

Уголовно-правовая характеристика преступлений, совершенных с использованием информационных и коммуникационных технологий

Criminal Law Characteristics of Crimes Committed Using Information and Communication Technologies

***Аннотация.** В статье исследуются уголовно-правовые признаки преступлений, совершаемых с использованием информационных и коммуникационных технологий (далее — ИКТ). Разграничиваются понятия преступлений в сфере компьютерной информации и преступлений, совершаемых с использованием ИКТ как способа совершения. Анализируются особенности объекта, объективной стороны, субъекта и субъективной стороны соответствующих деяний, рассматриваются проблемы квалификации дистанционных хищений и неправомерного доступа к компьютерной информации. Формулируются предложения по совершенствованию уголовного законодательства и правоприменительной практики.*

***Ключевые слова:** информационные и коммуникационные технологии, киберпреступность, преступления в сфере компьютерной информации, дистанционное мошенничество, компьютерная информация, уголовная ответственность, квалификация преступлений, цифровые доказательства.*

***Abstract.** This article examines the criminal law characteristics of crimes committed using information and communication technologies (hereinafter referred to as ICT). It distinguishes between crimes in the field of computer information and crimes in which ICT is used as a means or method of commission. The article analyzes the specific features of the object, objective element, subject, and subjective element of the relevant offences, as well as the issues involved in classifying remote theft and unauthorized access to computer information. Proposals are formulated for improving criminal legislation and law-enforcement practice.*

***Keywords:** information and communication technologies, cybercrime, crimes in the field of computer information, remote fraud, computer information, criminal liability, classification of crimes, digital evidence.*

Цифровизация экономики, государственного управления и повседневной коммуникации существенно изменила механизм совершения преступлений. Информационные и коммуникационные технологии используются не только как самостоятельный предмет уголовно-правовой охраны, но и как универсальный инструмент противоправного воздействия на собственность, общественную безопасность, права личности и порядок управления. Интернет, мобильная связь, банковские приложения, социальные сети, мессенджеры, электронные платёжные средства и программное обеспечение

позволяют совершать общественно опасные деяния дистанционно, серийно, анонимно и нередко трансгранично.

Проблема сохраняет высокую социальную значимость даже при сокращении зарегистрированной преступности рассматриваемой категории. По данным МВД России, в 2025 г. количество преступлений, совершённых с использованием информационно-телекоммуникационных технологий, уменьшилось на 11,8% по сравнению с 2024 г.; количество дистанционных краж сократилось на 23,6%, дистанционных мошенничеств — на 9%, а преступлений в сфере компьютерной информации — на 42,2%. Однако в абсолютном выражении речь идёт о 663 тыс. зарегистрированных киберпреступлений, 344 тыс. эпизодов мошенничества и 80 тыс. краж; материальный ущерб составил 189,5 млрд руб., а число потерпевших — 534,5 тыс. человек. Следовательно, снижение отдельных показателей не устраняет необходимости дальнейшего развития уголовно-правовых средств противодействия цифровой преступности.

Цель настоящей статьи заключается в комплексной характеристике преступлений, совершаемых с использованием ИКТ, и выявлении основных проблем их квалификации. Для её достижения необходимо определить содержание исследуемой категории, раскрыть признаки состава преступления и сформулировать практико-ориентированные направления совершенствования законодательства.

В законодательстве отсутствует единое легальное определение преступления, совершённого с использованием ИКТ. В правоприменительной статистике обычно объединяются две неодинаковые группы деяний: преступления, совершённые с использованием информационно-телекоммуникационных технологий, и преступления в сфере компьютерной информации. Такое объединение необходимо для учёта и профилактики, но в уголовно-правовом смысле эти группы не тождественны.

