С. Н. Вангородский

# ОСНОВЫ КИБЕРБЕЗОПАСНОСТИ

Учебно-методическое пособие

5-11 классы

ДРОФА

Российский учебник

С. Н. Вангородский

# ОСНОВЫ КИБЕРБЕЗОПАСНОСТИ

Учебно-методическое пособие

5–11 классы

Москва
ДРОФА
2019

УДК 373.167.1:004
УДК 32.97я72
В17

**Вангородский, С. Н.**

В17 Основы кибербезопасности : учебно-методическое пособие. 5—11 классы / С. Н. Вангородский. — М. : Дрофа, 2019. — 238, [1] с. — (Российский учебник).

ISBN 978-5-358-22190-1

Пособие адресовано учителям и учащимся общеобразовательных организаций, а также родителям школьников. В нем представлены наиболее распространенные виды киберугроз, цели и задачи системы кибербезопасности, небезопасные для детей и подростков интернет-сервисы.

Для педагогов и родителей в пособии предлагается полезная информация о программах контроля, позволяющих защитить школьников от опасных сайтов, и методические рекомендации по формированию у детей и подростков навыков безопасного поведения в Интернете.

**УДК 373.167.1:004**
**УДК 32.97я72**

ISBN 978-5-358-22190-1

# КИБЕРУГРОЗЫ (КИБЕРОПАСНОСТИ)

Информационные технологии все больше проникают в общественные сферы, что вызывает значительный рост разного рода **киберугроз** и приводит к серьезным изменениям в сознании миллиардов людей.

В результате исследований, проведенных «Лабораторией Касперского», установлено, что 9 из 10 компаний регулярно сталкиваются с внешними киберугрозами. За 2016 г. 91% иностранных и 96% российских компаний, представители которых приняли участие в опросе, сталкивались с угрозами информационной безопасности. Было осуществлено большое количество **кибератак**, направленных на финансовые организации и приведших к огромным финансовым потерям, простоям в работе.

Значительный ущерб был нанесен деловой репутации банков, коммерческим организациям и даже странам. Среди наиболее пострадавших — украинские энергосети, Центральный банк Бангладеш, Всемирное антидопинговое агентство (WADA).

Многие организации пострадали от киберпреступников: например, треть вирусных атак на иностранные компании (а на российские компании — почти половина) привела к потере данных, при этом для 10% фирм это была важная для бизнеса информация.

**Хакеры** не оставили без внимания и физических лиц: сотни миллионов **аккаунтов** и паролей пользователей были украдены у **LinkedIn** и **Yahoo**.

Кибератаки серьезно повлияли на политическую обстановку в мире: она изменилась в результате утечки писем Демократической партии США, раскрытия **оффшорных счетов Mossack Fonseca** и деятельности группировки **Fancy Bear**.

## ОСНОВНЫЕ ВИДЫ КИБЕРУГРОЗ

В настоящее время все киберугрозы принято разделять на внешние и внутренние.

Причины и источники внешних угроз находятся вне **компьютеров** компании, как правило, в глобальной сети. Внутренние угрозы зависят исключительно от персонала компании, **программного обеспечения** и оборудования.

К внешним угрозам относят:

- вирусы;
- **спам**;
- **фишинг**;
- удаленный взлом;
- DoS/DDoS-атаки;
- хищение мобильных устройств.

Основная опасность киберугроз в скорости их изменения.

**Вирусы** скрытно проникают в компьютерные системы, и без эффективной защиты бороться с ними невозможно.

Чтобы вирусы проникли в компьютер, достаточно всего лишь открыть вложение в электронном письме (при этом совершенно не обязательно, чтобы письмо было отправлено неизвестным адресатом, хорошо известный компаньон также может прислать вирус, если ранее его компьютер был заражен). Некоторым вирусам достаточно уже того, что компьютер просто подключен к **локальной сети**, к которой подключен и зараженный компьютер. Для распространения значительного числа вирусов используют съемные накопители информации (флешки, мобильные жесткие диски и оптические носители).

Использование нелицензионного (пиратского) программного обеспечения может привести к потере данных пользовательских аккаунтов, к блокировке устройства, где установлена нелегальная программа.

Продолжает расти число неизвестного вредоносного программного обеспечения: исследователями было за-

фиксировано 9-кратное увеличение количества неизвестных программ, атакующих организации. Каждый месяц специалисты обнаруживают почти 12 млн новых вариантов вредоносных программ.

В настоящее время создатели вирусов используют их в основном для получения финансовой выгоды. Средний размер выкупа, который требовали **кибервымогатели** со своих жертв, в 2016 г. вырос на 266% .

Атака вируса-вымогателя WannaCry заразила более 230 тыс. устройств в 150 странах.

Еще более опасно, если вирус **троянской программы** перехватит данные банковского счета.

Вирусы могут нарушить работоспособность компьютеров и программ, уничтожить файлы, используя для своих целей трафик, каналы связи, рассылая спам.

Наиболее опасным вирусом является кибероружие, которое направлено в некоторых случаях на уничтожение промышленной инфраструктуры. Появление вирусов Duqu, Stuxnet, Gauss, Flame обошлось не в один миллион долларов.

