Печатная продукция сделана по заказу
Правительства Москвы

# ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ МОСКВИЧА

# ВВЕДЕНИЕ

Цифровая экономика стремительно вытесняет старый уклад жизни и деятельности во всех сферах современного общества. Трансформируется частная жизнь и рабочие места, появляются новые профессии и инструменты коммуникаций. Благодаря цифровизации, за счет использования информационных технологий, повышается эффективность отраслей экономики, расширяются возможности совершения через компьютер различных операций, среди которых предоставление/получение услуг и выполнение транзакций.

Однако, помимо преимуществ, цифровая трансформация несет и определенные риски. Общее количество инцидентов в сфере информационной безопасности в 2020 году выросло на 51% по сравнению с 2019 годом.

**В ДОКТРИНЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ РОССИЙСКОЙ ФЕДЕРАЦИИ (ОТ 5 ДЕКАБРЯ 2016 Г.) ПОД ТЕРМИНОМ ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ ПОНИМАЕТСЯ СОСТОЯНИЕ ЗАЩИЩЕННОСТИ НАЦИОНАЛЬНЫХ ИНТЕРЕСОВ В ИНФОРМАЦИОННОЙ СФЕРЕ, ОПРЕДЕЛЯЕМЫХ СОВОКУПНОСТЬЮ СБАЛАНСИРОВАННЫХ ИНТЕРЕСОВ ЛИЧНОСТИ, ОБЩЕСТВА И ГОСУДАРСТВА.**

Искажение или фальсификация, уничтожение или разглашение определенной части информации, равно как и дезорганизация процессов ее обработки и передачи, наносят серьезный материальный и моральный урон. Таким образом, крайне остро встает вопрос обеспечения информационной безопасности как различных госструктур, так и персональных данных и коммерческих организаций.

Поэтому сегодня люди серьезно заинтересованы в том, чтобы определенная часть информации, касающаяся их деятельности, конфиденциальные коммерческие и персональная данные были бы, с одной стороны, постоянно легко доступны, но в то же время – надежно защищены от неправомерного использования.

Под информацией в этой брошюре мы будем понимать сведения, являющиеся объектом сбора, хранения, обработки, непосредственного использования и передачи в информационных системах. Соответственно, **ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ** будем считать **СОСТОЯНИЕ ЗАЩИЩЕННОСТИ ИНФОРМАЦИИ** от случайных или преднамеренных воздействий естественного или искусственного характера (информационных угроз, угроз информационной безопасности), при котором исключается возможность просмотра, изменения или уничтожения информации лицами, не имеющими на это права, а также утечки информации за счет побочных излучений и наводок, специальных устройств перехвата (уничтожения) при

передаче между объектами вычислительной техники. Также к информационной безопасности относится защита информации от непреднамеренного уничтожения (технические сбои).

**ВАЖНО ОТМЕТИТЬ, ЧТО ЗАЩИТА ИНФОРМАЦИИ – ЭТО ПРОЦЕСС, КОТОРЫЙ ДОЛЖЕН ВЫПОЛНЯТЬСЯ НЕПРЕРЫВНО НА ВСЕМ ПРОТЯЖЕНИИ ЖИЗНЕННОГО ЦИКЛА ИНФОРМАЦИОННОЙ СИСТЕМЫ.**

**Целью защиты информации** является сведение к минимуму потерь в управлении, вызванных нарушением целостности данных, их конфиденциальности или недоступности информации для потребителей.

При этом отрадно, что уровень грамотности россиян в вопросах информационной безопасности неуклонно растет.

## СОГЛАСНО ИССЛЕДОВАНИЯМ КОМПАНИИ ESET, ЧИСЛО РОССИЯН, КОТОРЫЕ ИГНОРИРУЮТ КИБЕРУГРОЗЫ, ЗА ДВА ГОДА УМЕНЬШИЛОСЬ

**с 23% в 2019 году до 12% в 2021 году**

Так, 46% россиян чаще используют для защиты сложные и разные пароли, 36% доверяют безопасность антивирусам, 28% используют двухфакторную аутентификацию. Еще 24% опрошенных рассказали, что избегают общественных точек Wi-Fi, 20% отказываются предоставлять сайтам личные данные, 13% постоянно создают резервные копии систем.

При этом 53% респондентов, которые используют сложные пароли, рассказали, что меняют их как минимум два раза в год.

Исследователи также отмечают, что 60% тех, кто пользуется антивирусами, предпочитают бесплатное ПО, 28% готовы за такие программы платить. Остальные опрошенные признались, что скачивают антивирусное ПО на пиратских сайтах.

# 1. ЗАЩИТА ПЕРСОНАЛЬНЫХ ДАННЫХ

## 1.1. ОПРЕДЕЛЕНИЕ ПЕРСОНАЛЬНЫХ ДАННЫХ

**ПЕРСОНАЛЬНЫЕ ДАННЫЕ** — это любая информация, прямо или косвенно относящаяся к физическому лицу и позволяющая его определить (ст. 3 ФЗ «О персональных данных», от 27.07.2006 № 152-ФЗ).

**К ПЕРСОНАЛЬНЫМ ДАННЫМ, СОГЛАСНО ФЗ № 152, ОТНОСЯТ:**

- **фамилия, имя, отчество;**
- **место, дата рождения;**
- **место постоянной или временной регистрации;**
- **фотография или видеозапись человека, позволяющие идентифицировать человека;**
- **сведения о детях, родственниках, семейном положении;**
- **сведения о заработной плате;**
- **оценка навыков, личностных качеств;**
- **индивидуальные личные данные (раса, национальность, политические или религиозные взгляды, философские убеждения; состояние здоровья);**
- **информация о судимостях, или их отсутствии;**
- **номер телефона, адрес электронной почты, иные идентификаторы в соц. сетях или мессенджерах;**
- **паспортные данные, СНИЛС, ИНН;**
- **биометрические данные.**

Стоит учесть, что некоторые из этих данных сами по себе, без связки с другими данными, персональными могут не являться. Если номер телефона сам по себе не относится к персональным данным, то в базе оператора, с указанием ФИО владельца — уже относится.

**Классификация персональных данных:**

| | |
|---|---|
| Общедоступные | На доступ к данным дано согласие субъекта персональных данных. Это не те данные, которые можно найти в общем доступе в интернете. |
| Специальные | Информация о расе, национальности и религии; политических и философских взглядах, здоровье, подробностях личной жизни, судимостях. |
| Биометрические | Информация о физиологических и биологических особенностях человека. Это отпечатки пальцев, генетическая информация, рисунок радужной оболочки глаз, образцы голоса, фотографии (здесь важна привязка к личности: например, отпечаток пальца, используемый для идентификации сотрудника при входе в офис). |
| Иные данные | Электронная почта или геолокация, информация о принадлежности к определенной социальной группе, стаж работы и пр. |

**СУБЪЕКТОМ ПЕРСОНАЛЬНЫХ ДАННЫХ** выступает физическое лицо, чьи данные обрабатывают. К примеру, собирают и хранят. А **ОПЕРАТОР ПЕРСОНАЛЬНЫХ ДАННЫХ** — юридические лица, государственные организации или ведомства. Они данные собирают, обрабатывают, хранят, передают и уничтожают.

## 1.2. ОТВЕТСТВЕННОСТЬ ФИЗИЧЕСКИХ И ЮРИДИЧЕСКИХ ЛИЦ ЗА РАСПРОСТРАНЕНИЕ ПЕРСОНАЛЬНЫХ ДАННЫХ ГРАЖДАН

**Виды ответственности за нарушение закона о персональных данных:**

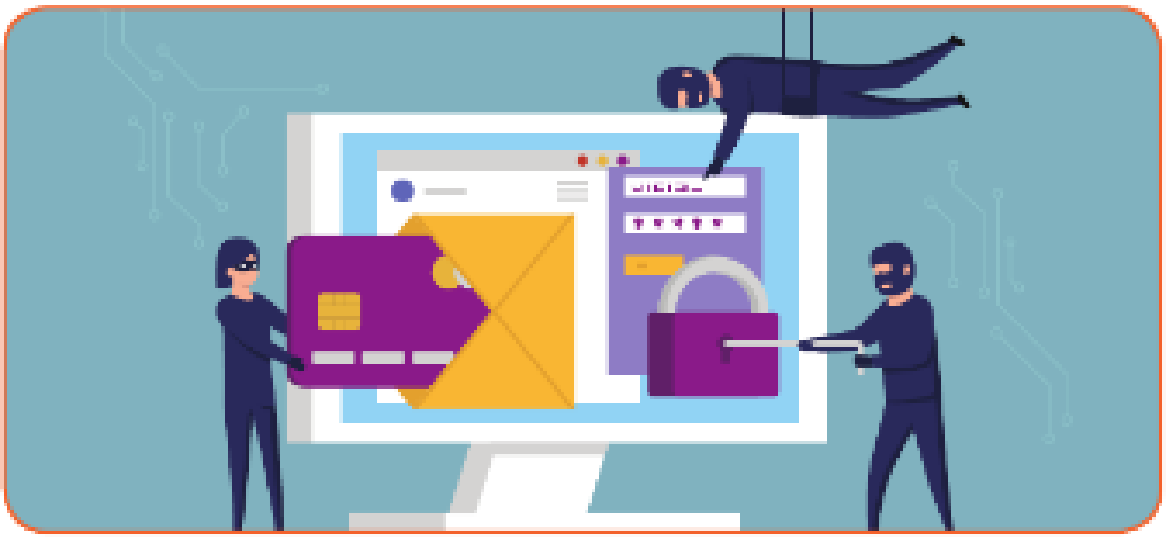
| Вид ответственности | Нарушение | Санкция | Норма |
|---|---|---|---|
| | Неправомерный отказ в предоставлении гражданину и (или) организации информации, предоставление которой предусмотрено законом, несвоевременное ее предоставление либо предоставление заведомо недостоверной информации | Административный штраф на должностных лиц в размере от 5 тыс. до 10 тыс. руб. | Статья 5.39 КоАП РФ |

