Противодействие преступности в сфере использования информационно-коммуникационных технологий

1.

2. **Преступления в сфере информационных технологий** включают как распространение вредоносных программ, взлом паролей, кражу номеров банковских карт и других банковских реквизитов, так и распространение противоправной информации (клеветы, материалов порнографического характера, материалов возбуждающих межнациональную и межрелигиозную вражду и т.д.) через Интернет, а также вредоносное вмешательство через компьютерные сети в работу различных систем.

В соответствии с действующим уголовным законодательством Российской Федерации под преступлением в сфере компьютерной информации понимаются совершаемые в сфере информационных процессов и посягающие на информационную безопасность деяния, предметом которых являются информация и компьютерные средства.

Ответственность за совершение указанных преступлений предусмотрена главой 28 Уголовного кодекса Российской Федерации.

По Уголовному кодексу Российской Федерации преступлениями в сфере компьютерной информации являются:

— 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 и распространение порнографии (ст. 274 УК РФ).

Общественная опасность противоправных действий в области электронной техники и информационных технологий выражается в том, что они могут повлечь за собой нарушение деятельности автоматизированных систем управления и контроля различных объектов, серьезное нарушение работы ЭВМ и их систем, несанкционированные действия по уничтожению, модификации, искажению, копированию информации и информационных ресурсов, иные формы незаконного вмешательства в информационные системы, которые способны вызвать тяжкие и необратимые последствия

3. В настоящее время **банковская система** все больше уделяет внимание упрощающим жизнь человека высоким технологиям, активно внедряя их в различные операционные процессы для взаимодействия финансового учреждения с многочисленными клиентами. Наиболее популярны телефонные приложения «СбербанкОнлайн», «ВТБ-Онлайн» и прочие, с помощью которых можно в любое время суток осуществлять банковские операции, оплатив, например, через личный кабинет с помощью банковской карты любой товар в интернет-магазинах.

Вместе с тем усиливающаяся информатизация современного общества имеет и негативные последствия, заключающиеся в появлении и росте особых разновидностей правонарушений, злоумышленники, в свою очередь, не стоят на месте.

Одна из таких групп преступных посягательств выражается в совершении различных корыстных действий (бездействия) в сферах ИТТ с применением компьютерной информации, электронных (цифровых) технологий и т.п. Чтобы не стать жертвой преступников, использующих ИКТ, применяйте эти простые правила:

- не сообщайте свои персональные данные, а также банковских карт и счетов третьим лицам, даже если неустановленное лицо представилось сотрудником банка, прекратите разговор и обратитесь в банк лично либо по телефону горячей линии;
- не выполняйте указания неизвестных лиц по вводу каких-либо команд и символов в телефоном режиме, а также с использованием банкомата;
- не перечисляйте денежные средства неизвестным лицам, представляющимся знакомыми ваших родных, сотрудниками правоохранительных органов (положите трубку и позвоните лицу, который по словам неизвестного попал в беду/нуждается в помощи);
- прежде чем приобретать какой-либо товар или услугу с использованием сети Интернет, ознакомьтесь с отзывами, оставленными ранее покупателями/клиентами;
- при вводе пин-кода банковской карты закрывайте его рукой, не храните пин-код совместно с банковской картой.

4. **Хищение, совершенное с использованием современных информационно-коммуникационных технологий** является общественно опасным деянием, причиняющим значительный имущественный вред гражданам. Наблюдается значительный рост преступлений, связанных с хищением денежных средств у физических и юридических лиц из банков и иных кредитных организаций, совершаемых в виде дистанционного мошенничества.

Злоумышленники используют разные способы обмана людей в интернете от спама до создания сайтов-двойников. Они преследуют цель - получить персональные данные пользователя, номера банковских карт, паспортные данные, логины и пароли. У потерпевших похищаются денежные средства под предлогом совершения каких-либо

банковских операций, направленных на восстановление якобы поврежденных данных о банковских вкладах, либо путем введения их в заблуждение. При этом зачастую злоумышленники представляются банковскими работниками или представителями правоохранительных органов.

В подавляющем большинстве случаев преступники используют следующие основные схемы обмана. Так, злоумышленник звонит или отправляет смс-сообщение на телефон, сообщая что банковская карта или счет мобильного телефона потерпевшего заблокированы в результате преступного посягательства, и затем представляясь сотрудником банка или телефонной компании, предлагает набрать комбинацию цифр на мобильном телефоне или банкомате для разблокировки, в результате чего денежные средства перечисляются на счет преступника.