**Спам** не только вызывает раздражение у пользователей, но и забивает **каналы связи**, расходует трафик, отвлекает от работы, вынуждая людей искать важную корреспонденцию среди рекламы. В конечном счете все это приводит к финансовым потерям. Помимо этого, спам также является одним из распространенных каналов внедрения троянских программ и вирусов.

**Фишинг**, в отличие от спама, нацелен на узкие группы пользователей и содержит сообщения с социальным контекстом, призывающие потенциальную жертву открыть исполняемый файл или перейти на сайт, содержащий вредоносный код.

Большую опасность представляет также **удаленный взлом компьютеров**, за счет которого злоумышленники могут получать возможность читать и редактировать документы, хранящиеся на файл-серверах и в компьютерах, по собственному желанию уничтожать их, внедрять собственные программы, которые следят за всеми действиями конкурентов и собирают определенную информацию, вплоть до незаметного аудио- и видеона-

блюдения через микрофоны ноутбуков и штатные веб-камеры.

Заражение SEO (Search Engine Optimization) приводит к тому, что сайты, содержащие вредоносный код, подставляются на высокие места в рейтингах поисковых систем при вводе запроса. Защититься от таких угроз можно, используя актуальные версии шлюзового антивируса и системы предотвращения вторжений.

Практически все вредоносное **программное обеспечение** может распространяться через популярные социальные сети.

Еще одна зона риска в **Интернете** — это угрозы для личной безопасности. Она связана с появлением мобильных устройств. Пользователь вынужден выдавать организаторам транзакций большой объем личной информации, которая может быть использована ему во вред.

Особого внимания для пользователей продукции **Android** заслуживают Android-трояны, распространенность которых обусловлена основными проблемами Android:

- повсеместным использованием старых версий операционных систем со слабой системой безопасности;
- разнообразием мобильных устройств, для ряда которых обновлений просто не существует;
- огромным количеством сторонних **маркетплейсов**, где можно скачать фальшивые и зараженные приложения.

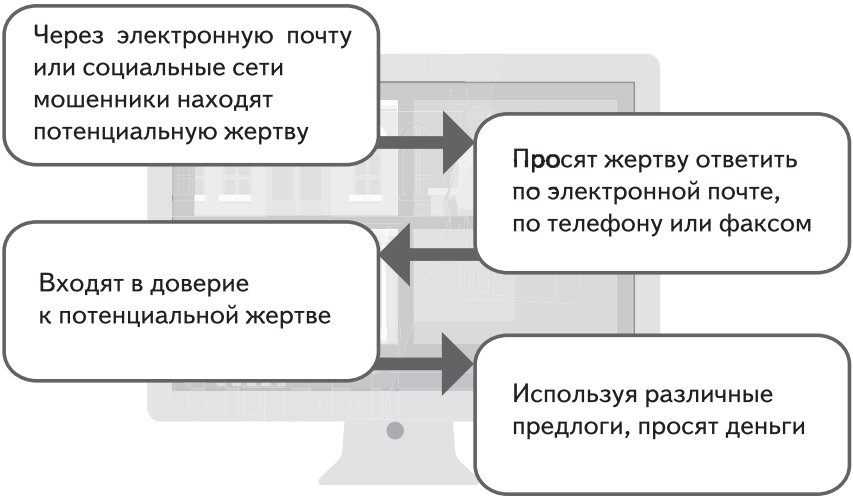
Пользователи продукции Apple тоже не могут чувствовать себя в полной безопасности. Угрозу несут в себе и новые технологии, особенно в случае отсутствия их профессиональной киберзащиты.

В 2016 г. на информационные ресурсы нашей страны было совершено свыше 50 млн кибератак, что в три раза превысило показатели 2015 г. Для надежной защиты собственной критической информационной инфраструктуры в России создана Государственная система обнаружения, предупреждения и ликвидации последствий компьютерных атак.

## ИНТЕРНЕТ-АФЕРЫ

Антивирусная лаборатория PandaLabs составила рейтинг наиболее распространенных в Интернете афер за последние 5 лет. Эти аферы основаны на доверии и имеют самое широкое распространение. Их цель — выманивание денег у пользователей.

В большинстве случаев мошенники действуют по одной схеме.




Ниже рассмотрены самые распространенные виды интернет-афер.

- **«Нигерийская афера».** Обычно пользователю приходит электронное письмо от незнакомца, которому срочно нужно перевести большую сумму денег из одной страны в другую (чаще всего из Нигерии, отсюда и название). Жертве обещают немалое вознаграждение за помощь в переводе денег. Однако сначала просят перевести определенную сумму, чтобы оплатить банковские расходы (это около 1000 долл. США). Как только перевод денег состоялся, мошенник исчезает.

- **«Лотерея».** Пользователь получает письмо по электронной почте, в котором сообщается, что он выиграл в лотерею и что для получения выигрыша ему необходимо прислать свои данные. Жертву просят перечислить около 1000 долл. США, чтобы покрыть банков-

ские и другие расходы. После перечисления денег мошенник исчезает.

• **«Подружка».** На электронную почту пользователя приходит письмо с просьбой о знакомстве. Часто во вложении имеется фотография красивой девушки. В письме говорится, что она мечтает побывать в вашей стране и встретиться с вами, так как влюбилась с первого взгляда. Она хочет приехать незамедлительно, но в последний момент возникают какие-то проблемы, и ей необходимы деньги (около 1000 долл. США должно хватить), чтобы купить билеты на самолет, заплатить за визу и так далее. Неудивительно, что после перевода названной суммы исчезают не только деньги, но и девушка.