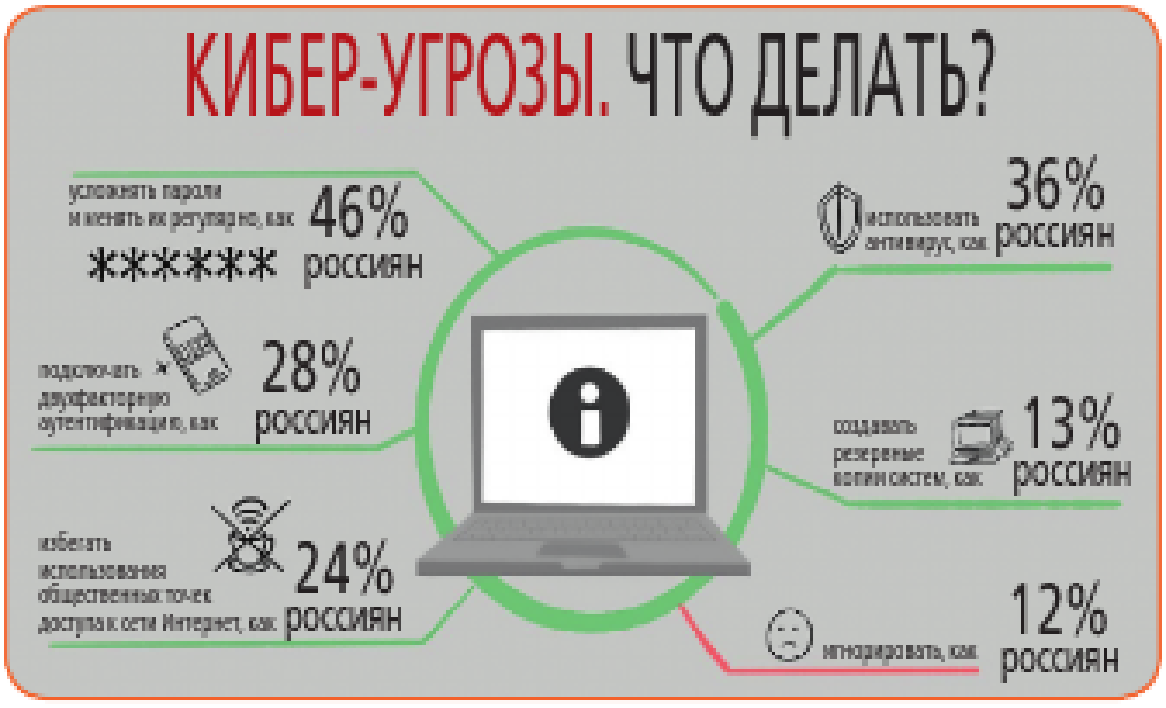
| | | | |
|---|---|---|---|
| Административная | Обработка персональных данных в случаях, не предусмотренных законом, либо обработка, несовместимая с целями сбора персональных данных | Предупреждение или административный штраф:<br>• на граждан – от 1 тыс. до 3 тыс. руб.;<br>• на должностных лиц – от 5 тыс. до 10 тыс. руб.;<br>• на юридических лиц – от 30 тыс. до 50 тыс. руб. | Часть 1 ст. 13.11 КоАП РФ |
| | Обработка персональных данных без письменного согласия субъекта, когда это необходимо, либо обработка данных с нарушением требований к составу сведений, включаемых в такое согласие | Административный штраф:<br>• на граждан – от 3 тыс. до 5 тыс. руб.;<br>• на должностных лиц – от 10 тыс. до 20 тыс. руб.;<br>• на юридических лиц – от 15 тыс. до 75 тыс. руб. | Часть 2 ст. 13.11 КоАП РФ |
| | Невыполнение оператором обязанности по опубликованию или обеспечению иным образом неограниченного доступа к политике обработки персональных данных | Предупреждение или административный штраф:<br>• на граждан – от 700 до 1 тыс. руб.;<br>• на должностных лиц – от 3 тыс. до 6 тыс. руб.;<br>• на индивидуальных предпринимателей – от 5 тыс. до 10 тыс. руб.;<br>• на юридических лиц – от 15 тыс. до 30 тыс. руб. | Часть 3 ст. 13.11 КоАП РФ |
| | Невыполнение оператором обязанности по предоставлению субъекту персональных данных информации, касающейся обработки его персональных данных | Предупреждение или административный штраф:<br>• на граждан – от 1 тыс. до 2 тыс. руб.;<br>• на должностных лиц – от 4 тыс. до 6 тыс. руб.;<br>• на индивидуальных предпринимателей – от 10 тыс. до 15 тыс. руб.;<br>• на юридических лиц – от 20 тыс. до 40 тыс. руб. | Часть 4 ст. 13.11 КоАП РФ |
| | Невыполнение оператором в установленные сроки требования субъекта персональных данных или его представителя либо Роскомнадзора об уточнении персональных данных, их блокировании или уничтожении (если данные являются неполными, устаревшими, неточными, незаконно полученными или не являются необходимыми для заявленной цели обработки) | Предупреждение или административный штраф:<br>• на граждан – от 1 тыс. до 2 тыс. руб.;<br>• на должностных лиц – от 4 тыс. до 10 тыс. руб.;<br>• на индивидуальных предпринимателей – от 10 тыс. до 20 тыс. руб.;<br>• на юридических лиц – от 25 тыс. до 45 тыс. руб. | Часть 5 ст. 13.11 КоАП РФ |

| | | | |
|---|---|---|---|
| Административная | Невыполнение оператором при обработке персональных данных без использования средств автоматизации обязанности по соблюдению условий, обеспечивающих их сохранность и исключающих несанкционированный к ним доступ, если это повлекло неправомерный или случайный доступ к данным, их уничтожение, изменение, блокирование, копирование, предоставление, распространение либо иные неправомерные действия в отношении них | Административный штраф:<br>• на граждан – от 700 до 2 тыс. руб.;<br>• на должностных лиц – от 4 тыс. до 10 тыс. руб.;<br>• на индивидуальных предпринимателей – от 10 тыс. до 20 тыс. руб.;<br>• на юридических лиц – от 25 тыс. до 50 тыс. руб. | Часть 6 ст. 13.11 КоАП РФ |
| | Невыполнение оператором, являющимся государственным или муниципальным органом, обязанности по обезличиванию персональных данных либо несоблюдение установленных для этого требований или методов | Предупреждение или наложение административного штрафа на должностных лиц в размере от 3 тыс. до 6 тыс. руб. | Часть 7 ст. 13.11 КоАП РФ |
| | Непредставление или несвоевременное представление в государственный или иной уполномоченный орган сведений, представление которых предусмотрено законом либо предоставление таких сведений в неполном объеме или в искаженном виде | Административный штраф:<br>• на граждан – от 100 до 300 руб.;<br>• на должностных лиц – от 300 до 500 руб.;<br>• на юридических лиц – от 3 тыс. до 5 тыс. руб. | Статья 19.7 КоАП РФ |
| Уголовная | Незаконное собирание или распространение сведений о частной жизни лица, составляющих его личную или семейную тайну, без его согласия либо распространение этих сведений в публичном выступлении, публично демонстрирующемся произведении или СМИ | Штраф до 200 тыс. руб., либо обязательные работы на срок до 360 часов, либо исправительные работы на срок до одного года, либо принудительные работы на срок до двух лет (с лишением права занимать определенные должности на срок до трех лет или без такового), либо арест на срок до четырех месяцев, либо лишение свободы на срок до двух лет (с лишением права занимать определенные должности на срок до трех лет) | Статья 137 Уголовного кодекса |

| | | | |
|---|---|---|---|
| Угрозы | То же деяние, совершенное с использованием служебного положения | Штраф от 100 тыс. до 300 тыс. руб., либо лишение права занимать определенные должности на срок от двух до пяти лет, либо принудительные работы на срок до четырех лет (с лишением права занимать определенные должности на срок до пяти лет или без такового), либо арест на срок до шести месяцев, либо лишение свободы на срок до четырех лет (с лишением права занимать определенные должности на срок до пяти лет) | Статья 137 Уголовного кодекса |
| | Незаконное публичное распространение информации, указывающей на личность лица, не достигшего 16 лет, по уголовному делу, либо информации, содержащей описание полученных им в связи с преступлением физических или нравственных страданий | Штраф от 100 тыс. до 300 тыс. руб., либо лишение права занимать определенные должности на срок от трех до пяти лет, либо принудительные работы на срок до пяти лет (с лишением права занимать определенные должности на срок до шести лет или без такового), либо арест на срок до шести месяцев, либо лишение свободы на срок до пяти лет (с лишением права занимать определенные должности на срок до шести лет) | Статья 137 Уголовного кодекса |
| | Неправомерный отказ должностного лица в предоставлении документов и материалов, непосредственно затрагивающих права и свободы гражданина, либо предоставление ему неполной или заведомо ложной информации, если это причинило вред правам и законным интересам граждан | Штраф до 200 тыс. руб., либо лишение права занимать определенные должности на срок от двух до пяти лет | Статья 140 УК РФ |
| | Неправомерный доступ к охраняемой законом компьютерной информации, если это повлекло ее уничтожение, блокирование, модификацию либо копирование | Штраф до 200 тыс. руб., либо исправительные работы на срок до одного года, либо ограничение свободы на срок до двух лет, либо принудительные работы на срок до двух лет, либо лишение свободы на тот же срок | Статья 272 УК РФ |

| | | | |
|---|---|---|---|
| Гражданско-правовая | Причинение лицу убытков в результате нарушения правил обработки его персональных данных. Под убытками при этом понимаются:<br>• расходы, которые лицо произвело или должно будет произвести для восстановления нарушенного права;<br>• утрата или повреждение его имущества;<br>• неполученные доходы, которые лицо получило бы, не будь его право нарушено. | Возмещение убытков | Статья 15 Гражданского кодекса |
| | Причинение гражданину морального вреда (нравственных страданий) вследствие нарушения правил обработки персональных данных | Компенсация морального вреда (независимо от возмещения имущественного вреда и понесенных субъектом убытков) | Статья 24 закона о персональных данных, ст. 151 ГК РФ |
| Дисциплинарная | Разглашение одним работником персональных данных другого, если они стали известны ему в связи с исполнением трудовых обязанностей | Увольнение | Подпункт «в» п. 6 ч. 1 ст. 81 Трудового кодекса |
| | Иные нарушения в области персональных данных при их обработке | Замечание или выговор | Статья 90, ст. 192 ТК РФ |






Наказание за нарушения закона неизбежно. Но и граждане должны быть внимательны при использовании своих персональных данных.

Так, важно помнить, что ваши персональные данные содержатся в паспорте. Тот, кому вы их предоставляете, становится оператором персональных данных и должен соблюдать требования закона: использовать данные для конкретной цели, хранить в защищенном месте и не допускать утечки. Операторы сами должны запрашивать ваше согласие на обработку персональной информации.

