



Information security and its criminal law enforcement

G. V. Krasnoshapka¹, M. A. Sokolova²

¹Cordiant, Yaroslavl, Russian Federation

²Kirovsky District Court of Yaroslavl, Yaroslavl, Russian Federation

DOI: 10.18255/1996-5648-2025-3-484-491

Research article
Full text in Russian

The article examines issues of criminal law enforcement in the field of information security in the context of digital transformation. Special attention is paid to law enforcement practice regarding crimes related to the illegal circulation of confidential information, unauthorized access to computer data, and the use of malicious software. The authors analyze problems of crime qualification in this area and propose ways to improve criminal legislation.

Keywords: information security; criminal law; confidential information; unauthorized access; data protection; cybercrime; insider information; criminal liability

INFORMATION ABOUT AUTHORS

Krasnoshapka, Grigory V. | E-mail: gkrasnoshapka@bk.ru

Sokolova, Maria A. | E-mail: mariy0037@gmail.com



Информационная безопасность и её уголовно-правовое обеспечение

Г. В. Красношاپка¹, М. А. Соколова²

¹Кордиант, Ярославль, Российская Федерация

²Кировский районный суд г. Ярославля, Ярославль, Российская Федерация

DOI: 10.18255/1996-5648-2025-3-484-491

Научная статья

УДК 343.2/.7

Полный текст на русском языке

В статье рассматриваются вопросы уголовно-правового обеспечения информационной безопасности в условиях цифровизации общества. Особое внимание уделяется правоприменительной практике, связанной с преступлениями в сфере незаконного оборота конфиденциальных сведений, неправомерного доступа к компьютерной информации и использования вредоносных программ. Анализируются проблемы квалификации преступных действий и предлагаются возможные направления совершенствования уголовного законодательства в данной области.

Ключевые слова: информационная безопасность; уголовное право; конфиденциальная информация; неправомерный доступ; защита данных; киберпреступления; инсайдерская информация; уголовная ответственность

ИНФОРМАЦИЯ ОБ АВТОРАХ

Красношاپка, Григорий Витальевич

Е-mail: gkrasnoshapka@bk.ru

Юрисконсульт – юрист по судебной
и претензионной работе филиала АО «Кордиант»
в г. Ярославле

Соколова, Мария Алексеевна

Е-mail: mariy0037@gmail.com

Специалист – секретарь Кировского районного
суда г. Ярославля

В эпоху информационного общества, в котором информация является одним из фундаментальных ресурсов, информационная безопасность стала одним из ключевых факторов обеспечения стабильности как отдельных граждан, так и государства в целом. Развитие информационных технологий и повсеместное внедрение цифровых платформ порождают новые социальные и правовые проблемы. Например, распространение конфиденциальной информации, которая, в свою очередь, может быть использована в преступной деятельности. Данные обстоятельства обуславливают усиление уголовно-правовой защиты информации, что становится приоритет-

© ЯрГУ, 2025

Статья открытого доступа под лицензией CC BY (<https://creativecommons.org/licenses/by/4.0/>)

ным направлением государственной политики. Так, в РФ принята «Стратегия развития информационного общества в Российской Федерации на 2017–2030 годы».

В условиях обеспечения динамичного, непрерывного развития общества и государства важное место занимают вопросы создания, модернизации и реализации эффективно функционирующих правовых механизмов, направленных на охрану прав и интересов субъектов информационных отношений. Необходимость формирования системы правового обеспечения целостной и научно обоснованной информационной среды возникла в период изменений в экономическом и государственном устройстве России конца XX - начала XXI века. Неслучайно в доктрине информационной безопасности РФ в качестве одной из задач указывается на важность правовой защиты интересов личности, общества и государства в информационной сфере.

Основополагающими нормативно-правовыми актами, касающимися вопроса информации и информационной безопасности, следует считать ФЗ «Об информации, информационных технологиях и о защите информации», который дает общее понимание информации и мероприятий по ее защите; ФЗ «О безопасности», определяющий основы обеспечения безопасности в различных сферах, в том числе информационной.

Ранее названная доктрина определяет «цели, задачи и меры по реализации внутренней и внешней политики Российской Федерации в сфере применения информационных и коммуникационных технологий, направленные на развитие информационного общества, формирование национальной цифровой экономики, обеспечение национальных интересов и реализацию стратегических национальных приоритетов».