Преступления в сфере компьютерной информации предусмотрены прежде всего главой 28 УК РФ. Их непосредственным объектом выступают

общественные отношения, обеспечивающие безопасность создания, хранения, обработки, передачи и использования компьютерной информации, а также устойчивое функционирование информационных систем и сетей. К ним относятся неправомерный доступ к компьютерной информации (ст. 272 УК РФ), создание, использование и распространение вредоносных компьютерных программ (ст. 273 УК РФ), нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей (ст. 274 УК РФ), неправомерное воздействие на критическую информационную инфраструктуру Российской Федерации (ст. 274.1 УК РФ) и иные предусмотренные главой составы.

Более широкую группу образуют преступления, в которых ИКТ выполняют роль средства, способа, обстановки либо канала совершения посягательства. К ним могут относиться мошенничество с использованием электронных средств платежа и в сфере компьютерной информации (ст. 159.3, 159.6 УК РФ), кража с банковского счёта или в отношении электронных денежных средств (п. «г» ч. 3 ст. 158 УК РФ), вымогательство с использованием сети «Интернет», незаконный оборот наркотических средств посредством информационно-телекоммуникационных сетей, публичные призывы к экстремистской деятельности, распространение заведомо ложной информации и иные деяния. В данных случаях основным объектом выступают не отношения по обеспечению безопасности компьютерной информации, а собственность, общественная безопасность, конституционные права личности или другие охраняемые уголовным законом блага.

Таким образом, под преступлениями, совершаемыми с использованием ИКТ, целесообразно понимать предусмотренные уголовным законом общественно опасные виновные деяния, при совершении которых информационные системы, информационно-телекоммуникационные сети, программно-технические средства, электронные сообщения или электронные платёжные инструменты используются как способ, средство, условие либо

предмет преступного посягательства. Это понятие охватывает преступления главы 28 УК РФ, но не сводится к ним.

Предлагаемый подход имеет значение для правильной квалификации. Сам факт использования телефона, банковского приложения или сети «Интернет» не превращает любое деяние в преступление в сфере компьютерной информации. Решающее значение имеет направленность умысла, характер воздействия на охраняемый объект и способ завладения имуществом либо причинения иного вреда.

Особенности объекта преступлений, совершаемых с использованием ИКТ, обусловлены многообразием соответствующих составов. При неправомерном доступе к компьютерной информации основным непосредственным объектом является установленный порядок охраны конфиденциальности, целостности и доступности компьютерной информации. В преступлениях против собственности объектом выступают отношения собственности, а ИКТ чаще всего являются способом преодоления воли потерпевшего, введения его в заблуждение либо незаконного распоряжения денежными средствами.

Предметом преступления по ст. 272 УК РФ является охраняемая законом компьютерная информация. Согласно примечанию к ст. 272 УК РФ под компьютерной информацией понимаются сведения (сообщения, данные), представленные в форме электрических сигналов независимо от средств их хранения, обработки и передачи. На практике это могут быть персональные данные, реквизиты банковских карт, пароли, сведения о движении денежных средств, базы клиентов, служебная переписка, программный код и иные цифровые данные. При этом уголовная ответственность по ст. 272 УК РФ наступает не за любой несанкционированный доступ, а при наличии предусмотренных законом последствий: уничтожения, блокирования, модификации либо копирования компьютерной информации.

Объективная сторона преступлений данной категории нередко отличается сложным и многоэтапным механизмом. Например, хищение

денежных средств может включать получение сведений о потерпевшем через фишинговый ресурс, убеждение потерпевшего сообщить код подтверждения посредством телефонного разговора, вход в личный кабинет банка, перевод денежных средств на подконтрольный счёт и последующее обналичивание. Отдельные действия в такой цепочке могут иметь самостоятельную уголовно-правовую оценку, если образуют признаки различных составов, в том числе неправомерного доступа к компьютерной информации, использования вредоносных программ, мошенничества или кражи.