Насторожитесь, когда копию паспорта делают без вашего согласия. Если паспортные данные окажутся у мошенников, вас могут ждать неприятные последствия.

### КАК ОБЕЗОПАСИТЬ СЕБЯ

**ВО-ПЕРВЫХ, предоставляйте паспортные данные только проверенным людям и компаниям, когда паспорт действительно необходим. Например, без паспорта не обойтись, если оформляете договор аренды квартиры или получаете кредит в банке. Если вы покупаете товар не в рассрочку, а в магазине у вас просят ксерокопию паспорта, лучше отказать.**

**ВО-ВТОРЫХ, не давайте делать копии всех страниц паспорта. Первой страницы и страницы с пропиской обычно достаточно.**

**НАКОНЕЦ, по возможности, напишите на копии паспорта, для какой фирмы она сделана. Либо замажьте или зачеркните какие-нибудь данные, например вашу подпись.**

# Преступления с использованием персональных данных

Персональные данные слишком привлекательны для мошенников. Эти примеры – малая часть того, что происходит с незаконным оборотом данных россиян.

## I. АФЕРЫ С ИМУЩЕСТВЕННЫМИ ВЫЧЕТАМИ.

*Мошенники отправляли в налоговую инспекцию поддельные документы на покупку квартир, справки 2-НДФЛ и заявления на налоговый вычет. Одновременно с этим открывали счет в банке. Налоговая инспекция проверяла документы и по-настоящему переводила НДФЛ на счета мошенников.*

*Пострадавшие узнавали об этом случайно, при проверке личного кабинета на сайте ФНС. Никаких уведомлений из банка или налоговой инспекции им не приходило.*

*Оказывается, все они «получили» имущественный вычет при покупке квартир в одном и том же доме и вернули НДФЛ.*

## II. ПОЛУЧЕНИЕ КРЕДИТОВ ПО ЧУЖИМ ПЕРСОНАЛЬНЫМ ДАННЫМ.

*Гражданин и трое его сообщников с целью хищения денежных средств банков зарегистрировал два юридических лица, которые якобы оказывали посреднические услуги при организации туристических поездок. Затем между банком и одной из фирм был заключен договор о сотрудничестве, по условиям которого организация имела право оформлять от имени банка документы на выдачу кредитов клиентам на оплату туристических услуг.*

*Посредством сети «Интернет», получив доступ к персональным данным ряда граждан РФ, фигурант уголовного дела составил договоры на получение потребительских кредитов на оплату туров. После этого денежные средства в сумме более 900 тыс. рублей были перечислены на счет фирмы, подконтрольной злоумышленнику.*

*По аналогичной схеме мужчина при помощи троих знакомых, похитил денежные средства еще двух кредитных организаций. Общая сумма причиненного трем банкам ущерба превысила 2 млн 750 тыс. рублей.*

### III. ХИЩЕНИЕ СРЕДСТВ С БАНКОВСКИХ СЧЕТОВ ПО ЧУЖИМ ПЕРСОНАЛЬНЫМ ДАННЫМ.

*За год жители нескольких регионов в составе организованной группы совершили хищения денежных средств со счетов клиентов одного из банков.* ***Они незаконно получали доступ к персональным данным клиентов финансового учреждения, по счетам которых длительное время не было движения, подделывали паспорта, в которые вклеивали свои фотографии,*** *оформляли у нотариуса доверенность на распоряжение счетом на одного из участников группы, после чего совершали финансовые операции в банке.*
*Таким способом ими похищено более 18 млн рублей.*

**Оформлением кредита и похищением средств с банковских счетов далеко не ограничивается изобретательность мошенников.**

**ВЫ МОЖЕТЕ СТАТЬ УЧРЕДИТЕЛЕМ ФИРМЫ-ОДНОДНЕВКИ.** Паспортных данных достаточно, чтобы зарегистрировать на ваше имя ООО или открыть ИП. Фирмы-однодневки используются для отмывания денег и организации преднамеренного или фиктивного банкротства, ответственность за которые несет в том числе учредитель.

**ВАШИ ДАННЫЕ МОГУТ ИСПОЛЬЗОВАТЬ ДЛЯ НЕЗАКОННЫХ ФИНАНСОВЫХ ОПЕРАЦИЙ.** Чтобы снять ограничения в некоторых платежных системах, достаточно предъявить фото паспорта. В этом случае вы рискуете стать участником дел о незаконной торговле или финансировании терроризма.

## 2. НЕЯСНАЯ (ТУМАННАЯ) ФОРМУЛИРОВКА ДОГОВОРА

Увы, мы всегда должны быть готовы к тому, что в договоре на приобретение товаров или услуг может быть некоторая неясность, двусмысленность формулировок или появится пресловутый мелкий шрифт, который трудно разобрать даже с сильной лупой…

При этом надо понимать, что умышленное использование стороной, разрабатывающей текст контракта, двусмысленных формулировок может использоваться для того, чтобы заказчик, покупатель, контрагент истолковал неоднозначное условие договора, как выгодное для себя, и подписал его.

Люди вносят темноту и двусмысленность в договоры для того, чтобы обеспечить себе предлог для уклонения от исполнения обязательств. И это мошенничество чистой воды.

## I. ДОГОВОР О КРЕДИТОВАНИИ МЕЛКИМ ШРИФТОМ.

*Прокуратура провела проверку по обращению 70-летней местной жительницы, являющейся инвалидом 1 группы по состоянию здоровья, о нарушении ее прав потребителя.*

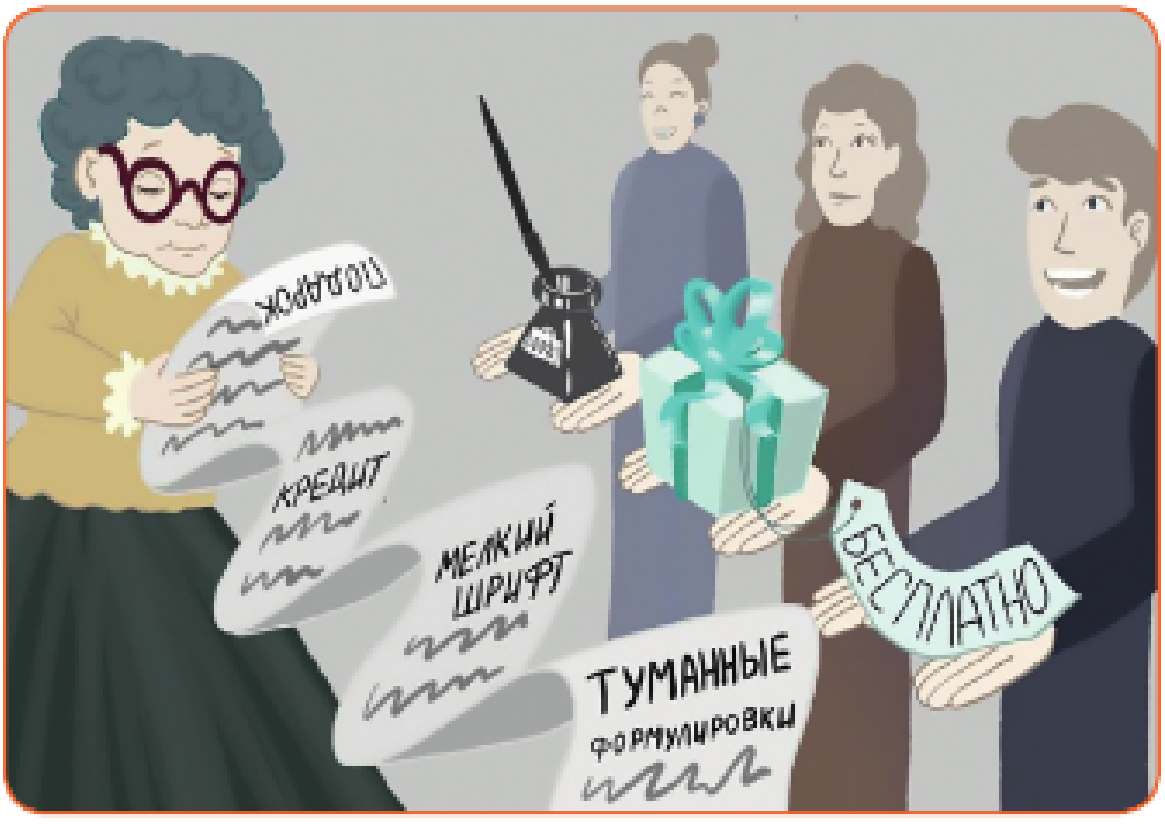
*Установлено, что заявительницу, имеющую инвалидность, представители фирмы ООО «ЭкоЛайфСтар» пригласили на бесплатную презентацию посуды. Во время торжественного мероприятия было сообщено, что женщина стала обладателем подарка.*

*За оформление так называемого подарка, состоящего из набора посуды и ножей, инвалид была вынуждена заплатить 4 тыс. рублей, а также расписаться в документах о его получении, выполненных мелким шрифтом и нечитаемым для нее.*

*Позже к заявительнице стали поступать требования банка о погашении имеющейся перед ним задолженности по кредиту за посуду. Тогда женщина узнала, что приобрела товары в кредит, о чем подписала договоры купли-продажи и потребительского кредитования, а не получила его в подарок.*

*Сумма покупки с учетом необходимости возврата заемных денежных средств и процентов по нему составила около 125 тыс. рублей, что для нее как инвалида было финансово невозможным.*

*За защитой своих прав она обратилась в прокуратуру. Прокурорская проверка подтвердила обоснованность доводов о нарушении прав, поскольку при заключении договора купли-продажи пенсионерке не была*



*предоставлена полная и достоверная информация о товаре, его производителе, основных свойствах и характеристиках. По иску прокурора в пользу пенсионерки взыскана стоимость посуды, компенсация морального вреда и штраф за несоблюдение в добровольном порядке удовлетворения требований потребителя на общую сумму свыше 130 тыс. рублей.*