• **«Приглашение на работу».** Жертва получает письмо с приглашением на работу от иностранной компании, которая ищет финансовых агентов в ее стране. Работа предельно проста, ее можно выполнять, не выходя из дома, и при этом зарабатывать до 3000 долл. США при трех- или четырехчасовом рабочем дне. Если жертва соглашается с данным предложением, ее просят прислать банковские реквизиты. Деньги перечисляют на счёт жертвы, а потом просят снять деньги со счета и переслать их через **Western Union**. Так жертва становится «переходным звеном» в цепочке мошенников, а когда дело попадает в полицию, жертва превращается в соучастника. В отличие от афер другого типа, в этом случае жертва, даже не подозревая о том, совершает преступление.

• **«Личные страницы».** Мошенники похищают данные для входа на личные страницы, затем меняют логин, чтобы у хозяина страницы больше не было возможности пользоваться своим аккаунтом. Далее преступники отправляют с этой страницы всем контактам сообщения, указывая, что владелец страницы сейчас в отпуске за границей, что его ограбили как раз перед возвращением домой. К счастью, билеты на самолет не пропали, но необходимо 500—1000 долл. США для оплаты отеля.

• **«Компенсация».** В электронном письме сообщается, что был создан специальный фонд для выплаты компенсаций жертвам «Нигерийской аферы» и что адрес

жертвы был в списке пострадавших. Размер компенсации может доходить до 1 млн долл. Но, как и в других аферах, чтобы их получить, необходимо оплатить предварительные расходы — около 1000 долл. США.

- **«Ошибка».** Этот тип мошенничества очень популярен. Мошенники выходят на контакт с жертвой, которая недавно размещала рекламу о продаже, например, дома, соглашаются купить дом и быстро высылают чек на определенную сумму, которая всегда «случайно» оказывается неверной (как ни странно, всегда больше, чем сумма, о которой договаривались). Жертву просят вернуть разницу. Позже оказывается, что чек недействителен, дом так и не продан, а переведенные жертвой деньги потеряны.

## КИБЕРПРЕСТУПНОСТЬ, ЕЕ КЛАССИФИКАЦИЯ И БОРЬБА С НЕЙ

**Киберпреступность** не знает государственных границ. По некоторым данным, в мире работают более 40 млн киберпреступников. Примерный ущерб от их действий оценивается в 500 млрд долл. При этом количество вирусных атак в мире увеличивается на 3% в месяц, атак на веб-сервисы — на 2,5%, а число краж денег с различных устройств или электронных кошельков — на 3,5%.

Согласно Европейской конвенции по киберпреступлениям (преступлениям в киберпространстве) (см. Приложение 4), компьютерные преступления можно разделить на четыре типа:

- **незаконный доступ;**
- **незаконный перехват;**
- **вмешательство в данные;**
- **вмешательство в систему.**

Остальные преступления связаны с компьютером либо совершаются с помощью компьютера:

- преступления, связанные с нарушением **авторских** и **смежных прав**;

- действия, в которых компьютеры используются как орудия преступления (электронные хищения, мошенничества);

- преступления, в которых компьютеры играют роль интеллектуальных средств (размещение в сети Интернет детской порнографии; информации, разжигающей национальную, расовую, религиозную вражду).

Компьютерные мошенничества, кражи и вымогательства не являются новыми видами противоправных деяний, их составы включены в национальное уголовное законодательство. Однако киберпреступления зачастую выходят за рамки обычных составов, не признают государственных границ, а кроме того, их виртуальный характер позволяет быстро уничтожить следы, что значительно затрудняет поиск преступника.

В 2000 г. на X Конгрессе ООН была принята следующая классификация **киберпреступлений** (схема 1).

*Схема 1*

Взаимный дефицит доверия между государствами мешает работе по созданию эффективных международных механизмов по борьбе с киберпреступностью.

В настоящее время фактически отсутствует механизм межгосударственного расследования киберпреступлений, а противодействие им на уровне национальных законов осложняется тем, что зачастую организаторы атаки, а также серверы, на которых расположено вредоносное программное обеспечение, находятся в разных странах. В глобальной системе цифровых отношений обеспечить безопасность силами отдельно взятого государства невозможно.

Одним из серьезных шагов, направленных на урегулирование этой проблемы, явилось принятие в Будапеште 23 ноября 2001 г. Европейской конвенции по киберпреступлениям. Однако Конвенцию ратифицировало только 53 страны. Остальные, в том числе и Россия, которая готовит альтернативный вариант Конвенции, не ратифицировали.

Этот документ стал первым международным соглашением по юридическим и процедурным аспектам расследования и криминального преследования киберпреступлений. Им предусмотрены скоординированные действия на национальном и межгосударственном уровнях по пресечению несанкционированного вмешательства в работу компьютерных систем, незаконного перехвата данных и вмешательства в компьютерные системы.