Особое значение имеет разграничение кражи и мошенничества при посягательствах на безналичные денежные средства. Если виновный тайно использует реквизиты карты, полученные без участия владельца, либо самостоятельно осуществляет перевод с банковского счёта потерпевшего, содеянное при наличии прочих признаков следует квалифицировать как кражу с банковского счёта или в отношении электронных денежных средств. Если же потерпевший под влиянием обмана сам переводит средства на счёт виновного или сообщает сведения, предоставляющие возможность распорядиться деньгами, содеянное может образовывать мошенничество. Однако этот критерий требует оценки фактической роли потерпевшего: добровольное внешне действие, совершённое вследствие обмана, не исключает хищения, но влияет на выбор конкретной уголовно-правовой нормы.

Объективная сторона цифровых преступлений осложняется возможностью совершения действий на территории нескольких государств. Сервер, с которого направлена вредоносная программа, потерпевший, банк, оператор связи и лицо, получающее похищенные средства, могут находиться в разных субъектах Российской Федерации или в разных странах. Это затрудняет установление места совершения преступления, определение подследственности и получение цифровых следов. Поэтому особое значение приобретают фиксация IP-адресов, журналов событий, данных о соединениях, сведений операторов связи и кредитных организаций, а также соблюдение

процессуального порядка изъятия и исследования электронных носителей информации.

Субъект большинства преступлений, совершаемых с использованием ИКТ, общий: вменяемое физическое лицо, достигшее возраста уголовной ответственности. Вместе с тем квалифицирующее значение может иметь использование виновным служебного положения, участие в организованной группе, наличие специального доступа к информационной системе или принадлежность к лицам, обязанным соблюдать правила эксплуатации соответствующих средств и сетей. Так, при нарушении правил эксплуатации средств хранения, обработки или передачи компьютерной информации субъект обладает специальными признаками, вытекающими из его обязанностей по доступу, эксплуатации или защите информационной инфраструктуры.

Субъективная сторона преимущественно характеризуется умышленной формой вины. При хищениях виновный осознаёт противоправность обращения чужого имущества в свою пользу или пользу иных лиц, предвидит причинение имущественного вреда и желает этого; обязательным признаком выступает корыстная цель. Для неправомерного доступа к компьютерной информации важно установить осознание отсутствия законных оснований для доступа к охраняемым сведениям. Наличие технической возможности войти в систему само по себе не означает правомерность такого доступа: необходимо учитывать пределы предоставленных полномочий, режим доступа к информации и цели использования полученных данных.

Одной из наиболее сложных проблем является квалификация деяний, совершаемых с применением методов социальной инженерии. Злоумышленник может представляться сотрудником банка, правоохранительного органа, оператора связи или государственного органа, сообщать ложные сведения о «безопасном счёте», убеждать установить приложение удалённого доступа либо назвать одноразовый код. В подобных случаях следует установить, получил ли виновный доступ к банковской

системе самостоятельно либо потерпевший, введённый в заблуждение, сам распорядился средствами. Формальное отнесение всех дистанционных хищений к мошенничеству не учитывает различия в механизме изъятия имущества и способно привести к ошибочной квалификации.

Не менее важна проблема конкуренции норм. В случае, когда неправомерный доступ к компьютерной информации является способом последующего хищения, необходимо выяснить, охватывается ли причинённый вред составом преступления против собственности либо требует самостоятельной квалификации по ст. 272 УК РФ. Самостоятельная оценка оправдана, когда действия по незаконному доступу причиняют вред отношениям в сфере информационной безопасности, выходящий за пределы механизма хищения, либо обладают всеми признаками самостоятельного оконченного состава. В противном случае следует избегать искусственного удвоения уголовно-правовой оценки одного деяния.

Для доказывания субъективной стороны важны не только показания потерпевших и обвиняемого, но и цифровые данные: переписка в мессенджерах, сведения о регистрации аккаунтов, записи телефонных соединений, история операций по банковским счетам, данные об использовании устройств, программ и сетевых идентификаторов. Вместе с тем цифровой след не должен восприниматься как безусловное доказательство вины конкретного лица. Использование VPN, чужих учётных записей, SIM-карт, удалённого доступа и вредоносного программного обеспечения требует комплексной проверки происхождения и достоверности электронных доказательств.