## II. ТУМАННАЯ ФОРМУЛИРОВКА СУТИ УСЛУГ.

*Прокуратура Юго-Восточного административного округа г. Москвы утвердила обвинительное заключение по уголовному делу в отношении 29-летнего жителя столицы. Он обвиняется в совершении пяти преступлений, предусмотренных ч. 4 ст. 159 УК РФ (мошенничество, совершенное с причинением значительного ущерба гражданам организованной группой).*
*По версии следствия, злоумышленник совместно с другими участниками группы под видом осуществления финансово-хозяйственной деятельности заключал с гражданами договоры на оказание юридических услуг.*
*При этом сообщники действовали от имени подконтрольного им ООО «Московский Центр Правовой Поддержки» и использовали регистрационные, учредительные и финансовые документы организации.*
*Однако обвиняемые* ***не намеревались и не имели возможности исполнить взятые на себя обязательства*** *по заключенным договорам, а денежными средствами распоряжались по собственному усмотрению.*
*Всего в период с марта по июнь 2020 года им удалось обмануть 5 граждан, которым причинен ущерб в размере более 320 тыс. рублей.*

## III. ДОГОВОР, СОДЕРЖАЩИЙ ЗАВЕДОМО НЕВЫГОДНЫЕ УСЛОВИЯ.

*В четырех автосалонах г. Санкт-Петербурга участники преступного сообщества продавали гражданам новые и подержанные автомобили. Если у покупателей не хватало денег, злоумышленники вводили потерпевших в заблуждение относительно низкой процентной ставки при оформлении кредита в автосалоне.*
*Граждане, не подозревающие об обмане, заключали договоры о кредитовании, содержащие заведомо невыгодные условия о стоимости транспортных средств, которая была необоснованно завышена.*
*После одобрения заявок по кредитам участники преступного сообщества присваивали разницу между реальной стоимостью транспортных средств и размером фактически выданных банком денежных средств. За период времени с апреля 2014 г. по март 2018 г. злоумышленники завладели денежными средствами 262 потерпевших, причинив им ущерб на общую сумму более 69 млн рублей.*

# 3. КЛЕВЕТА

В России, как и в большинстве стран мира, с августа 2012 года действует уголовная ответственность за клевету. До этого клевета предполагала лишь гражданскую ответственность.

**В СООТВЕТСТВИИ СО СТАТЬЕЙ 128.1 УГОЛОВНОГО КОДЕКСА РФ, КЛЕВЕТА – НЕ ПРОСТО ПОВЕДЕНИЕ, НЕ КРАСЯЩЕЕ ЧЕЛОВЕКА, ЭТО РАСПРОСТРАНЕНИЕ ЗАВЕДОМО ЛОЖНЫХ СВЕДЕНИЙ, ПОРОЧАЩИХ ЧЕСТЬ И ДОСТОИНСТВО ДРУГОГО ЛИЦА ИЛИ ПОДРЫВАЮЩИХ ЕГО РЕПУТАЦИЮ, ЗА ЧТО УСТАНОВЛЕНА УГОЛОВНАЯ ОТВЕТСТВЕННОСТЬ.**

Уголовное дело о клевете законом отнесено к делам частного обвинения, которые возбуждаются мировым судом по заявлению потерпевшего.

Лицо, подавшее заявление в суд, является частным обвинителем и самостоятельно представляет обвинение. Им может быть потерпевший или его законный представитель, если речь идет о несовершеннолетнем, недееспособном или ограниченно дееспособном лице, а также представитель потерпевшего по доверенности.

Давность привлечения к уголовной ответственности за клевету составляет 2 года с момента совершения преступления.

Для наступления ответственности за клевету ложные сведения должны быть конкретными, т. е. содержать факты, поддающиеся проверке, например, о заражении лица ВИЧ-инфекцией или о состоянии на учете в психоневрологическом диспансере и т. п.

**УГОЛОВНАЯ ОТВЕТСТВЕННОСТЬ ЗА КЛЕВЕТУ** наступает в том случае, если виновный заведомо осознавал ложность сообщаемых им сведений, порочащих честь и достоинство других лиц или подрывающих их репутацию, и желал их распространить.

## I. НЕПРАВОМЕРНЫЕ ДЕЙСТВИЯ (КЛЕВЕТА) КОЛЛЕКТОРОВ.

*В июле 2015 года гражданка заключила договор с компанией ООО «Домашние деньги», зарегистрированной в г. Москва, на получение займа в размере 15 тыс. рублей под 0,7% в день. Денежные средства ей были необходимы для приобретения ребенку школьной одежды. В связи с финансовыми затруднениями у женщины перед микрофинансовой организацией образовалась задолженность.*

*В марте текущего года мать должницы в почтовом ящике обнаружила листок с фотографией дочери. К ней прилагалась записка, содержащая*

*угрозы распространения информации о якобы имеющегося у должницы ВИЧ-инфекции, в случае, если задолженность не будет погашена.*
*Согласно данным центра по профилактике и борьбе со СПИДом и инфекционными заболеваниями, женщина на учете не состоит.*
*В связи с наличием в действиях коллекторов признаков состава преступления, предусмотренного ч. 4 ст. 128.1 УК РФ (клевета), прокуратура направила материалы проверки в управление МВД России. По итогам их рассмотрения возбуждено уголовное дело.*

## II. РАСПРОСТРАНЕНИЕ НЕДОСТОВЕРНЫХ СВЕДЕНИЙ О МАССОВОМ ЗАБОЛЕВАНИИ КОРОНАВИРУСНОЙ ИНФЕКЦИЕЙ.

*Уссурийская городская прокуратура Приморского края утвердила обвинительное заключение по уголовному делу в отношении местного жителя, 1992 г.р. Он обвиняется в совершении преступления, предусмотренного ч. 4 ст. 128.1 УК РФ (клевета о том, что лицо страдает заболеванием, представляющим опасность для окружающих).*
*По версии следствия, злоумышленник является слесарем по ремонту подвижного состава локомотиворемонтного завода в г. Уссурийске. Имея доступ в помещения завода, он оделся в похожий на противочумный защитный костюм и маску и записал себя на видео, которое распространил в группе одного из мессенджеров. На видеозаписи мужчина сообщил о массовом заболевании сотрудников предприятия, включая руководство, новой коронавирусной инфекцией. Видеозапись была распространена в социальных сетях и получила широкий резонанс.*
*Вину в совершенном преступлении мужчина признал частично. Уголовное дело направлено в суд.*

# 4. ПРИЗЫВ К ЭКСТРЕМИЗМУ

В Российской Федерации экстремистская деятельность находится под запретом, а соблюдение этого запрета – под строгим контролем. Подобная строгость обусловлена в том числе многонациональным и многоконфессиональным составом нашего государства, что требует пристального внимания и необходимости быстрого реагирования на попытки отдельных лиц и организаций посеять рознь между народами и различными группами населения нашей страны.

Цифровой мир таков, что каждый наш шаг в интернете, социальных сетях или мессенджерах оставляет свой след. Поэтому нужно осознавать ответственность за свои действия и понимать, что любой перепост, необдуманный комментарий или, казалось бы, смешная картинка в интернете могут привести к риску уголовного преследования. Чтобы свести его к минимуму, нужно знать законодательство «О противодействии экстремистской деятельности».

**Экстремистская деятельность (экстремизм) это:**

— насильственное изменение основ конституционного строя и нарушение целостности Российской Федерации;

— публичное оправдание терроризма и иная террористическая деятельность;

— возбуждение социальной, расовой, национальной или религиозной розни;

— пропаганда исключительности, превосходства либо неполноценности человека по признаку его социальной, расовой, национальной, религиозной или языковой принадлежности или отношения к религии;

— нарушение прав, свобод и законных интересов человека и гражданина в зависимости от его социальной, расовой, национальной, религиозной или языковой принадлежности или отношения к религии;

— воспрепятствование осуществлению гражданами их избирательных прав и права на участие в референдуме или нарушение тайны голосования, соединенные с насилием либо угрозой его применения;

— воспрепятствование законной деятельности государственных органов, органов местного самоуправления, избирательных комиссий, общественных и религиозных объединений или иных организаций, соединенное с насилием либо угрозой его применения;

— совершение преступлений по мотивам, указанным в пункте «е» части первой статьи 63 Уголовного кодекса Российской Федерации;

— пропаганда и публичное демонстрирование нацистской атрибутики или символики либо атрибутики или символики, сходных с нацистской атрибутикой или символикой до степени смешения, либо публичное демонстрирование атрибутики или символики экстремистских организаций;

— публичные призывы к осуществлению указанных деяний либо массовое распространение заведомо экстремистских материалов, а равно их изготовление или хранение в целях массового распространения;

— публичное заведомо ложное обвинение лица, замещающего государственную должность Российской Федерации или государственную должность субъекта Российской Федерации, в совершении им в период исполнения своих должностных обязанностей деяний, указанных в настоящей статье и являющихся преступлением;

— организация и подготовка указанных деяний, а также подстрекательство к их осуществлению;

— финансирование указанных деяний либо иное содействие в их организации, подготовке и осуществлении, в том числе путем предоставления учебной, полиграфической и материально-технической базы, телефонной и иных видов связи или оказания информационных услуг.

Ответственность за публичные призывы к осуществлению экстремистской деятельности устанавливает **статья 280 УК РФ**. Во-первых, данной статьей предусмотрен достаточно большой штраф – до трехсот тысяч рублей или в размере заработной платы осужденного за период до двух лет. Во-вторых, возможен также арест на срок от четырех до шести месяцев, либо лишение свободы на срок до трех лет.

**И СТОИТ УЧЕСТЬ, ЧТО ПРЕСТУПЛЕНИЕ СЧИТАЕТСЯ СОВЕРШЕННЫМ С МОМЕНТА ПУБЛИЧНОГО ПРОВОЗГЛАШЕНИЯ (РАСПРОСТРАНЕНИЯ) ХОТЯ БЫ ОДНОГО ОБРАЩЕНИЯ – НЕЗАВИСИМО ОТ ТОГО, УДАЛОСЬ ПОБУДИТЬ ДРУГИХ ГРАЖДАН К ОСУЩЕСТВЛЕНИЮ ЭКСТРЕМИСТСКОЙ ДЕЯТЕЛЬНОСТИ ИЛИ НЕТ.**

При наличии в вашем аккаунте/блоге или на вашем сайте «экстремистского материала» или даже материала, на него очень похожего, от вас могут потребовать его удалить. Обычно это делают прокуратура или Роскомнадзор РФ,

зачастую через администрацию сети или хостинг-провайдера. Если вы не согласны удалять материал, то можете обжаловать это требование в суде.

Но если вы его не удалили, то вне зависимости от обжалования, доступ пользователей из России к вашему сайту или блогу будет заблокирован.