Может поступить звонок от «сотрудника» службы технической поддержки оператора мобильной связи с предложением подключить новую услугу или для перерегистрации во избежание отключения связи из-за технического сбоя, или для улучшения качества связи абоненту предлагается набрать под диктовку код, который является комбинацией для перевода денежных средств со счета абонента на счет мошенника.

Потерпевший заказывает товар через сеть Интернет, оплачивает его путем перечисления денежных средств на банковскую карту продавца, но не получает заказ. В таких случаях важно быть внимательным и не использовать непроверенные сайты, в том числе сайты-двойники.

При возникновении подобных ситуаций необходимо оперативно самостоятельно связаться с оператором банка, сотовой связи с целью блокировки карты, номера телефона, отключения услуг и т.д. Данные действия способствуют незамедлительному установлению злоумышленника и предотвращению совершения преступления.

Важно помнить! Ни одна организация, включая банк, не вправе требовать реквизиты Вашей карты включая CVV-код.

Исключите разговоры с неизвестными лицами по поводу состояния Ваших банковских счетов. При необходимости получить кредит или воспользоваться иными банковскими услугами обращайтесь непосредственно в офисы банковских организаций или пользуйтесь официальными сайтами и приложениями проверенных банков.

5. В соответствии с распоряжением Президента Российской Федерации Генеральному прокурору Российской Федерации поручено подписание **Конвенции ООН против киберпреступности.**

Государства-члены ООН в декабре 2024 года приняли первую юридически обязывающую Конвенцию по киберпреступности, которая является универсальным международным договором в борьбе с противоправными деяниями в цифровой сфере.

25 октября 2025 года Генеральный прокурор России Александр Гуцан, а также уполномоченные представители 71 государства подписали Конвенцию ООН против киберпреступности.

Документ предусматривает оказание оперативной помощи для ускорения расследования киберпреступлений, процедур экстрадиции, изъятия доходов от преступной деятельности и возврата активов, защиты детей от сексуального насилия с использованием IT, помощи пострадавшим от действий киберпреступников, а также обязанность стран-участниц разрабатывать программы компенсации ущерба жертвам мошенничества, программы реабилитации и восстановления пострадавших.

Такое сотрудничество позволит объединить усилия правоохранительных органов различных стран в области информационной безопасности в интересах всего мирового сообщества.

6. Кибергруминг — это современное понятие интернет преступлений эротического характера, совершенного против несовершеннолетних детей в процессе доверительного общения в сети Интернет.

Жертвой интернет злоумышленника может стать любой, но чаще это дети, не достигшие совершеннолетнего возраста, которые более подвержены манипуляциям. Бывают случаи, когда ребенок страдает от дефицита внимания и хочет восполнить недостаток заинтересованности родителей в его жизни. Находясь в такой обстановке, он может начать воспринимать любое положительное внимание к себе, как праздник, не подозревая опасности.

Любопытство и недостаток жизненного опыта могут сделать ребенка легко доступной жертвой преступления. Пытаясь узнать больше об интимной жизни, вопреки страху родительского наказания, дети доверяются незнакомцам из интернета, которые подробно рассказывают об интимных отношениях и предлагают вступить в половую связь.

Как все начинается? Злоумышленник знакомится с ребенком в социальных сетях, мессенджерах или на форумах, притворяясь сверстником и, скрывая свой истинный возраст, начинает самое простое общение. Параллельно он узнает личную информацию о ребенке, об отношениях в семье, где проживает, с кем общается, какой адрес школы или дома, номер мобильного телефона, другие профили в социальных сетях.

Наладив доброжелательное общение, лжедруг приглашает на видеозвонки, личные встречи, выманивая интимные изображения несовершеннолетнего. С помощью видеозвонков и отправленных фотографий создаётся порнографический материал, который в дальнейшем может незаконно распространяться и использоваться, как инструмент шантажа. Дети не знают, что делать в таких ситуациях, поэтому продолжают поддаваться на манипуляции.

Как понять, что ваш ребенок в опасности? Он становится более скрытным и замкнутым. Пытается скрыть такого рода переписку, резко реагирует, если родители забирают гаджеты, начинает просить больше денег на «карманные расходы». Он может удалять свои социальные сети и просить поменять ему номер телефона. Эти проблемы могут привести к снижению его успеваемости в школе и он перестает общаться с друзьями.