В Федеральном законе «Об информации, информационных технологиях и о защите информации» под информацией понимаются сведения (сообщения, данные) независимо от формы их представления. Данный акт также указывает на существование общедоступной (открытой) и конфиденциальной (закрытой) информации, доступ к которой ограничен ФЗ и актами Президента РФ. Конфиденциальная информация охватывает различные категории, каждая из которых имеет свои особенности и правовые рамки: государственная – информация, которая охраняется государственными органами и может повлиять на безопасность страны (например, военные данные, разведывательная информация); коммерческая – информация, которая имеет экономическое значение для хозяйствующих субъектов и не является общедоступной (например, данные о производственных процессах, технологии производства, списки клиентов, сведения о ценах); служебная – информация, относящаяся к внутренней деятельности организации и не подлежащая распространению (документы, касающиеся кадрового состава организации, внутренние отчеты); профессиональная тайна – информация, полученная в результате профессиональной деятельности, защищаемая законодательно для определенных профессий (например, для медицины, юриспруденции, бухгалтерии); персональные данные (личные данные) – информация, отно-

сящаяся к конкретному лицу (например, ФИО лица, дата и место его рождения, адрес проживания, регистрации, номер телефона и т. д.).

Информация, обладающая различной степенью закрытости, требует применения разнообразных мер по ее защите и обеспечению конфиденциальности. Это связано с тем, что разглашение информации, классифицированной по различным категориям закрытости, может иметь разнообразные социальные и правовые последствия. Например, утечка персональных данных может привести к нарушению прав человека, причинению морального вреда или финансового ущерба, а также негативным последствиям для репутации как физических, так и юридических лиц.

Каждый уровень конфиденциальности информации влечет за собой необходимость разработки специфических подходов и балансировки между правом на информацию и правом на неприкосновенность частной жизни. При этом ключевым аспектом является необходимость правильного применения.

Таким образом, адекватная реакция на потенциальные угрозы, связанные с раскрытием информации, требует комплексного подхода, учитывающего как юридические нормы, так и социальные аспекты, что в конечном итоге способствует созданию безопасной информационной среды.

Конфиденциальность информации – один из важнейших институтов права, позволяющий установить степень информационной защищенности, оптимально соотнести интересы личности, общества и государства, частного и публичного начала, определить границы дозволенного на вмешательства в сферу частного и личного интереса на законодательном уровне. Результативность и эффективность мер, в частности уголовно-правовых, реализуемых государством в области защиты информации, напрямую влияет на нормальное функционирование государственно-правовых институтов (институт законодательной, исполнительной и судебной власти).

Как отмечает Д. А. Калмыков в своей работе, информационная безопасность становится стратегическим направлением в борьбе с угрозами, связанными с несанкционированным доступом к данным и их искажением. Однако реализация этой задачи сопряжена с существенными вызовами, особенно в части создания эффективных правовых механизмов защиты [1, с. 10].

Е. В. Красненкова подчеркивает необходимость разработки четких уголовно-правовых норм для защиты интересов граждан и организаций. Среди наиболее серьезных угроз она выделяет киберпреступления, финансовые махинации и неправомерное использование данных, которые требуют оперативного реагирования со стороны правоохранительных органов [2, с. 10].

Вместе с тем потребность граждан и общества в целом в свободном обмене информацией обуславливает необходимость сохранения отдельных законодательно регламентированных ограничений ее распространении. Кроме того, в условиях чрезвычайного положения для обеспечения обороны страны, безопасности граждан и государства допускаются исключения из общего принципа открытости информации путем установления ограни-

чений в сфере поиска, получения, хранения и обмена информацией, а также введения режима защиты сведений.

Уголовное законодательство играет важную роль в обеспечении информационной безопасности. Например, статья 183 УК РФ предусматривает ответственность за разглашение или неправомерное использование сведений, составляющих коммерческую, налоговую или банковскую тайну, без согласия их владельца лицом, которому она была доверена или стала известна по службе или работе. Тем не менее её применение сопряжено с рядом трудностей. К ним относятся сложность доказывания умысла, установления размера ущерба и квалификации действий обвиняемых. Для преодоления данных проблем предлагается ввести четкие критерии определения состава преступлений и усовершенствовать методы доказывания ущерба.

Одной из ключевых проблем в борьбе с преступлениями в сфере информационной безопасности является их высокая латентность. Многие инциденты остаются незамеченными или не фиксируются, что затрудняет анализ и разработку эффективных мер защиты. Как отмечает И. В. Крупнов, причиной латентности часто являются недостаточное сотрудничество между государственными и частными структурами, а также слабое техническое оснащение правоохранительных органов [3, с. 163–168].