# КИБЕРБЕЗОПАСНОСТЬ

## ХАРАКТЕРИСТИКА КИБЕРБЕЗОПАСНОСТИ

Компьютерная безопасность **(кибербезопасность)** — это один из разделов информационной безопасности, характеризующий невозможность возникновения ущерба от всех заранее выявленных и изученных источников отказов устройства при определенных условиях функционирования на заданном временном отрезке. Предполагает использование ряда мер, обеспечивающих конфиденциальность, целостность, но в то же время и доступность информации.

Современное общество зависимо от информационных систем, поэтому компьютерная безопасность в наши дни становится все более и более популярной.

Кибербезопасность включает в себя изучение процессов формирования, развития и функционирования различных киберобъектов для выявления возможных источников киберопасности, образующихся при этом.

Новые угрозы информационной безопасности характеризуются приставкой «кибер».

В законодательстве Российской Федерации на данный момент понятия **«киберпространство»** и «кибербезопасность» отсутствуют. Несмотря на это, кибертерминологию необходимо учитывать, так как вопросы кибербезопасности прочно вошли в международные сообщества и Международной организацией по стандартизации выпущен стандарт ISO/MEC 27032:2012 «Информационные технологии. Методы обеспечения безопасности. Руководящие указания по кибербезопасности».

Самые популярные меры, применяемые для защиты от киберугроз в мире и России, — антивирусная защита, клиентские межсетевые экраны, установка об-

новлений (в том числе и устраняющих уязвимости в программном обеспечении) и резервное копирование данных.

В настоящее время мировые затраты на обеспечение безопасности корпоративной сети в год составляют в среднем 8000 долл. США для малого бизнеса, 80 000 долл. США для среднего бизнеса и 3,2 млн долл. США для крупных корпораций. Но этого явно недостаточно.

В России ситуация отличается в худшую сторону — объема вкладываемых средств не хватает не только на финансирование мероприятий по кибербезопасности, но и на подготовку персонала. Большинство российских **IT-специалистов** считают уровень инвестиций в информационную безопасность недостаточным: 95% опрошенных считают, что инвестиции нужно увеличить на 25% и более.

Однако зачастую распределение финансов в компаниях осуществляется без учета важности вопросов информационной безопасности. 63% представителей компаний считают, что их руководство придает проблеме защиты корпоративных сетей недостаточное значение. В России эта проблема стоит более остро — 73% принявших участие в опросе думают, что их руководители должны проявлять больший интерес к вопросам IT-безопасности. 44% российских компаний считают киберугрозы одним из главных бизнес-рисков в будущем.

## ЦЕЛИ СИСТЕМЫ КИБЕРБЕЗОПАСНОСТИ

Главная цель системы кибербезопасности — защита информации, как хранящейся, так и передаваемой, предназначенной для обмена. В рамках обеспечения кибербезопасности могут быть приняты контрмеры:

- контроль доступа к данным;
- обучение персонала;
- соответствующая отчетность и аудит;
- оценка **киберрисков**;

• тестирование на возможность проникновения вредоносных программ.

Так как личные данные практически любого из нас доверены информационным системам, социальным сетям, мобильным приложениям, цифровым устройствам, знать основы кибербезопасности необходимо каждому.

В современном мире экономика и Интернет тесно взаимосвязаны. Если электрическая система выйдет из строя и выключится Интернет, то рухнет экономика.

С ростом цифровой экономики увеличивается и количество киберугроз. Затраты глобальной экономики на борьбу с киберпреступностью составляют миллиарды долларов ежегодно.

Сфера кибербезопасности должна постоянно совершенствоваться, опережая киберпреступников.

Для развития цифровой экономики в нашей стране необходимо готовить специалистов, учить население пользоваться компьютерными технологиями.

Необходимо, чтобы уроки цифровой грамотности были включены в обязательную школьную программу и стали регулярными. Проводимые сейчас уроки носят периодический и точечный характер, что, конечно, не позволяет говорить о повышении цифровой грамотности всего населения России. В развитых же европейских странах (к примеру, в Великобритании) сегодня обучение цифровой грамотности проводится уже со школьной скамьи. В частности, у юных граждан формируют навыки, которые в будущем помогут защитить их организацию от сетевых хакерских атак, идет обсуждение с учениками актуальных проблем кибербезопасности, обучение их самостоятельному поиску пути решения этих проблем. Обучение проводится в форме как онлайн-уроков, так и внеклассных занятий.

# ДЕТИ И ИНТЕРНЕТ

Мы живем в эпоху постоянного информационного потока. Интернет вводит для нас новые понятия и стандарты.

Постепенно дети становятся частью виртуальной среды, оказывающей огромное влияние на их поведение, образование и социальную адаптивность.

По результатам исследования фонда «Общественное мнение», 96% детей в возрасте от 10 до 17 лет пользуются Интернетом и 51% из них не знают об опасностях в сети. 52% детей выходят в Интернет прежде всего для общения в социальных сетях, где оставляют данные о своем телефоне (46%), о домашнем адресе (36%), а также личные фото (51%).

Киберпреступники умело манипулируют сознанием ребенка, внушают ему чувства безнаказанности и недосягаемости, вовлекают в преступные группировки и заставляют выполнять преступные действия.

В последнее время самым страшным и необратимым процессом воздействия на детей стало массовое вовлечение их в суицидальные группы, в которых романтизируется смерть, популяризируется уход из жизни.