Если ваш ребенок оказался в такой ситуации, постарайтесь сохранять спокойствие и действовать последовательно. Сохраните все фотографии, адреса, скрины переписок и другие улики, обратитесь в правоохранительные органы. Знайте, такие деяния против половой неприкосновенности несовершеннолетних и общественной нравственности влекут уголовную ответственность вплоть до 20 лет лишения свободы.

В такие моменты детям нужна максимальная поддержка, а не осуждение за проступок. Не нужно стыдить, осуждать или обвинять ребёнка. Лучше сказать, что вы его любите и поможете ему. Контролируйте свои негативные эмоции: страх, обиду, гнев. Они усиливают тревогу и переживания ребёнка. Нужно быть готовым к тому, что у ребёнка могут появиться эмоциональные и поведенческие проблемы во взаимоотношениях или в учёбе. Нужно помочь ему вернуться к ежедневным делам, чаще

разговаривать й слушать его. Если вы чувствуете, что ребенок и вы сами не справляетесь с этой ситуацией самостоятельно, следует обратиться за психологической поддержкой.

Чтобы ваш ребенок не стал жертвой такого рода преступления, выстраивайте с ним доверительные отношения, проявляйте заботу, оказывайте поддержку, предупреждайте об опасности общения с незнакомыми людьми, своим примером показывайте, как интересно можно проводить время без гаджетов.

Помните, что родители несут ответственность за жизнь и здоровье ребенка, его нравственное развитие.

7. Под **хищением** понимаются совершенные с корыстной целью противоправные безвозмездное изъятие и (или) обращение чужого имущества в пользу виновного или других лиц, причинившие ущерб собственнику или иному владельцу этого имущества (п. 1 примечаний к ст. 158 УК РФ).

Обман как способ совершения хищения или приобретения права на чужое имущество может состоять в сознательном сообщении (представлении) заведомо ложных, не соответствующих действительности сведений, либо в умолчании об истинных фактах, либо в умышленных действиях (например, в предоставлении фальсифицированного товара или иного предмета сделки, использовании различных обманных приемов при расчетах за товары или услуги или при игре в азартные игры, в имитации кассовых расчетов и т.д.), направленных на введение владельца имущества или иного лица в заблуждение. Злоупотребление доверием при мошенничестве заключается в использовании с корыстной целью доверительных отношений с владельцем имущества или иным лицом, уполномоченным принимать решения о передаче этого имущества третьим лицам. Доверие может быть обусловлено различными обстоятельствами, например служебным положением лица либо его личными отношениями с потерпевшим (п. п. 2, 3 Постановления Пленума Верховного Суда РФ от 30.11.2017 № 48 "О судебной практике по делам о мошенничестве, присвоении и растрате", далее - Постановление Пленума Верховного Суда РФ от 30.11.2017 N 48).

Мошенничество признается оконченным с момента, когда имущество поступило в незаконное владение виновного или других лиц и они получили реальную возможность пользоваться или распорядиться им по своему усмотрению.

8. Как не стать жертвой телефонного мошенничества?

Если гражданин предполагает, что стал жертвой телефонного мошенничества, ему необходимо обратиться в органы внутренних дел с соответствующим заявлением. В заявлении следует максимально подробно рассказать о всех обстоятельствах события. Кроме этого, следует сообщить о факте телефонного мошенничества в абонентскую службу мобильного оператора, который обслуживает номер преступника. Если гражданин, к примеру, совершил перевод денежной суммы по мобильной сети, то принятие оператором экстренных мер может позволить заблокировать перевод и вернуть деньги.

Для того чтобы не стать такой жертвой, необходимо следовать определенным правилам. Например:

- если получен звонок с просьбой о срочной денежной помощи для известного гражданину лица (знакомого, родственника и т.п.), следует не принимать решение сразу,

идя на поводу у позвонившего, а проверить полученную от него информацию, перезвонив вышеуказанным лицам, или связаться с ними иными способами;

- нельзя сообщать по телефону личные сведения или данные банковских карт, которые могут быть использованы злоумышленниками для неправомерных действий;

- нельзя перезванивать на номер, если он незнаком, и т.п.

9. Телефонное мошенничество в зависимости от размера похищенного и других обстоятельств деяния (например, имеются или отсутствуют признаки преступления) может повлечь административную или уголовную ответственность.