Для надлежащей информационной защиты необходимо разработать, совершенствовать и применять соответствующие технические и организационные меры, которые могут включать в себя установление прав доступа, шифрование данных, регулярное обновление программного обеспечения, а также обучение работников основам информационной безопасности, развитие программы обучения сотрудников правоохранительных органов по направлению информационных технологий.

Развитие цифровых технологий создает дополнительные риски для финансовых рынков. Одной из ключевых угроз является манипуляция рыночной информацией, что подрывает доверие к рынкам и наносит значительный ущерб экономике. Статья 185.6 УК РФ регулирует ответственность за такие действия, однако при ее реализации возникают проблемы выявления сложных схем манипуляций.

Деяние, описанное статьей 183 УК РФ, зачастую совершается с применением методов, подпадающих под статью 272 УК РФ (неправомерный доступ к компьютерной информации). В современном цифровом пространстве незаконное получение конфиденциальных сведений зачастую осуществляется с помощью несанкционированного проникновения в информационные системы, обхода средств защиты или использования вредоносного ПО. Таким образом, лицо, совершая взлом корпоративных сетей, баз данных или учетных записей сотрудников компании, получает доступ к коммерческой тайне, банковским операциям или налоговой отчетности, после чего может использовать соответствующую информацию в личных интересах либо передать третьим лицам.

Фактически неправомерный доступ к компьютерной информации (ст. 272 УК РФ) становится инструментом для реализации преступного

умысла, связанного с незаконным оборотом защищённых данных (ст. 183 УК РФ). Это особенно актуально в случаях промышленного шпионажа, финансовых махинаций и конкурентной борьбы, когда злоумышленники целенаправленно проникают в базы данных компаний или финансовых учреждений для хищения стратегически важных сведений. В таких случаях деяния виновного могут квалифицироваться по совокупности преступлений, что увеличивает тяжесть уголовной ответственности и влечёт за собой более серьёзные правовые последствия. Квалификация по совокупности преступлений целесообразна, поскольку посягательство в описанных случаях осуществляется на два объекта: информационную безопасность как отдельных граждан, так и организации, и на отношения, складывающиеся в экономической сфере.

Следует остановиться подробнее именно на статье 273 УК РФ «Создание, использование и распространение вредоносных компьютерных программ».

Первая часть указанной статьи предусматривает уголовную ответственность за создание программ или их модификацию, заведомо приводящие к несанкционированному уничтожению, блокированию, изменению либо копированию информации, нарушению работы цифровых систем, а также использованию программ или их носителей (дискеты, диски, флэш-накопители, съёмные жесткие диски).

Изменение программы подразумевает под собой существенное изменение функционала программного обеспечения в сравнении с авторским исполнением, например, появление в программе дополнительных функций, утрата имеющихся либо ограничение некоторых из них.

Вредоносная программа – это программное обеспечение в электронной форме, предназначенное для выполнения действий, наносящих вред информационным системам, данным или пользователям. Такие программы могут реализовывать различные вредоносные функции – от несанкционированного копирования, изменения и удаления информации до блокировки работы устройств и систем, а также обхода средств защиты.

Субъективная сторона данного преступления характеризуется прямым умыслом, то есть физическое вменяемое лицо, достигшее шестнадцатилетнего возраста, совершающее преступление, осознаёт, что создает программу – «вирус», «червь» и т. д. либо модифицирует ее, доводя до такого качества (таких функций) обычную программу, предвидит возможность или неизбежность наступления при её использовании другими пользователями вредных последствий и желает их наступления либо относится к ним безразлично.

Для данного преступления неважно наступление вредных или общественно опасных последствий. Преступление считается совершенным в тот момент, когда вредоносная программа использована либо распространена. Этот факт является одним из отличий от ст. 272 УК РФ.

Важно подчеркнуть, что для первой части данного преступления обязательны два признака, характеризующие способ совершения преступления и конкретное средство: действия не должны быть санкционированы вла-

дельцем информации (не разрешены); наличие самой вредоносной программы или существенные изменения в уже существующей.

Использование информационно-телекоммуникационных сетей, включая сеть Интернет, существенно трансформировало характер угроз, способных повлиять не только на техническую, но и на психосоциальную сферу общества.

Законодатель, учитывая данные обстоятельства, в целях дифференциации уголовной ответственности предусмотрел квалифицирующий признак — совершение противоправных деяний с использованием средств массовой информации либо информационно-телекоммуникационных сетей. Это связано с тем, что деструктивное воздействие информации определённого характера на психику человека может быть значительным, особенно при широком и неконтролируемом распространении таких сведений.