Первым направлением является унификация понятийного аппарата. В уголовном законодательстве и правоприменительной практике используются близкие, но не совпадающие термины: «компьютерная информация», «информационно-телекоммуникационные сети», «электронные средства платежа», «информационные технологии». Представляется обоснованным закрепить в разъяснениях Верховного Суда РФ единые подходы к пониманию

роли ИКТ как предмета, средства или способа совершения преступления. Это позволит сократить различия в квалификации и повысить предсказуемость судебных решений.

Вторым направлением должна стать разработка детализированных разъяснений о разграничении дистанционных краж, мошенничества с использованием электронных средств платежа и мошенничества в сфере компьютерной информации. Для правоприменителя принципиально важно установить: кто совершил юридически значимое действие по распоряжению деньгами; был ли доступ к информационной системе правомерным; каким способом получены реквизиты и коды; являлось ли вмешательство в работу системы необходимым элементом хищения. Единые ориентиры особенно необходимы в ситуациях социальной инженерии, использования программ удалённого доступа и компрометации банковских аккаунтов.

Третье направление связано с повышением качества расследования. Следователь и дознаватель должны своевременно обеспечивать сохранность электронных носителей, получать сведения от банков, операторов связи и владельцев информационных систем, назначать компьютерно-технические экспертизы, фиксировать цифровую информацию с соблюдением требований уголовно-процессуального закона. Значимым является повышение специализации сотрудников правоохранительных органов и развитие устойчивых каналов взаимодействия с кредитными организациями, операторами связи и цифровыми платформами.

Четвёртым направлением выступает совершенствование профилактики. Снижение зарегистрированных ИТ-преступлений в 2025 г. сопровождалось уменьшением дистанционных краж и мошенничеств, однако преступники приспосабливаются к новым ограничительным мерам и переносят активность в менее урегулированные сегменты цифровой среды. Поэтому уголовно-правовые меры должны дополняться техническими средствами защиты, ограничением оборота инфраструктуры, используемой для массовых

мошеннических звонков, оперативным блокированием фишинговых ресурсов и регулярным информированием граждан о типичных схемах обмана.

Преступления, совершаемые с использованием информационных и коммуникационных технологий, представляют собой широкую и неоднородную группу уголовно наказуемых деяний. Она включает как собственно преступления в сфере компьютерной информации, так и традиционные по объекту посягательства преступления, совершаемые с применением цифровых средств. Их объединяет не единый родовый объект, а способ, средство, условия либо предмет преступной деятельности.

Ключевое значение для верной уголовно-правовой оценки имеют установление механизма доступа к компьютерной информации или денежным средствам, определение фактической роли потерпевшего, анализ направленности умысла и исключение необоснованной совокупности составов. Учитывая масштаб причиняемого вреда, а также быстрое изменение мошеннических технологий, требуется последовательное развитие нормативных разъяснений, специализации расследования и механизмов межведомственного взаимодействия. Комплексный подход позволит обеспечить баланс между эффективной защитой личности, собственности и информационной безопасности, с одной стороны, и соблюдением принципов законности и справедливой квалификации — с другой.

Список использованных источников

1. МВД: число преступлений, совершённых с использованием информационно-телекоммуникационных технологий, в 2025 году сократилось на 11,8% // ТАСС. 29 января 2026 г. URL: <https://tass.ru/obschestvo/26280465> (дата обращения: 16.09.2026).
2. МВД сообщило о снижении числа киберпреступлений в РФ в 2025 году на 12% // Интерфакс. 18 февраля 2026 г. URL: <https://www.interfax.ru/digital/1073418> (дата обращения: 16.09.2026).
3. Уголовный кодекс Российской Федерации от 13.06.1996 № 63-ФЗ (в действующей редакции).

4. Уголовно-процессуальный кодекс Российской Федерации от 18.12.2001 № 174-ФЗ (в действующей редакции).

5. Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации».

6. Постановление Пленума Верховного Суда Российской Федерации от 30.11.2017 № 48 «О судебной практике по делам о мошенничестве, присвоении и растрате».