На основании ч. 1 ст. 7.27 КоАП РФ мелкое хищение чужого имущества, стоимость которого не превышает 1 000 руб., путем кражи, мошенничества, присвоения или растраты при отсутствии признаков преступления влечет наложение административного штрафа в размере до пятикратной стоимости похищенного имущества, но не менее 1 000 руб., либо административный арест на срок до 15 суток, либо обязательные работы на срок до 50 часов.

Согласно ч. 2 указанной статьи мелкое хищение чужого имущества стоимостью более 1 000 руб., но не более 2 500 руб. путем кражи, мошенничества, присвоения или растраты при отсутствии признаков преступления влечет наложение административного штрафа в размере до пятикратной стоимости похищенного имущества, но не менее 3 000 руб., либо административный арест на срок от 10 до 15 суток, либо обязательные работы на срок до 120 часов.

Кроме того, на основании ст. 7.27.1 КоАП РФ причинение имущественного ущерба собственнику или иному владельцу имущества путем обмана или злоупотребления доверием при отсутствии признаков уголовно наказуемого деяния влечет наложение административного штрафа в размере до пятикратной стоимости причиненного ущерба, но не менее 5 000 руб.

Статья 159 УК РФ предусматривает различные виды наказания за мошенничество в зависимости от конкретных обстоятельств.

Согласно ч. 1 указанной статьи мошенничество наказывается штрафом в размере до 120 000 руб. или в размере заработной платы или иного дохода осужденного за период до 1 года, либо обязательными работами на срок до 360 часов, либо исправительными работами на срок до 1 года, либо ограничением свободы на срок до 2 лет, либо принудительными работами на срок до 2 лет, либо арестом на срок до 4 месяцев, либо лишением свободы на срок до 2 лет.

Квалифицирующими признаками телефонного мошенничества, к примеру, являются следующие:

- совершение группой лиц по предварительному сговору, а равно с причинением значительного ущерба гражданину;

- совершение лицом с использованием своего служебного положения, а равно в крупном размере.

10. **Прокурор разъясняет, за какие преступления в сфере компьютерной информации предусмотрена конфискация имущества**

С 24 июня 2023 года вступают в силу изменения, внесенные Федеральным законом от 13.06.2023 № 214-ФЗ в статью 104.1 Уголовного кодекса Российской Федерации (конфискация имущества).

С учетом изменений подлежит принудительному безвозмездному изъятию и обращению в собственность государства на основании обвинительного приговора имущество, полученное в результате:

- создания, использования и распространения вредоносных компьютерных программ;

- неправомерного воздействия на критическую информационную инфраструктуру Российской Федерации;

- неправомерного доступа к компьютерной информации;

- нарушения правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей.

11. **Прокурор разъясняет: существенно ужесточена ответственность физических и юридических лиц за нарушения закона при обращении с персональными данными**

С 30 мая 2025 года действует Федеральный закон от 30 ноября 2024 года № 420-ФЗ «О внесении изменений в Кодекс Российской Федерации об административных правонарушениях», которым внесены изменения в статью 13.11 указанного Кодекса. Ею установлена административная ответственность за нарушение законодательства Российской Федерации в области персональных данных при отсутствии признаков уголовно наказуемого деяния.

Размер административного штрафа за обработку персональных данных в случаях, не предусмотренных законодательством, либо за обработку персональных данных, несовместимую с целями их сбора, для граждан составит от 10 до 15 тыс. руб., для должностных лиц – от 50 до 100 тыс. руб., для юридических лиц – от 150 до 300 тыс. руб. Повторное совершение данного правонарушения лицом, подвергнутым административному наказанию, повлечет наложение административного штрафа на граждан от 15 до 30 тыс. руб., на должностных лиц – от 100 до 200 тыс. руб., на юридических лиц – от 300 до 500 тыс. руб.

Введена административная ответственность операторов при обработке персональных данных.

Невыполнение оператором обязанности по уведомлению уполномоченного государственного органа о намерении осуществлять обработку персональных данных повлечет наложение административного штрафа на граждан от 5 до 10 тыс. руб., на должностных лиц – от 30 до 50 тыс. руб., на юридических лиц – от 100 до 300 тыс. руб.

Ненадлежащее уведомление оператором уполномоченного органа о неправомерной или случайной передаче персональных данных повлечет наложение административного штрафа на граждан от 50 до 100 тыс. руб., на должностных лиц – от 400 до 800 тыс. руб., на юридических лиц – от 1 до 3 млн руб.