**За совершение преступления, предусмотренного ст. 280 УК РФ, установлено максимальное наказание в виде лишения свободы на срок до четырех лет, а за совершение указанных деяний с использованием средств массовой информации либо информационно-телекоммуникационных сетей, в том числе сети «Интернет», – в виде лишения свободы на срок до пяти лет с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до трех лет.**

ТАК, РЕГИОНАЛЬНЫМИ ОРГАНАМИ ПРОКУРАТУРЫ НА САЙТЕ СЕРВИСА YOUTUBE ВЫЯВЛЕНО ВИДЕО ПОД НАЗВАНИЕМ «КОРОНАВИРУСА НЕТ И НЕ БУДЕТ!» ОТ 19.03.2020 г., *в котором говорится об отсутствии коронавирусной инфекции в России и мире, распространении заведомо ложной информации о данной инфекции лидерами США с целью дестабилизации мировой экономики. Аналогичные видеоролики были выявлены еще на ряде интернет-ресурсов.*

*В социальной сети «Инстаграм» установлена публикация «У медсестры из Кировской больницы не подтвердили коронавирус». В своем комментарии к указанной статье один из пользователей, отрицая факт существования новой коронавирусной инфекции, заявил о глобальном обмане и заговоре. Также, обращаясь к неопределенному кругу лиц, он призвал «восстать против власти» ради спасения.*

*По данному факту региональным Центром по противодействию экстремизму проводится проверка в связи с наличием в действиях неустановленного лица признаков преступления, предусмотренного в том числе ч. 2 ст. 280 УК РФ (публичные призывы к осуществлению экстремистской деятельности).*

## 5. РАСПРОСТРАНЕНИЕ ДЕЗИНФОРМАЦИИ

С развитием современных средств коммуникации дезинформация стала практически тотальной.

**ДЕЗИНФОРМАЦИЯ** – это распространение искаженных или заведомо ложных сведений для достижения пропагандистских, военных (введение противника в заблуждение) или других целей.

Дезинформацией называется сам процесс манипулирования информацией: введение кого-либо в заблуждение путем предоставления неполной информации, искажения контекста, искажения части информации.

**Основные способы дезинформации**

**Дозирование информации.** Сообщается только часть сведений, а остальные тщательно скрываются. Это приводит к тому, что картина реальности искажается в ту или иную сторону, либо вообще становится непонятной.

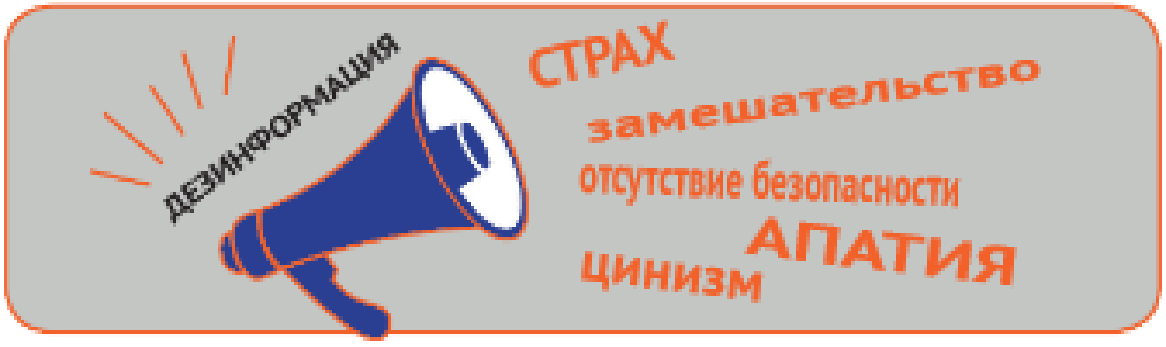
**Большая ложь.** Любимый прием министра пропаганды нацистской Германии Й. Геббельса. Он утверждал, что чем наглее и неправдоподобнее ложь, тем скорее в нее поверят, главное – подавать ее максимально серьезно.

**Смешивание истинных фактов со всевозможными предположениями,** допущениями, гипотезами, слухами. В результате становится невозможным отличить правду от вымысла.

**Затягивание времени** – под различными предлогами оттягивается обнародование действительно важных сведений до того момента, когда будет уже поздно что-то изменить.

**Возвратный удар.** Суть этого способа в том, что вымышленную (естественно, выгодную для источника) версию тех или иных событий через подставных лиц распространяют в СМИ, нейтральных по отношению к обеим конфликтующим сторонам. Пресса соперника повторяет эту версию, ибо она считается более «объективной», чем мнения прямых участников конфликта.

**Своевременная ложь.** Способ заключается в сообщении совершенно лживой, но чрезвычайно ожидаемой в данный момент («горячей») информации. Чем больше содержание сообщения отвечает настроениям объекта, тем эффективнее его результат. Потом обман раскрывается, но за это время острота ситуации спадает, либо определенный процесс принимает необратимый характер.




## 5.1. ФАЛЬШИВЫЕ НОВОСТИ.

Проблема распространения недостоверной информации – ложных сведений под видом достоверных – в Интернете обсуждается уже не первый год, в том числе на международном уровне. Законодательство разных стран дополняется положениями об ответственности за распространение фейковых новостей (от англ. fake news – фальшивые новости).

Соответствующая тенденция существует и в России.

Под фейковыми новостями в российском законодательстве понимается заведомо недостоверная общественно значимая информация, распространяемая под видом достоверных сообщений и создавшая определенную угрозу жизни или здоровью граждан, имуществу, общественному порядку и общественной безопасности (ч. 1 ст. 15.3 Федерального закона от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации»).

Так, распространение в СМИ и Интернете заведомо недостоверной общественно значимой информации под видом достоверных сообщений влечет административную ответственность в виде штрафа в размере от 30 тыс. до 100 тыс. руб. для граждан, от 60 тыс. до 200 тыс. руб. для должностных лиц, от 200 тыс. до 500 тыс. руб. для организаций с возможной конфискацией предмета административного правонарушения, если правонарушение совершено гражданином или юридическим лицом (ч. 9 ст. 13.15 КоАП РФ).

Куда более серьезная ответственность за распространение фейковых новостей предусмотрена в случае, если оно повлекло создание помех функционированию объектов жизнеобеспечения, транспортной или социальной инфраструктуры и т. п., – штраф для граждан составляет от 100 тыс. до 300 тыс. руб., для должностных лиц от 300 тыс. до 600 тыс. руб., а для юридических лиц – от 500 тыс. до 1 млн руб., с конфискацией предмета административного правонарушения или без таковой для граждан и юридических лиц (ч. 10 ст. 13.15 КоАП РФ).

Повторное совершение данного правонарушения влечет наложение на граждан административного штрафа в размере от 300 тыс. до 400 тыс. руб., на должностных лиц – от 600 тыс. до 900 тыс. руб., на юридических лиц – от 5 млн до 10 млн руб.

Увеличение числа распространяемых заведомо ложных новостей в период пандемии новой коронавирусной инфекции обусловило необходимость поиска новых решений для борьбы с такой недостоверной информацией.

В апреле 2020 года ст. 13.15 КоАП РФ была дополнена новыми положениями. В отдельный состав правонарушения выделено распространение в СМИ и Интернете информации об обстоятельствах, представляющих угрозу жизни и безопасности граждан, или о принимаемых мерах по обеспечению безопасности населения и территорий, приемах и способах защиты от указанных обстоятельств.

К ответственности за данное правонарушение в виде штрафа в размере от 1,5 млн до 3 млн руб. с конфискацией предмета административного правонарушения или без таковой привлекаются только юридические лица (ч. 10.1 ст. 13.15 КоАП РФ).

Если распространение фейковых новостей о перечисленных обстоятельствах повлекло смерть человека, причинение вреда здоровью человека или имуществу, массовое нарушение общественного порядка или общественной безопасности, штраф для юридических лиц составляет уже от 3 до 5 млн руб. (ч. 10.2 ст. 13.15 КоАП РФ).

**Публичное распространение заведомо ложной общественно значимой информации, повлекшее тяжкие последствия, теперь является уголовным составом (ст. 207.2 Уголовного кодекса), так же, как публичное распространение заведомо ложных сведений об обстоятельствах, представляющих угрозу жизни и безопасности граждан (ст. 207.1 УК РФ)**

*В ходе мониторинга сети «Интернет» Генеральной прокуратурой Российской Федерации выявлены факты размещения недостоверной общественно значимой информации, распространяемой под видом достоверных сообщений, создающих угрозу массового нарушения общественного порядка и общественной безопасности.*

*Так, в социальной сети «ВКонтакте» на одной из страниц выявлена публикация, в которой говорится о 60 случаях подтвержденных фактов заражения коронавирусной инфекцией в г. Пензе, а также о свободном перемещении по городу больных граждан.*

*Материал спровоцировал широкое обсуждение. При этом комментарии были связаны с негодованием граждан о такой недостоверной «осведомленности» фактами заражения коронавирусом на территории Пензенской области и недопустимостью дезинформации населения региона.*

*Вместе с тем, согласно информации министерства здравоохранения Пензенской области, на территории субъекта зарегистрировано двое лиц, у которых имеется подозрение на коронавирус.*

*На сайте видеосервиса YouTube.com выявлен видеоролик под названием «Срочно! В Москву стянули войска! Карантин или госпереворот!», в котором автор выражает позицию относительно силового сценария подавления очагов коронавируса со стороны властей. При этом в ролике показаны передвижения войск национальной гвардии.*

*Между тем, согласно информации Правительства г. Москвы, названные автоколонны осуществляют перевозку сотрудников Росгвардии в г. Алябино для тренировок в рамках подготовки к Параду, посвященному 75-й годовщине Победы в Великой Отечественной войне 1941–1945 гг.*

*На этом же ресурсе найден видеоролик под названием «Колонны военной техники и военных двигаются к Москве. Силовикам отдадут все права к применению оружия», в котором автор на основании якобы достоверных сведений предупреждает зрителей о том, что политическим руководством отдан приказ о применении оружия по отношению к гражданам.*

## 5.2. ОТВЕТСТВЕННОСТЬ ЗА СПАМ-ЗВОНКИ.

Переход населения на удаленную работу, которая повышает значимость средств коммуникации и лояльность людей к входящим незнакомым звонкам, привел к значительному росту телефонного мошенничества.

Только за полгода Банк России блокировал почти 10 тыс. мошеннических телефонных номеров. И их количество растет в геометрической прогрессии.