Совершение общественно опасных действий посредством цифровых каналов связи представляет собой серьёзную угрозу информационной безопасности, так как такие действия нередко сопровождаются высокой степенью латентности, вирусностью распространения контента и сложностями в установлении источника информации. В этой связи М. В. Бавсун указывает, что публичные призывы к совершению противоправных деяний и распространение информации соответствующего характера «вполне можно рассматривать в качестве синонимов», при этом особое значение имеют способ и средства распространения [4, с. 431].

Таким образом, распространение противоправной информации через цифровые каналы представляет собой одно из ключевых направлений угроз информационной безопасности, требующее соответствующей уголовно-правовой реакции.

Среди важных и дискуссионных вопросов остается вопрос о двубъектности (многообъектности) указанных преступлений. Как ранее было указано, посягательство в ряде случаев осуществляется на два объекта: информационную безопасность и отношения, складывающиеся в экономической сфере. Однако, как считает К. В. Степанова [5, с. 174], информация может выступать средством совершения преступления. Так, Р. Г. Асланян на примере ст. 170 УК РФ указывает, что «информация выступает средством, с помощью которого происходит негативное воздействие на объект преступления. Негативная информация деформирует развитие экономических отношений, обеспечивая «легализацию» в экономическом обороте земельных участков, зарегистрированных с нарушением законных требований» [6, с. 50].

Таким образом, названные ранее статьи направлены на обеспечение информационной безопасности и защиты доступа к информации, а также защиту имущества от неправомерных действий, поскольку в них рассматриваются акты, связанные с неправомерным использованием, раскрытием или доступом к защищенной информации. Названные в статьях деяния могут привести к нарушению информационной безопасности субъектов права, ставя под угрозу конфиденциальность, целостность и доступность информации. Приведенные уголовно-правовые нормы формируют комплекс-

ную защиту информационной безопасности, предотвращая незаконный доступ и использование критически важной информации. Однако вопрос о недостаточной адаптации права к стремительно изменяющимся современным технологиям остается актуальным; проблемы, связанные с излишней формализацией, неоправданной усложненностью юридического языка, его декларативностью, двусмысленностью, отсутствием терминологического единообразия также требуют решения.

На наш взгляд, необходимо совершенствовать, корректировать уже имеющиеся в уголовном законодательстве термины, связанные с информационным пространством, при изложении норм преимущественно использовать абстрактно-казуистический метод изложения, который в наибольшей степени будет способствовать одновременной стабильности и динамичности правовой области. Принимая во внимание сложность правоотношений, связанных с цифровыми технологиями, с технической, криминалистической точек зрения, мы считаем целесообразным использование бланкетного способа изложения норм.

Современное уголовное законодательство не всегда успевает за развитием технологий, что создаёт сложности в квалификации новых видов преступлений. В этом контексте важно не только совершенствовать нормативно-правовую базу, но и разрабатывать специальные обучающие программы для специалистов, работающих в этой области. Введение обязательных стандартов по защите информации для организаций, работающих с конфиденциальными данными, позволит повысить общий уровень кибербезопасности и сократить количество инцидентов, связанных с посягательством на информационную безопасность.

Ссылки

1. Калмыков Д. А. Информационная безопасность: понятие, место в системе уголовного законодательства РФ, проблемы правовой охраны: дис. ... канд. юрид. наук. Ярославль, 2005. 219 с. EDN NNOMVB
2. Красненкова Е. В. Обеспечение информационной безопасности в Российской Федерации уголовно-правовыми средствами: дис. ... канд. юрид. наук. М., 2006. 216 с. EDN NNUNXR
3. Крупнов И. В. К вопросу о понятии латентной преступности // 35 лет Российской правовой академии Министерства юстиции Российской Федерации и ее роль в развитии юридического образования: материалы международной научно-практической конференции: 2 т. (Москва, 13 октября 2005 г.). М.: РПА МЮ РФ, 2005. Т. 2. С. 163-168.
4. Бавсун М. В. Влияние признака публичности на криминализацию деяний и дифференциацию уголовной ответственности // Демидовский юридический журнал. 2023. Т. 13, № 3. С. 426-433. DOI 10.18255/2306-5648-2023-3-426-433
5. Степанова К. В. Информация как средство совершения преступления против собственности // Гуманитарные, социально-экономические и общественные науки. 2018. № 6. С. 174-177. DOI 10.23672/SAE.2018.6.14840
6. Асланян Р. Г. Информация как объект и средство совершения преступления в сфере экономики: вопросы взаимосвязи // Вестник КРУ МВД России. 2016. № 1. С. 48-52. EDN VYUDNN