Установлена административная ответственность операторов за действия или бездействие, повлекшие неправомерную передачу информации, включающей персональные данные или идентификаторы, то есть уникальные сведения для определения лиц с использованием биометрических персональных данных.

Ответственность начинается с незаконной передачи информации от тысячи до 10 тыс. субъектов персональных данных или от 10 тыс. до 100 тыс. идентификаторов, за что административный штраф составит для граждан от 100 до 200 тыс. руб., для

должностных лиц – от 200 до 400 тыс. руб., для юридических лиц – от 3 до 5 млн руб., заканчивается штрафом за незаконную передачу информации о более 100 тыс. субъектов персональных данных или более 1 млн идентификаторов для граждан от 300 до 400 тыс. руб., для должностных лиц – от 400 до 600 тыс. руб., для юридических лиц – от 10 до 15 млн руб. Повторное совершение указанных действий, лицом, подвергнутым административному наказанию, повлечет наложение административного штрафа на граждан от 400 до 600 тыс. руб., на должностных лиц – от 800 тыс. руб. до 1,2 млн руб., для юридических лиц – от 1 до 3 % совокупного размера суммы выручки за предшествующий год или часть года, в котором совершено правонарушение, или той же части собственных средств кредитной организации, но не менее 20 и не более 500 млн руб.

Также введена ответственность за неправомерную передачу специальной категории персональных данных, биометрических персональных данных, в том числе повторно лицом, подвергнутым административному наказанию.

Особое внимание следует обратить на то, что 50-процентная скидка при быстрой уплате штрафа не применяется по всем составам, предусмотренным статьей 13.11 Кодекса Российской Федерации об административных правонарушениях.

Кроме того, статьей 272.1 УК РФ, введенной Федеральным законом от 30 ноября 2024 года № 420-ФЗ «О внесении изменений в Уголовный кодекс Российской Федерации», с 11 декабря 2024 года установлена уголовная ответственность занезаконные действия с персональными данными.

В соответствии с ней незаконные использование, передача, сбор и хранение компьютерной информации с персональными данными, полученной путем неправомерного доступа к средствам ее обработки, хранения либо иным незаконным путем, повлекут наказание для лица, совершившего преступление, от штрафа в размере до 300 тыс. руб. до лишения свободы на срок до 4 лет.

За те же деяния в отношении компьютерной информации, содержащей персональные данные несовершеннолетних лиц, специальные категории персональных данных и биометрические персональные данные, может быть назначено наказание от штрафа до 700 тыс. руб. до лишения свободы на срок до 5 лет.

При совершении указанных преступлений из корыстной заинтересованности, с причинением крупного ущерба, группой лиц по предварительному сговору, с использованием своего служебного положения наказание составит от штрафа до 1 млн руб. до лишения свободы на срок до 6 лет.

Также предусмотрена уголовная ответственность за подобные преступления, сопряженные с трансграничной передачей компьютерной информации, содержащей персональные данные, и трансграничным перемещением носителей информации с такими данными, а также за их совершение с тяжкими последствиями либо организованной группой.

Одновременно уголовно преследуется создание и обеспечение функционирования информационного ресурса, в том числе в сети «Интернет», заведомо предназначенного для незаконных хранения, передачи, распространения, предоставления, доступа к полученной незаконным путем компьютерной информации, содержащей персональные данные. Подобные действия повлекут наказание от штрафа до 700 тыс. руб. до лишения свободы на срок до 5 лет.

К уголовной ответственности за незаконные действия с персональными данными может быть привлечено любое физическое лицо.

12. **Прокурор разъясняет: введена уголовная ответственность за пропаганду в информационно-телекоммуникационных сетях наркотических средств, психотропных веществ, их аналогов, веществ, используемых при производстве, изготовлении и переработке наркотических сред**

С 01 сентября 2025 года действует Федеральный закон от 08.08.2024 № 226-ФЗ «О внесении изменений в Уголовный кодекс Российской Федерации и статьи 31 и 151 Уголовно-процессуального кодекса Российской Федерации», которым Уголовный кодекс Российской Федерации дополнен статьей 230.3.

Ею установлена уголовная ответственность за пропаганду наркотических средств, психотропных веществ, их аналогов или прекурсоров, растений, содержащих наркотические средства или психотропные вещества либо их прекурсоры, в информационно-телекоммуникационных сетях, включая сеть «Интернет», совершенную лицом после его привлечения к административной ответственности за аналогичное деяние два раза в течение одного года либо имеющим судимость за совершение преступления, предусмотренного настоящей статьей.