**ТАК, ЗА 2020 ГОД ТЕЛЕФОННЫЕ АФЕРИСТЫ И ОНЛАЙН-МОШЕННИКИ ЗАРАБОТАЛИ НА РОССИЯНАХ ПОЧТИ 150 МЛРД РУБ., ПОДСЧИТАЛИ АНАЛИТИКИ BRANDMONITOR НА ОСНОВЕ ДАННЫХ ВЦИОМ. МОШЕННИКИ УСОВЕРШЕНСТВОВАЛИ ТАКТИКУ И ДЕЛЕГИРОВАЛИ ПЕРВИЧНЫЙ ОБЗВОН РОБОТАМ, ЧТОБЫ УДЕШЕВИТЬ СТОИМОСТЬ АТАКИ.**

При этом **66 млрд руб.** приходится на доходы псевдобанковских сотрудников. А наиболее дорогостоящими в среднем оказались разговоры с фиктивными медработниками, которые выманивают более **50 тыс. руб.** с человека.

Финансовые организации и телеком-операторы активно борются с мошенниками и блокируют их номера, хотя существенно улучшить ситуацию сможет только повышение финансовой и цифровой грамотности граждан.

Так называемые спамеры могут нарушать сразу три закона: **о связи, о рекламе и о персональных данных**. За эти нарушения предусмотрена административная ответственность, то есть штраф. Сумма штрафа зависит от того, что именно было нарушено и какое ведомство это контролирует.

**Реклама по телефону допускается только с вашего согласия (ст. 18 Федерального закона «О рекламе» № 38-ФЗ (ред. от 30.04.2021)). Вам может казаться, что вы никогда не соглашались на рекламу, но есть много способов получить это согласие незаметно. Вы могли подписать согласие, например, при оформлении дисконтной карты или при подписке на рассылку интернет-магазина.**

**Согласие на предоставление справочной и рекламной информации может быть зафиксировано в договоре, который вы тоже могли сами подписать. В этом случае звонки будут законными.**

Если вы уверены, что не давали согласия на рекламу, можно вести речь об ответственности для нарушителей.

Соблюдение закона о рекламе контролирует Федеральная антимонопольная служба. Для этого ей нужно найти нарушителя, а вам – доказать, что факт рекламы был.

ПАМЯТКА ПАМЯТКА

**ЗВОНОК С НЕЗНАКОМОГО ИЛИ СКРЫТОГО НОМЕРА.** Из банка всегда звонят с официальных номеров, указанных на сайте. Он может быть федеральным, может быть мобильным, но он не будет скрытым.

**КТО ГОВОРИТ.** Если вам звонит незнакомый человек, нужно узнать, кто он. Обычно спамеры произносят наименование компании в первые секунды звонка, когда внимание на разговоре еще не сосредоточено. Вам нужно узнать точное наименование организации, не стесняйтесь переспросить.

Иногда звонит человек как физлицо и предлагает услуги от себя лично. В этом случае спросите его полное имя и откуда он узнал ваш номер.

**СОБЕСЕДНИК НЕ МОЖЕТ ОТВЕТИТЬ НА ПРОСТЫЕ ВОПРОСЫ.** Оператор банковского колцентра видит на экране все, что банк о вас знает. Если собеседник не готов ответить на простой вопрос, например назвать остаток по карте, это мошенник.

**ТРЕВОЖНАЯ ТЕМА СООБЩЕНИЯ ИЛИ ЗВОНКА.**

Чтобы заставить вас совершить нужное действие, мошенники придумывают пугающие сценарии. Говорят, что банк заблокировал счет, начислил штраф за кредит или что проведена подозрительная операция. В такой ситуации не спешите, позвоните в банк по телефону, указанному на сайте или на карте, и уточните ситуацию.

**СОБЕСЕДНИК СПРАШИВАЕТ ДАННЫЕ КАРТЫ ИЛИ СМС-КОД.** Смс-код – это пароль. Сотрудники банка никогда его не спросят, а номер карты они и так знают.

ПАМЯТКА ПАМЯТКА

# 6. БЛОКИРОВКА САЙТОВ

Раньше взрослые люди и не думали, что воспитание ребенка будет сопряжено с опасностями, таящимися в интернете. И это еще одна обратная сторона тотальной цифровизации общества.

Ранний доступ детей к электронно-цифровым продуктам порождает новые проблемы от их взаимодействия с компьютерами и смартфонами:

– неспособность детей к самоуглублению, к концентрации на каком-либо занятии, отсутствие заинтересованности делом;

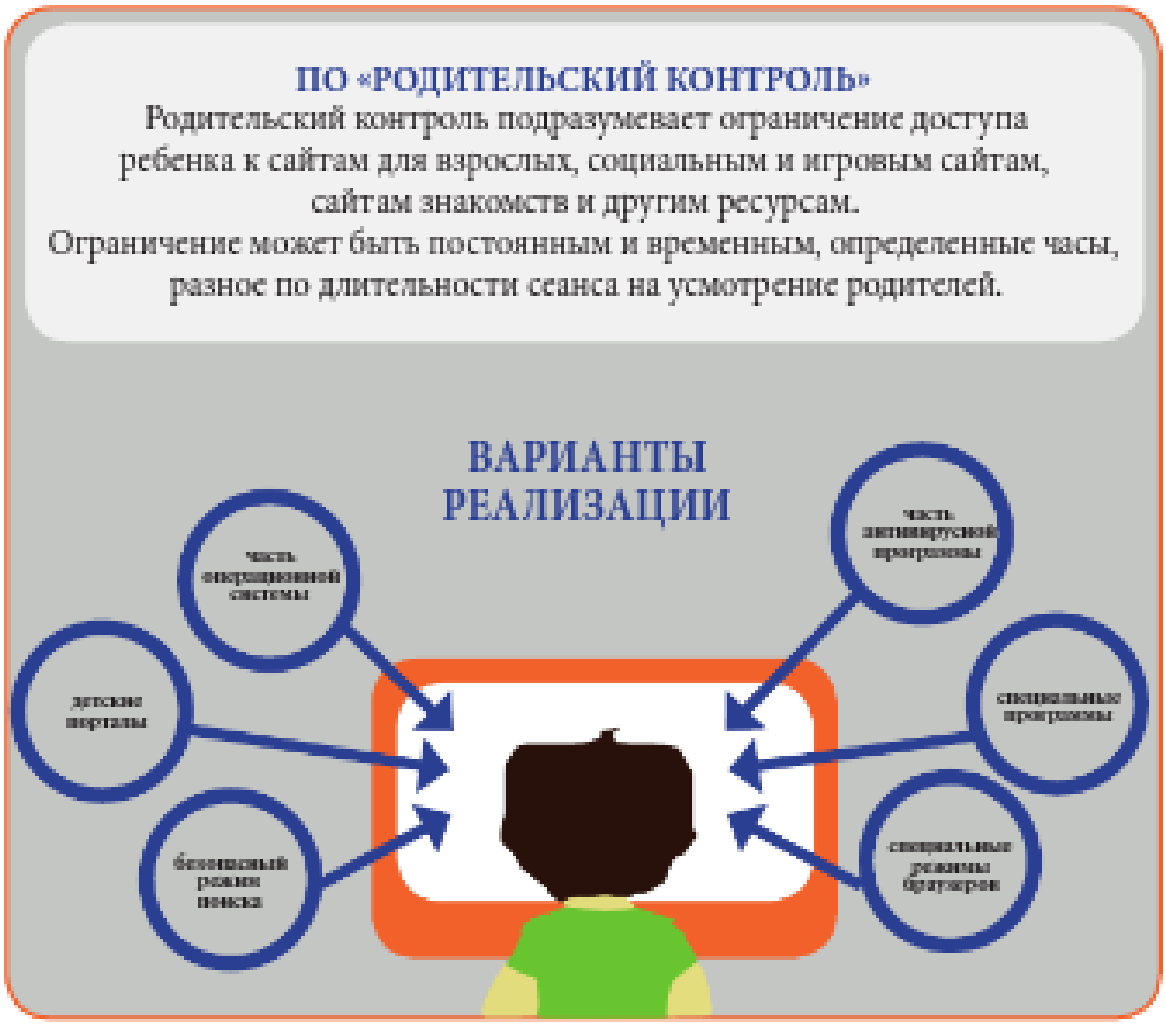
– снижение детской фантазии и творческой активности;

– повышение детской жестокости и агрессивности.

– отрицательное влияние на физическое здоровье ребенка, его зрение (по некоторым данным с 1997 года, когда впервые смартфоны поступили в продажу, число пациентов с близорукостью возросло на 35%).

– невозможность контролировать и защищать ребенка от вредной информации.

## 6.1. РОДИТЕЛЬСКИЙ КОНТРОЛЬ.



Под **РОДИТЕЛЬСКИМ КОНТРОЛЕМ** подразумевается программа в Интернете для предотвращения предполагаемого негативного воздействия на ребенка. Обычно используется либо дополнительное программное обеспечение, либо встроенные приложения. Программы родительского контроля предназначены, в первую очередь, для создания ограничений ребенку, они призваны обеспечить его безопасность, оградить от того, что, возможно, ему еще рано знать и видеть.

Одна из основных задач приложений – создание фильтра web-сайтов: на одни страницы заходить можно, на другие – нельзя.

Часто применяется более жесткий способ контроля – создание белого списка. Ребенок может посещать только те web-сайты, которые ему разрешили родители.

Еще один способ родительского контроля заключается в фильтрации сайтов по их содержимому. Вы задаете набор ключевых слов, и если что-либо из их списка обнаруживается на web-странице, то она не открывается.

Обеспечение безопасности ребенка за компьютером заключается не только в ограничении доступа к web-сайтам. Есть еще одна зона риска – это программы обмена мгновенными сообщениями.

Ребенок наивен, он может нечаянно сообщить незнакомцу ваши личные данные. Злоумышленники же хитры, притворяются ровесниками, задают каверзные вопросы. Вторая опасность – собеседники могут научить ребенка, в лучшем случае, мелким пакостям; в худшем – довести до самоубийства и др.

Некоторые программы родительского контроля способны производить анализ информации, отправляемой с компьютера. Если в ней встречаются некие ключевые слова, например адрес, номер школы или телефона, то происходит блокировка отправки сообщения.