Преступники воздействуют на ребенка не только путем прямого контакта в переписке в социальных сетях, но и предлагая посмотреть видео, фотографии, поучаствовать в обсуждении фильмов. Также детям могут предлагать определенные онлайн-книги, рекомендации по прочтению литературы и прослушиванию музыки, вовлекать их в разные игровые сообщества, виртуальные клубы по интересам в зависимости от наклонностей ребенка. Тем самым преступники устанавливают круг интересов ребенка, получают данные о его личной жизни и могут влиять на его психику.

## БЕЗОПАСНОСТЬ ДЕТЕЙ В ИНТЕРНЕТЕ

Безопасность детей в Интернете — это главная задача родителей и педагогов, которая должна решаться постоянно.

Федеральный закон от 29 декабря 2010 г. № 436-ФЗ «О защите детей от информации, причиняющей вред их здоровью и развитию» устанавливает правила, обеспечивающие защищенность детей от ненужной им информации, в том числе распространяемой в сети Интернет.

Однако всего предусмотреть нельзя. Нет никакой гарантии, что ребенок с подсказки сверстников или телевизионной рекламы не зайдет на запрещенный ему **интернет-сервис** (схема 2).

С помощью Интернета любой человек может познакомиться с ребенком, например под видом симпатичной девушки, и назначить ему свидание. Ребенок приходит на место встречи, а к нему вместо девушки подходит мужчина, представляется отцом девушки и предлагает отвезти его к ней, так как она якобы заболела. Что может произойти далее, не знает никто. Необходимо научить ребенка не доверять незнакомым людям.

В Интернете много мошенников, и им легче подобраться к детям. Есть много способов обмануть ребенка. Например, ребенка просят ввести номер телефона, потом ему приходит сообщение о выигрыше крупной суммы денег. Чтобы получить выигрыш, мошенники просят ребенка отправить смс-сообщение со своего телефона на другой номер. В результате с мобильного счета списываются все деньги.

Как обезопасить ребенка и что необходимо предпринять? В Интернете существуют и довольно успешно работают программы для родительского контроля. Именно с их помощью можно надежно защитить детей от доступа на запрещенные для них сайты. Рассмотрим некоторые из них.

- Программа **«KinderGate Родительский Контроль»** блокирует сайты для взрослых, есть настройки для ограничения доступа к игровым сайтам, сайтам с пропагандой насилия или наркотиков. Можно установить

*Схема 2*

**ОСНОВНЫЕ НЕБЕЗОПАСНЫЕ ДЛЯ ДЕТЕЙ ИНТЕРНЕТ-СЕРВИСЫ**

Сервисы, пропагандирующие нездоровые сексуальные отношения (секс за деньги, разные извращения)

Сервисы, распространяющие информацию о запрещенных вещах и понятиях (терроризм, сектантство, фашизм)

Сервисы, предлагающие знакомство. Они вовлекают ребенка в виртуальный мир. У него в сети возникает дружба с большим количеством людей, он там отлично общается. А в реальности у ребенка могут быть проблемы в общении со сверстниками

Сервисы с азартными играми. Они обещают большие деньги за короткий срок. А ведь ребенку гораздо сложнее устоять перед таким соблазном, чем взрослым. Под влиянием жажды выигрыша ребенок может начать растрачивать родительские деньги

Сервисы с онлайн-играми. Во многих играх присутствуют насилие, убийства. Кроме того, игры начинают заменять реальный мир, ребенку все тяжелее выходить из игры, особенно если он чувствовал себя настоящим героем в игре и у него там много друзей

расписание, когда ребенок сможет находиться в Интернете. Можно увидеть, на какие сайты он заходит.

- Детский интернет-фильтр **«КиберПапа»** позволяет включить фильтр, чтобы ребенок заходил только на

детские сайты, которые тщательно проверены. Выключить его смогут только родители, зная пароль.

- Программа **«КиберМама»** позволяет создавать расписание, когда ребенок может находиться в сети. Все это контролируется. Также можно заблокировать доступ в Интернет.

- Детский Интернет **«Гогуль»**. В этом браузере есть свои детские сайты. Здесь составляется время, когда ребенок может находиться в Интернете. Можно ограничить посещение Интернета. Родители получают полный отчет, на каких сайтах были их дети.

- Программа **NetKids** позволяет родителям контролировать все сайты, которые посещает их ребенок, и блокировать опасные.

- Программа **KidsControl** позволяет установить ограничение доступа к сомнительным ресурсам, контролировать время нахождения ребенка в Интернете, т. е. задать расписание работы.

Дети очень любознательны, и, оставаясь дома без контроля родителей, ребенок обязательно проявит интерес к компьютеру: как им управлять, как войти в Интернет и найти там свои любимые мультфильмы. С этого момента проблема безопасности детей в Интернете становится весьма актуальной, а ее решение — неотложной задачей.

Поэтому именно родители и педагоги, а не сверстники обязаны показать своему ребенку, как безопасно войти в Интернет и что необходимо сделать для того, чтобы начать работу с требуемым ресурсом.

Ребенок легко улавливает смысл и последовательность действий, а затем, во время отсутствия родителей, он обязательно применит на практике полученные знания.

