveness of Changes Made to Chapter 28 of the Criminal Code of the Russian Federation]. Vestnik YUGU - Bulletin of the Southern Federal University. 2015, vol. 36, no. 1, pp. 102-104. (In Russ.).

3. Efremova M. A. Ugolovnaya otvetstvennost' za nepravomernoe vozdejstvie na kriticheskuyu informacionnuyu infrastrukturu Rossijskoj Federacii [Criminal liability for unlawful impact on the critical information infrastructure of the Russian Federation]. Vestnik Kazanskogo yuridicheskogo instituta MVD Rossii - Vestnik of the Kazan Law Institute of the Ministry of Internal Affairs of Russia. 2022, vol. 13, no. 4 (50), pp. 86-92. (In Russ.).

4. Saitbekov A. M. Osvobozhdenie ot ugolovnoj otvetstvennosti v svyazi s deyatel'nym raskayaniem: teoreticheskie i prakticheskie aspekty [Release from criminal liability in connection with active repentance: theoretical and practical aspects]. Vestnik Moskovskogo universiteta MVD Rossii - Vestnik of the Moscow University of the Ministry of Internal Affairs of Russia. 2025, no. 2, pp. 152-156. (In Russ.).

5. Mosechkin I. N. Problemy ugolovno-pravovoj ohrany kriticheskoj informacionnoj infrastruktury Rossijskoj Federacii [Problems of Criminal Law Protection of the Critical Information Infrastructure of the Russian Federation]. Vserossijskij kriminologicheskij zhurnal - All-Russian Journal of Criminology. 2023, vol. 1, no. 17, pp. 22-34. (In Russ.).

ИНФОРМАЦИЯ ОБ АВТОРЕ

Гафурова Эльмира Равиловна, доцент кафедры «Юриспруденция». Ижевский государственный технический университет имени М. Т. Калашникова. 426069, Приволжский ФО, Удмуртская Республика, г. Ижевск, ул. Студенческая, д. 7.

INFORMATION ABOUT AUTHOR

Gafurova Elmira Ravilevna, Associate Professor, Department of Jurisprudence, Kalashnikov Izhevsk State Technical University. 7 Studencheskaya St., Izhevsk, Udmurt Republic, Volga Federal District, 426069.

Статья поступила в редакцию 03.03.2026; одобрена после рецензирования 03.03.2026; принята к публикации 22.04.2026.

The article was submitted 03.03.2026; approved after reviewing 03.03.2026; accepted for publication 22.04.2026.