**ДЛЯ ЗАЩИТЫ ДЕТЕЙ ОТ ОПАСНОГО КОНТЕНТА В РОССИИ РАБОТАЮТ ТРИ ОСНОВНЫХ ЗАКОНА:**

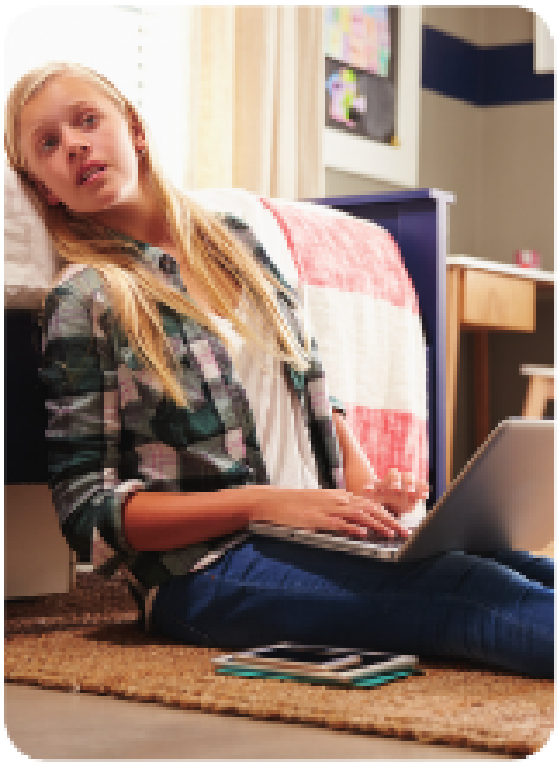
1. 436-ФЗ «О защите детей от информации, причиняющей вред их здоровью и развитию»;
2. 124-ФЗ «Об основных гарантиях прав ребенка в Российской Федерации» (статья 14);
3. 149-ФЗ «Об информации, информационных технологиях и о защите информации».

## ВИДЫ ОПАСНОЙ ДЛЯ ДЕТЕЙ ИНФОРМАЦИИ

Все три закона делят опасную для детей информацию на две основные категории: полностью запрещенную для показа детям (а в случае 149-ФЗ – вообще всем категориям граждан) и информацию, к которой следует ограничить доступ детей определенного возраста (те самые 6+, 12+,16+ и т.д.)

Полностью запрещено демонстрировать несовершеннолетним информацию: побуждающую к нанесению вреда здоровью, к самоубийству, к насилию и жестокости по отношению к людям и животным; подталкивающую к наркомании, курению и алкоголизму, к проституции, нетрадиционным сексуальным отношениям, а также содержащую порнографию; пропагандирующую азартные игры, бродяжничество и попрошайничество; содержащую нецензурную брань. Также запрещена пропаганда национальной, классовой, социальной, расовой нетерпимости и неравенства, войн, терроризма и экстремизма.

Особняком стоит запрет на распространение информации о несовершеннолетнем, пострадавшем в результате противоправных действий (бездействия). Так обеспечивается защита всех данных ребенка, которые позволяют установить его личность.



**ТЕПЕРЬ О ТОМ, К ЧЕМУ НУЖНО ОГРАНИЧИТЬ ДОСТУП ПО ВОЗРАСТНЫМ КАТЕГОРИЯМ –**

**К ИЗОБРАЖЕНИЯМ ИЛИ ОПИСАНИЯМ: ЖЕСТОКОСТИ, ФИЗИЧЕСКОГО И (ИЛИ) ПСИХИЧЕСКОГО НАСИЛИЯ, ПРЕСТУПЛЕНИЙ, ПОЛОВЫХ ОТНОШЕНИЙ МЕЖДУ МУЖЧИНОЙ И ЖЕНЩИНОЙ; К ИНФОРМАЦИИ, ВЫЗЫВАЮЩЕЙ У ДЕТЕЙ СТРАХ, УЖАС ИЛИ ПАНИКУ (НЕНАСИЛЬСТВЕННАЯ СМЕРТЬ, БОЛЕЗНЬ, САМОУБИЙСТВО, АВАРИЯ/КАТАСТРОФА), СОДЕРЖАЩЕЙ БРАНЬ, НЕ ОТНОСЯЩУЮСЯ К НЕЦЕНЗУРНОЙ.**

Законодательство предписывает защиту детей от опасной информации в общественных местах. Обязанность не допустить детей к информации, не соответствующей их возрасту, возлагается на лиц, обеспечивающих вход и пребывание детей в таких местах. То есть, проще говоря, если ребенок находится в школе, то ответственность несут руководство и учителя, если в цирке/кинотеатре/магазине – администрация и сотрудники заведений. Ответственность – согласно статье 6.7 КоАП РФ.

При этом закон освобождает операторов связи от обязанности защищать детей от опасной информации в общественном месте. Например, если в фойе кинотеатра вдруг запустят рекламный ролик, содержащий сцены насилия, отвечать перед законом будет не интернет-провайдер, а владелец заведения.

## 6.2. КУДА МОЖНО ОБРАТИТЬСЯ С ЖАЛОБОЙ НА ЗАПРЕЩЕННЫЙ КОНТЕНТ.

Одной из инстанций, куда можно пожаловаться на сайт, нарушающий законы РФ, является Роскомнадзор. Любой желающий – как гражданин РФ, так и житель любой другой страны – на официальном сайте федеральной службы может заполнить форму обращения (http://rkn.gov.ru/treatments/ask-question/) или позвонить в справочно-информационный центр.

Кроме того, на сайте «Центра безопасного Интернета в России» (www.saferunet.ru) есть ссылка на «горячую линию» – кликнув по красной картинке, вы попадете в раздел, где сможете пожаловаться на ту или иную страницу в Сети, которая, по вашему мнению, нарушает чьи-то права или даже российские законы.

Подать жалобу на «плохие» страницы можно в службу поддержки поисковых систем, таких как Яндекс и Google. У Яндекса есть страница обратной связи, расположенная по адресу webmaster.yandex.ru/delspam.xml. Там можно сообщить администрации о том, что вы нашли в результатах поиска страницу, с которой распространяются вирусы, или рассказать о сайте, который, по вашему мнению, создали мошенники.

В свою очередь, на сайте Google есть раздел, помогающий разобраться с особенностями поиска. Найдите пункт «Я хочу убрать из своих результатов поиска сайты с непристойным и опасным содержанием, сайты, распространяющие спам, а также сообщить в Google о наличии таких сайтов в результатах». Выбрав его, вы увидите описание нескольких проблем, среди которых может оказаться и ваша. Пункты «Я хочу пожаловаться на спам в результатах поиска» и «Я хочу сообщить о вредоносном ПО» позволят вам отправить в Google информацию о вредоносных сайтах.

## 6.3. БЛОКИРОВКА САЙТОВ.

(контент, который блокируется и запрещается к распространению на территории Российской Федерации: ответственность лиц, его размещающих, и владельцев интернет-ресурсов).

В соответствии со статьей 15.1 Федерального закона от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации» в целях ограничения доступа к противоправной информации в сети Интернет создана и ведется единая автоматизированная информационная система «Единый реестр доменных имен, указателей страниц сайтов в сети «Интернет» и сетевых адресов, позволяющих идентифицировать сайты в сети «Интернет», содержащие информацию, распространение которой в Российской Федерации запрещено», там же подать сообщение о ресурсе, содержащем запрещенную информацию (https://eais.rkn.gov.ru/feedback).

Частью 5 статьи 15.1 Федерального закона № 149-ФЗ предусмотрены следующие основания включения сведений в единый реестр во внесудебном порядке:

1) решения уполномоченных Правительством Российской Федерации федеральных органов исполнительной власти, принятые в соответствии с их компетенцией в порядке, установленном Правительством Российской Федерации, в отношении распространяемых посредством сети «Интернет»:

а) материалов с порнографическими изображениями несовершеннолетних и (или) объявлений о привлечении несовершеннолетних в качестве исполнителей для участия в зрелищных мероприятиях порнографического характера;

б) информации о способах, методах разработки, изготовления и использования наркотических средств, психотропных веществ и их прекурсоров, новых потенциально опасных психоактивных веществ, местах их приобретения, способах и местах культивирования наркосодержащих растений;

в) информации о способах совершения самоубийства, а также призывов к совершению самоубийства;

г) информации о несовершеннолетнем, пострадавшем в результате противоправных действий (бездействия), распространение которой запрещено федеральными законами;

д) информации, нарушающей требования Федерального закона от 29 декабря 2006 года N 244-ФЗ «О государственном регулировании деятельности по организации и проведению азартных игр и о внесении изменений в некоторые законодательные акты Российской Федерации» и Федерального закона от 11 ноября 2003 года N 138-ФЗ «О лотереях» о запрете деятельности по организации и проведению азартных игр и лотерей с использованием сети «Интернет» и иных средств связи;

2) вступившее в законную силу решение суда о признании информации, распространяемой посредством сети «Интернет», информацией, распространение которой в Российской Федерации запрещено.

# 7. ДИСТАНЦИОННОЕ МОШЕННИЧЕСТВО

**ДИСТАНЦИОННОЕ МОШЕННИЧЕСТВО** – это совершение такого вида преступлений, при котором виновный, чаще всего используя компьютерные и телефонные сети, воздействует на сознание потерпевшего путем обмана, склоняет к передаче имущества удаленным образом.

Бесконтактный и быстрый способ совершения таких преступлений делает общество все более уязвимым перед новыми вызовами. При этом правоохранительные органы зачастую оказываются к ним неготовыми.

Низкая выявляемость и раскрываемость киберпреступлений порождает безнаказанность и чувство вседозволенности.

Злоумышленник вводит в заблуждение потенциальную жертву, в дальнейшем похищая у нее деньги. Потерпевшие сами сообщают мошеннику нужную информацию. Преступник получает доступ к счету мобильного телефона или к банковской карте, с которой впоследствии похищаются деньги.