Конечно, родители испытывают гордость от того, что ребенок может самостоятельно осуществлять вход в сеть и воспроизводить мультимедийный контент, и радуются, что это экономит их время. Но эта радость и гордость будут недолгими, если не принять во внимание, что информационная безопасность детей в Интер-

нете на сегодняшний день — довольно серьезная проблема, так как, по сути, Всемирная паутина невероятно опасна для ребенка. И у родителей есть все основания переживать за своего ребенка, когда их нет рядом, а он в это время проводит интернет-сессию.

## ПРИЗНАКИ НЕГАТИВНОГО ВОЗДЕЙСТВИЯ ИНТЕРНЕТА НА РЕБЕНКА

Зачастую педагоги и родители считают, что при правильном воспитании, хорошем социальном статусе семьи и школы, достаточном благосостоянии, избытке внимания и понимания между детьми, педагогами и родителями беда не придет, что ребенок застрахован от негативного воздействия Интернета.

Это не так! Необходимо постоянно помнить и учитывать, что в социальных сетях по отработанной схеме детям преподносится информация, формирующая у них деструктивное восприятие мира и окружения независимо от его психологического настроя. Взрослым для предотвращения возможного негативного влияния на ребенка со стороны Интернета следует соблюдать определенные правила поведения, выработать правила контроля потока информации и воспитывать культуру получения ее ребенком.

Необходимо постоянно анализировать личные страницы детей в социальных сетях. Первое, на что стоит обратить внимание, — псевдоним ребенка, **аватар**, открытость (закрытость) профиля, группы (сообщества), видеозаписи, фотографии и «друзья». Если профиль закрыт для просмотра, нужно попытаться выяснить причину, а также предложить показать его содержимое. Излишняя анонимность любого пользователя в Интернете имеет веские причины. Открытый профиль ребенка в сети тоже небезопасен. Из него киберпреступники получают практически всю нужную им информацию и активно ею пользуются.

Важно знать признаки, по которым можно определить, не попал ли ребенок под влияние киберпреступников:

• в сохраненных картинках ребенка появляются изображения из групп, в которых пропагандируются вседозволенность, критика семьи и школы, традиций и праздников, курение, наркотики, нетрадиционные половые взаимоотношения;

• в своих изображениях, публикуемых на страницах социальных сетей, дети размещают фотографии самоунижения, оскорбления себя в разных и порой даже жестоких формах, вплоть до нанесения себе травм;

• на странице ребенка сохранены фотографии китов, медуз, кошек, бабочек, единорогов, съемки с высоты, крыш и чердаков;

• размещены стихотворения поэтов, афоризмы писателей, пропагандирующих суицид и эвтаназию;

• в своих комментариях ребенок поддерживает все это, делится с друзьями.

К внешним признакам воздействия на ребенка киберпреступников можно отнести:

• неоправданное желание похудеть, вступление в группы анорексии, сохранение фотографий худых девушек и юношей и, наоборот, размещение изображений, критикующих полных людей в оскорбительных формах;

• чрезмерное потребление кофе, нарушение сна, ранний утренний подъем;

• долгое времяпрепровождение за компьютером, планшетом, с мобильным телефоном, постоянный обмен сообщениями;

• предпочтение одежды преимущественно черных тонов, возможно с символикой, пропагандирующей смерть;

• рисование на руках планет, сайентистских, масонских знаков, перевернутых крестов, сатанинских звезд и различных символов, побуждение сделать татуировки;

• перекрывание лица на фотографиях руками или закрытие деталями одежды, демонстрация на фотографиях безымянного пальца;

- копирование на страницы музыки с откровенной символикой мартинизма, сатанизма и даже фашизма;

- скрывание от родителей и близких внутренних переживаний;

- просмотр и обсуждение сериалов мистической направленности, со сценами жестокости, насилия;

- установление паролей, скрытие информации на всех девайсах, использование графического ключа для входа, постоянная очистка используемых браузеров, корзины;

- выбривание девушками височной части головы, окрашивание волос в яркие зеленые, красные, синие цвета;

- сохранение различных **аниме**, в том числе порнографического характера;

- использование определенного сленга в переписках и сообщениях, оставляемых в общем доступе, к примеру в комментариях;

- размещение и копирование записей музыкальных групп определенной направленности, информации о различных музыкальных направлениях и течениях с использованием символики, пропагандирующей смерть;

- ведение специальных дневников с характерными рисунками и подборками и возможными дальнейшими публикациями в сети;

- желание установить напротив кровати зеркало;

- открытие электронных кошельков и банковских платежных систем;

- установление специальных **браузеров** для анонимного просмотра и входа в глубинный Интернет;

- игры в определенных приложениях, в которых имеются внутренние чаты;

- установление на смартфоны приложений для видео- и аудио-онлайн-трансляции.

## ГЛОБАЛЬНЫЙ ИНТЕРНЕТ: УГРОЗЫ И ДЕЙСТВИЯ РОДИТЕЛЕЙ

Даже не каждый взрослый понимает, чего нужно остерегаться в сети Интернет. Тем не менее ребенок должен быть не только проинформирован о том, какие угрозы существуют, но и понимать, как их избежать в случае возникновения нестандартных ситуаций.

К угрозам относятся:

- опасность заражения компьютера посредством вредоносного программного обеспечения;
- беспрепятственный доступ к нежелательному контенту (содержание интернет-страниц);
- знакомство и общение с другими пользователями сети;
- афиширование конфиденциальных данных;
- осуществление неконтролируемой покупки.