В соответствии с Федеральным законом от 08.01.1998 № 3-ФЗ «О наркотических средствах и психотропных веществах» прекурсоры наркотических средств и психотропных веществ – это вещества, часто используемые при производстве, изготовлении, переработке наркотических средств и психотропных веществ, включенные в Перечень наркотических средств, психотропных веществ и их прекурсоров, подлежащих контролю в Российской Федерации, в соответствии с действующим законодательством и международными договорами Российской Федерации, в том числе Конвенцией Организации Объединенных Наций о борьбе против незаконного оборота наркотических средств и психотропных веществ 1988 года.

Административная ответственность за пропаганду наркотических средств, психотропных веществ или их прекурсоров, растений, содержащих наркотические средства, психотропные вещества или их прекурсоры, их частей, содержащих наркотические средства, психотропные вещества или их прекурсоры, либо новых потенциально опасных психоактивных веществ с использованием информационно-телекоммуникационной сети «Интернет» установлена частью 1.1 статьи 6.13 Кодекса об административных правонарушениях Российской Федерации.

Пропагандой является размещение в информационно-телекоммуникационной сети «Интернет», в частности, на видеохостингах, страницах социальных сетей, сведений о способах, методах разработки, изготовления и использования наркотических средств, психотропных веществ, их прекурсоров, местах их приобретения, способах и местах культивирования наркосодержащих растений, а также совершение иных действий в целях побуждения интереса у зрителя (читателя) к наркотическим средствам, психотропным веществам и их прекурсорам, способам их употребления, формирования представления о совершении подобных действий для достижения состояния наркотического опьянения как допустимого и желательного.

Например, запрещено законом и является наказуемым размещение в свободном публичном доступе фотографий, изображений, аудио- и видеофайлов, в которых дается положительная оценка наркотикам и допустимости их употребления, указываются способы употребления наркотических средств, демонстрируются наркотические средства, способы их выращивания, содержатся инструкции по незаконному обороту наркотиков и распространению наркотических средств и психотропных веществ.

Преступления, предусмотренные статьей 230.3 Уголовного кодекса Российской Федерации, будут расследоваться следователями органов внутренних дел Российской Федерации.

За их совершение виновным лицам может быть назначено наказание от штрафа в размере от ста тысяч до трехсот тысяч рублей до лишения свободы на срок до двух лет с лишением права занимать определенные должности или заниматься определенной деятельностью на тот же срок.

13. **Прокурор разъясняет: Подписан закон об уголовной ответственности для дропперов**

С 5 июля 2025 года вступили в силу изменения статьи 187 Уголовного кодекса Российской Федерации («Неправомерный оборот средств платежей»).Данные изменения направлены на борьбу с «дропперами» – лицами, которые за вознаграждение предоставляют свои банковские карты и счета для совершения незаконных финансовых операций.Согласно нововведениям статья 187 УК РФ дополнена новыми частями 3-6:Часть 3 предусматривает ответственность лица за передачу из корыстной заинтересованности предоставленных ему оператором по переводу денежных средств электронного средства платежа и (или) доступа к нему другому лицу для осуществления таким лицом неправомерных операций.

В части 4 речь идет об уголовной ответственности лица за осуществление из корыстной заинтересованности неправомерных операций с использованием электронного средства платежа, предоставленного ему оператором по переводу денежных средств, по указанию другого лица и (или) в интересах такого лица.При этом, лицо, являющееся клиентом оператора по переводу денежных средств, впервые совершившее преступление, предусмотренное вышеуказанными частями, освобождается от уголовной ответственности за его совершение, если активно способствовало его раскрытию и (или) расследованию и добровольно сообщило о лицах, совершивших другие преступления с использованием предоставленного ему оператором по переводу денежных средств электронного средства платежа.

К категории тяжких преступлений (лишение свободы до 6 лет) относятся 5 и 6 часть, которые устанавливают ответственность лица за приобретение либо передачу другому лицу из корыстной заинтересованности электронного средства платежа и (или) доступа к нему для осуществления неправомерных операций, совершенные лицом, не являющимся стороной договора об использовании этого электронного средства платежа, заключенного с оператором по переводу денежных средств, либо приобретение таким лицом электронного средства платежа и (или) доступа к нему для последующей их передачи другому лицу из корыстной заинтересованности и за осуществление неправомерной операции с использованием электронного средства платежа, совершенное лицом, не являющимся стороной договора об использовании этого электронного средства платежа, заключенного с оператором по переводу денежных средств, соответственно.