## ДИСТАНЦИОННЫЕ МОШЕННИЧЕСТВА МОЖНО РАЗДЕЛИТЬ НА ТРИ ГРУППЫ:

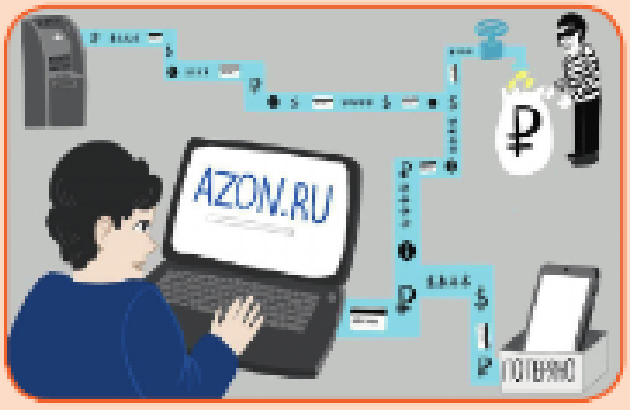
**Мошенничества, совершенные с использованием средств сотовой связи и сети Интернет.** Предлоги, которые используют преступники, разнообразны и являются только условием для получения информации о банковской карте, счете или способствуют перечислению самим потерпевшим денежных средств на используемые мошенниками расчетные счета (такие как: разблокировка банковской карты, приобретение и реализация товаров на интернет-площадках, в случаях, когда размещенный на них товар только предлог для звонка потенциальному потерпевшему, компенсация за ранее приобретенные медицинские препараты, компенсация от Пенсионного фонда и так далее).

**Мошенничества, совершенные с использованием средств сотовой связи и непосредственного контакта с потерпевшим.** Как правило, данный способ характерен при использовании предлога – родственник попал в беду, ДТП, полицию и так далее).

**Мошенничества, совершенные только с использованием интернет-ресурсов.** Покупка, продажа товара на различных интернет — площадках, в том числе использование «зеркальных» сайтов (сайтов, схожих с оригинальными, которые принадлежат известным организациям), взлом страниц в социальных сетях и рассылка от имени пользователя страницы в социальной сети просьбы перечислить деньги.

Оценить размер таких хищений сложно, так как люди часто не сообщают о своих потерях. По предварительным оценкам «Лаборатории Касперского», большое количество инцидентов в русскоязычном сегменте интернета было связано со скамом, то есть с онлайн-мошенничеством, при котором злоумышленники обещают пользователю денежное вознаграждение, для получения которого ему нужно уплатить комиссию.

**ЕЩЕ ОДНИМ КРАЙНЕ РАСПРОСТРАНЕННЫМ ВИДОМ ИНТЕРНЕТ-МОШЕННИЧЕСТВА ЯВЛЯЮТСЯ ФАЛЬШИВЫЕ ИНТЕРНЕТ-МАГАЗИНЫ.**




**Мошенники берут с покупателя предоплату за товар и не выполняют своих обязательств. Платежные страницы на таких сайтах только маскируются под оплату товаров и услуг, на самом деле потенциальная жертва переводит деньги на карты мошенников или на номера мобильных телефонов, с которых впоследствии мошенники снимут деньги. Кроме того, на поддельных сайтах мошенники собирают реквизиты карт, которые потом используют для несанкционированных операций. После совершения такой оплаты жертва даже может получить подтверждение по почте, но товаров ни услуг доставлено и оказано не будет.**

ПАМЯТКА ПАМЯТКА

## КАК ОТЛИЧИТЬ ПОДДЕЛЬНЫЕ САЙТЫ ОТ НАСТОЯЩИХ?

1. Внимательно изучите адресную строку. Дизайн может полностью копировать оригинальный сайт, но в адресной строке точно будет что-то не так, хотя бы один символ.
2. Сайт новый и о нем нет никакой информации в интернете.
3. Тексты на сайте могут содержать ошибки и неработающие ссылки.
4. Дизайн страницы ввода одноразового пароля может отличаться от привычного дизайна вашего банка, а еще название магазина будет написано порски, а не латинскими буквами как обычно в легальных платежных системах.
5. Вместо названия магазина на аутентификационной странице символы P2P, PEREVODNAKARTU, или CARD2CARD, то есть информация о переводе средств с карты на карту.
6. Сумма на аутентификационной странице банка может быть изменена.
7. После введения корректных данных сайта для одноразового пароля жертве сообщают, что пароль неверный и просят ввести новый пароль на самом деле, чтобы провести новую операцию.

ПАМЯТКА ПАМЯТКА

# 8. КРАЖА ДЕНЕГ С БАНКОВСКИХ КАРТ – КАК ЗАЩИТИТЬСЯ

Сразу повторим. Чтобы уберечь свои средства, не сообщайте никому конфиденциальные сведения (коды, пароли), а также осматривайте денежные терминалы на присутствие подозрительных устройств.

Если мошенник снял деньги с карты – срочно звоните в банк и блокируйте операции по ней, а затем отправляйтесь в офис кредитной организации и полицию.

Сегодня похитить ваши деньги аферисты могут самыми различными способами: при помощи скимминга, фишинга, фальшивого банкомата, pos-терминала, смс-сообщений и поддельных сайтов. Сделать данные карты доступными мошенникам можно, пользуясь бесплатными wi-fi и совершая безналичные платежи в интернете.

Потенциально опасным является приложение для смартфонов «Мобильный банк». Похитив гаджет, грабители способны приобрести доступ к вашим деньгам. Такой риск существует и при смене сим-карты.

**ПРЕСТУПНИКАМ ИЗВЕСТНО БОЛЬШОЕ КОЛИЧЕСТВО МЕТОДОВ ПОХИЩЕНИЯ КАПИТАЛОВ С ПЛАСТИКОВОЙ КАРТЫ СВОЕЙ ЖЕРТВЫ. И ПОРОЙ САМ ДЕРЖАТЕЛЬ ПЛАТЕЖНОГО ИНСТРУМЕНТА ОКАЗЫВАЕТСЯ ВИНОВАТ В КРАЖЕ ЛИБО СПОСОБСТВУЕТ ЕЕ СОВЕРШЕНИЮ СВОЕЙ НЕОСМОТРИТЕЛЬНОСТЬЮ.**

### СКИММИНГ

*Это хищение бандитами информации с карты в процессе снятия денег или оплаты услуги в банкомате посредством специального изобретения — скиммера. Устройство может быть сделано в виде накладной клавиатуры или вставляться внутрь картоприемника.*

### БАНКОМАТЫ: ОТ ФАЛЬШИВОК ДО ПРОПАВШИХ

*Аферисты выкупают банкоматы, ранее используемые банками, и снабжают их скиммерами. Когда клиент вставляет карту и пытается произвести транзакцию, аппарат отказывает в выполнении операции, а мошенники получают нужные им данные. Фальшивые банкоматы могут маскироваться под устройства известных банков, их бывает трудно обнаружить.*

### ПОРОЙ ПРЕСТУПНИКИ ВОРУЮТ БАНКОМАТЫ

### НЕБЕЗОПАСНЫЕ ПРИЛОЖЕНИЯ

*К таким программам относится «Мобильный банк». Похитив телефон, преступник может войти в приложение и воспользоваться картой, оплатив что-либо или выполнив перевод.*

**POS-ТЕРМИНАЛЫ.** *Мошенники устанавливают в терминалы оплаты устройства или программное обеспечение, считывающие данные карты, а затем используют их в личных целях. Другой вариант: недобросовестный сотрудник магазина или кафе приписывает небольшие суммы к оплачиваемому счету в надежде на невнимательность покупателя. С помощью собственного беспроводного терминала преступники могут снимать деньги у своих жертв через одежду или сумки в местах большого скопления людей.*

## БЕЗНАЛИЧНЫЙ РАСЧЕТ

*Обманщики создают поддельные интернет-магазины, в которых возможен только один способ приобретения продукции — стопроцентная предоплата посредством безналичного расчета. Покупатель перечисляет деньги на номер карты нечистого на руку лица, а товар ему так и не присылают либо приходит подделка. При расчетах на торговых площадках можно пострадать от грабителей. Владелец карты по полученной ссылке переходит на сайт злоумышленников, где им становятся доступны сведения о его банковской карте.*

## БЕСПЛАТНЫЙ WI-FI

*Кибер-преступники могут создавать поддельные wi-fi сети, маскируя их под бесплатные. Когда владелец гаджета подключается к такой сети, все данные, находящиеся на его устройстве, оказываются у аферистов. Подобные бесплатные сети чаще всего используют в барах, ресторанах, аэропортах и т.п.*

## ЗАГАДОЧНЫЕ СООБЩЕНИЯ

*Это могут быть sms якобы от попавших в неприятную ситуацию родных, о выигрыше, о блокировке карты, о случайном пополнении счета мобильного незнакомцем с требованием возвратить деньги и т.п. Очень часто воры присылают смс-сообщения с поддельных сервисных номеров банка с требованием указать пин-код карты или прочую конфиденциальную информацию.*

## ФЕЙКОВЫЕ САЙТЫ

*Аферисты создают фейковые веб-страницы, похожие на официальные сайты известных банков, и обязывают обладателей карт оставить свою конфиденциальную информацию. Получив данные, злоумышленники крадут денежные средства.*

## ФИШИНГ

*Это выманивание данных платежных карт у их обладателей. Например, по вашему объявлению о продаже чего-либо звонит человек, который предлагает внести предоплату и запрашивает данные карты, совершенно не интересуясь при этом самим характеристиками товара.*

**КАК ТОЛЬКО ВАМИ УСТАНОВЛЕНО, ЧТО НЕКТО ВОСПОЛЬЗОВАЛСЯ ДЕНЬГАМИ С ВАШЕЙ КАРТЫ, НЕОБХОДИМО СРОЧНО:**

**1. Созвониться с обслуживающим банком, установить блокировку и сообщить о незаконном использовании средств.**

**2. Пойти в офис кредитной организации с паспортом и составить бумагу о несогласии с произведенной транзакцией.**

**3. Оформить заявление в полицию о краже денег с карты.**

**Банк проводит расследование в течение месяца. При отрицательном решении банка касаемо возврата средств можно подавать документы в суд.**

ПАМЯТКА ПАМЯТКА

## КАК ЗАЩИТИТЬСЯ ОТ ДЕЙСТВИЙ МОШЕННИКОВ

1. Держите в секрете свои личные данные (пароли, пин-коды, номера счетов).
2. Не отвечайте на СМС с требованием выслать данные по карте, особенно если номер приславшего вызывает подозрения.
3. Обеспечьте безопасность компьютера, с которого производите вход в личный кабинет банка.
4. Прикрывайте клавиатуру при вводе пин-кода, работая с банкоматом, терминалом или оплачивая покупку в магазине.
5. До совершения операции осмотрите банкомат на наличие подозрительных приспособлений.
6. Не оформляйте заказы и не платите в интернет-магазинах, не вызывающих доверия.
7. При перемене мобильного номера оповестите финансово-кредитную организацию.

ПАМЯТКА ПАМЯТКА ПАМЯТКА ПАМЯТКА

# СОДЕРЖАНИЕ