Необходимо обсуждать с ребенком все вышеперечисленные пункты, причем это должно быть не какое-то одноразовое мероприятие, а систематические беседы, которые должны стать семейной традицией.

Ребенок должен знать, что:

- появляющиеся на экране монитора предложения с текстом «Установи это бесплатно» могут быть попыткой злоумышленников установить на ваш компьютер приложение, которое постоянно будет отправлять ваши данные неизвестно куда и неизвестно кому. Объясните, что компьютер может попросту выйти из строя в результате установки в общем-то простой игры;
- нельзя общаться в виртуальной среде с незнакомыми людьми, а также делиться с ними какой-либо информацией, касающейся личных данных;
- нельзя заполнять различного рода анкеты, в которых необходимо указывать свою фамилию, имя и отчество, а в некоторых случаях адрес проживания;
- нельзя указывать номер банковского счета при совершении покупок через Интернет.

Не важно, сколько лет детям, насколько родители уверены в том, что ребенок будет выполнять установленные правила. Доверять ребенку — это прекрасно, но, учитывая «волшебные» возможности Интернета, вовремя отреагировать на неблагоприятную ситуацию родителям помогут доверительные отношения с ребенком. Необходимо быть в курсе его интересов, обращать внимание на малейшее изменение в поведении ребенка.

Для того чтобы более качественно повлиять на воспитание своих детей, родители могут предложить собраться всей семьей и совместно с детьми разработать «семейное соглашение», в котором будут отражены все права и обязанности каждого из домашних, так или иначе использующих компьютер с целью выхода в сеть, в том числе и правила безопасности детей в Интернете.

Дети любят, когда родители считают их взрослыми и учитывают их мнения и пожелания, поэтому семейное соглашение будет принято со всей доступной детскому пониманию серьезностью. Такое семейное мероприятие по интернет-безопасности позволит ребенку проникнуться уважением к оказанному ему доверию, и он будет стараться оправдать это доверие.

Необходимо разработать и включить в семейное соглашение следующие положения:

- какие именно интернет-сайты могут посещать дети и с какой целью;
- сколько времени и как часто ребенок может находиться в Сети;
- какие действия необходимо предпринять в случае, если что-то пошло не так;
- как защитить личные данные;
- вежливость и принципы поведения в Интернете;
- какие правила безопасности детей в Интернете существуют.

Все эти пункты должны иметь четкую и однозначно понимаемую формулировку. Периодически что-то придется корректировать, вносить поправки. Однако суть

соглашения должна оставаться неизменной — безоговорочное выполнение всеми взятых на себя обязательств.

## ПАМЯТКИ ДЛЯ РОДИТЕЛЕЙ

Ведущий вид деятельности у школьников — это общение со сверстниками, и не стоит им запрещать общаться в социальных сетях. Родителям необходимо помнить о том, что дети растут и их интересы постоянно меняются, и постараться сделать так, чтобы в жизни ребенка было больше положительных и интересных событий, чем тех, которые он переживает в виртуальном мире. Тогда Интернет станет подспорьем в учебе, вспомогательным средством поиска информации и общения, а не способом ухода от реальности и бегства от проблем.

Ниже приведены общие рекомендации для родителей.

- Установите программу «Родительский Контроль», чтобы всегда быть в курсе того, какие сайты посещает ребенок.
- Вместе с ребенком разработайте домашние правила посещения Интернета и требуйте их выполнения.
- Требуйте от ребенка соблюдения временны́х норм нахождения в Интернете.
- Компьютер с подключенным Интернетом должен находиться в общей комнате под контролем родителей.
- Используйте программы блокирования нежелательных сайтов.
- Создайте семейный электронный ящик, не разрешайте ребенку иметь свой адрес электронной почты.
- Приучите ребенка советоваться с вами при размещении в социальных сетях информации о себе или о семье.
- Не разрешайте ребенку загружать без вашего согласия файлы, музыку, игры, фото.
- Не разрешайте ребенку использовать службы мгновенного обмена сообщениями.

- Ребенок может посещать только проверенные сайты.

- Почаще разговаривайте с ребенком о его друзьях в социальных сетях и в жизни.

- Не избегайте обсуждать с ребенком вопросы личной гигиены и половой жизни. Беседуйте на эти темы. В противном случае ребенок найдет ответы (не всегда правильные) в Интернете.

- Постарайтесь приучить ребенка смело и открыто рассказывать вам обо всех проблемах, угрозах или тревогах при общении с друзьями в повседневной жизни и в Интернете.

## Как безопасно пользоваться смартфоном или планшетом

Смартфоны и планшеты представляют собой небольшие стационарные компьютеры. Опасность в том, что программного обеспечения по их защите очень мало. Вирусы и вредоносные программы очень быстро могут вывести смартфон или планшет из строя.

- В Интернете нет ничего, что является по-настоящему бесплатным. В предложенном бесплатном контенте чаще всего скрыты платные услуги.

- Прежде чем отправить смс-сообщение, фото или видео, необходимо знать, кому они попадут, не используют ли их компьютерные мошенники.

- Необходимо почаще обновлять операционную систему смартфона или планшета.

- Нужно использовать только лицензионные антивирусные программы для мобильных телефонов.