14. **Прокурор разъясняет: в целях противодействия спам-звонкам и телефонному мошенничеству с 1 сентября 2025 года установлен порядок регулирования массовых телефонных вызовов**

В целях принятия дополнительных мер по борьбе с кибермошенничеством с 1 сентября 2025 года вступили в силу положения статьи 44.1-1 Федерального закона от 07.07.2003 № 126-ФЗ «О связи», которыми предусмотрено право абонента отказаться от получения массовых телефонных звонков.

Такие вызовы теперь должны осуществляться при условии получения предварительного согласия абонента, выраженного его действиями, однозначно идентифицирующими этого абонента и позволяющими достоверно установить его волеизъявление на получение массовых вызовов. Если заказчик массовых вызовов (в случае массовых вызовов по его инициативе) или оператор связи (в случае массовых вызовов по его инициативе) не докажет, что согласие абонента было получено, то массовые вызовы признаются осуществленными без предварительного согласия.

Массовые вызовы по инициативе заказчика массовых вызовов должны производиться на основании договора, заключенного с оператором, абоненту которого предназначены массовые вызовы.

Указанные требования не распространяются на массовые вызовы по инициативе государственных органов и подведомственных им организаций, органов местного самоуправления и подведомственных им организаций, а также иных органов и организаций, перечень которых устанавливается Правительством Российской Федерации.

В свою очередь, абонент в соответствии с требованиями пунктов 222-226 постановления Правительства Российской Федерации от 30.12.2024 № 1994 «Об утверждении Правил оказания услуг телефонной связи и перечня организаций, имеющих право осуществлять подтверждение сведений об абоненте – физическом лице» лично или с использованием сети «Интернет», в том числе системы самообслуживания оператора связи, вправе направить оператору связи отказ от получения массовых вызовов.

Получив отказ гражданина от массовых телефонных вызовов, оператор связи обязан их прекратить на следующий за днем подачи заявления день.

15. **Прокурор разъясняет: с 30 сентября 2025 г. вводятся правила, приравнивающие предъявление персональных данных в мобильном приложении Единого портала государственных услуг, к оригиналу паспорта.**

Возможность предоставления гражданами России сведений, содержащихся в документах, удостоверяющих личность, с использованием информационных технологий была предусмотрена Указом Президента Российской Федерации от 18.09.2023 № 695.

Однако до сентября текущего года конкретные ситуации, в каких случаях это разрешается делать официально не были определены.

В развитие названного Указа Президента постановлением Правительства Российской Федерации от 19.09.2025 № 1443 приняты Правила применения мобильного приложения федеральной государственной информационной системы "Единый портал государственных и муниципальных услуг (функций)".

Данным нормативным документом уточняется, что мобильным приложением разрешается пользоваться гражданам, достигшим 14-летнего возраста и получившим паспорт Российской Федерации.

Предусматривается поэтапное введение возможности предъявления сведений, заменяющих официальные документы, через мобильное приложение Единого портала госуслуг. Всего таких этапов 6. На первом из них можно будет подтверждать возраст

покупателя алкогольной, табачной и никотиносодержащей продукции, безалкогольных энергетических напитков, кальянов и устройств для потребления никотинсодержащей продукции, пиротехнических изделий и сжиженного газа, а также при посещении музея и(или) зрелищного мероприятия, при приеме почтовых отправлений.

В дальнейшем удостоверять личность посредством мобильного приложения можно будет в банках, многофункциональных центрах предоставления государственных услуг, пунктах оказания услуг мобильной связи, при заселении в гостиницы и в других случаях.

В целях удостоверения личности через мобильное приложение необходимо предъявлять свою фотографию, а также генерируемый в автоматическом режиме двухмерный штриховой код (QR-код), который будет считываться специальным техническим устройством, в том числе с использованием технологии NFC.

Чтобы воспользоваться возможностью предъявления персональных данных, удостоверяющих личность, взамен паспорта необходимо пройти процедуру идентификации в многофункциональном центре предоставления государственных и муниципальных услуг с размещением сведений в единой биометрической системе. Гражданам, ранее разместившим свои биометрические персональные данные в государственной единой биометрической системе, в том числе при получении заграничного паспорта, осуществлять заново подтверждение личности не требуется.