- Для безопасности смартфона или планшета приложения можно загружать только из известного источника. Это позволит избежать вредоносного программного обеспечения.

- После посещения любого сайта, в котором была введена личная информация, нужно зайти в настройки браузера и удалить cookies.

• Периодически нужно проверять, какие платные услуги активированы на номере мобильного телефона.

• Номер своего мобильного телефона, а также адрес электронной почты можно давать только знакомым людям, которым доверяешь.

• Следует регулярно проверять Bluetooth: он должен быть выключен, когда им не пользуются.

### Как защищаться от компьютерных вирусов

• Использовать современные операционные системы, имеющие большой уровень защиты от вредоносных программ и вирусов.

• Включать режим автоматического обновления своей операционной системы, скачивать программные обновления только с официального сайта разработчика операционной системы. Устанавливать **патчи**.

• Работать на своем компьютере как пользователь, а не администратор. В этом случае большинство вредоносных программ не смогут инсталлироваться на персональном компьютере.

• Использовать антивирусные программные продукты известных разработчиков с автоматическим обновлением баз.

• Посторонние лица не должны иметь доступ к вашему смартфону или планшету.

• Перед использованием внешних носителей следует проверять их на наличие вирусов.

• Прежде чем открывать подозрительные компьютерные файлы, нужно проверить, из каких источников они поступили. Если источник ненадежен, файл не открывать и удалить его.

### Как безопасно пользоваться сетью Wi-Fi

Многие считают, что бесплатный доступ в Интернет через сети Wi-Fi в кафе, отелях и аэропортах является безопасным. Это не так.

- Нельзя передавать свою личную информацию через общедоступные сети Wi-Fi: вводить свои пароли доступа, логины и какие-то номера.

- При работе через Wi-Fi нужно использовать **брандмауэр** и систематически обновлять антивирусные программы.

- При использовании Wi-Fi нельзя подключать функцию «Общий доступ к файлам и принтерам».

- Следует использовать только защищенное соединение через HTTPS, а не HTTP, т. е. при наборе веб-адреса вводить именно «https://».

- В мобильном телефоне нужно отключить функцию «Подключение к **Wi-Fi** автоматически»; не допускать автоматического подключения устройства к сетям Wi-Fi без вашего согласия.

### Как вести себя в социальных сетях

Социальные сети так прочно вошли в нашу жизнь, что многие люди работают и общаются там постоянно. Например, в Facebook уже зарегистрирована седьмая часть жителей планеты, а это около 1 млрд человек. Помните, что информация, размещенная в социальных сетях, может быть найдена и использована кем угодно, в том числе с недобрыми намерениями.

- Следует ограничить список друзей, среди них не должно быть случайных и незнакомых людей.

- Не указывать в социальных сетях пароли, телефоны, адреса, дату рождения, другую личную информацию и информацию о своей семье.

- Прежде чем что-то опубликовать, написать и загрузить, необходимо подумать, нужно ли, чтобы это видели другие пользователи.

- При общении с незнакомыми людьми не использовать свое реальное имя и другую личную информацию, не называть место жительства, место учебы или работы.

- Не размещать в Интернете фотографии, по которым можно определить ваше местоположение.

• При регистрации в социальной сети использовать только сложные пароли, состоящие из букв и цифр и с количеством знаков не менее 8.

• Для социальной сети, почты и других сайтов использовать разные пароли.

### Как безопасно пользоваться электронной почтой

• Выбирать только проверенный почтовый сервис.

• Не указывать в почте личную информацию. Придумать себе какой-либо позывной, например «футболист2018@».

• Выбирать сложный пароль.

• Использовать несколько почтовых ящиков, один из которых — только для частной переписки.

• Никогда не открывать в почтовом ящике сомнительные вложения, удалять их без просмотра.

• Перед закрытием почтового ящика обязательно нажать кнопку «Выйти».

### Как вести себя в случае кибербуллинга

• Если через Интернет в ваш адрес поступили угрозы или оскорбления, не нужно отвечать аналогично. Следует посоветоваться с учителем или родителями, как себя вести.

• Постоянно поддерживать свою киберрепутацию, даже если вы находитесь под вымышленным именем. Существует множество способов определить, кто стоит за анонимным аккаунтом.

• Не хулиганить в Интернете: он запоминает все действия и сохраняет их. Удалить эту информацию затруднительно.

• Помнить, что простая единичная агрессия, если на нее не обращать внимания, прекращается на начальной стадии.

• Блокировать агрессора. В программах обмена сообщениями, в социальных сетях есть возможность блокировки отправки сообщений с определенных адресов.

## Основные правила безопасности в онлайн-играх

Онлайн-игры — это красочные, захватывающие развлечения, объединяющие сотни тысяч человек по всему миру. В процессе игры игроки получают удовольствие, имеют возможность общаться, совместно выполняют задания, ведут битвы. Они покупают диски, оплачивают абонемент или приобретают какие-то опции.

Все полученные разработчиками средства идут на поддержание и развитие игры, а также обеспечение безопасности. В играх стоит опасаться кражи вашего пароля, на котором основана система авторизации большинства игр.

- Если другой игрок ведет себя плохо или создает вам неприятности, следует заблокировать его в списке игроков.
- Можно пожаловаться администраторам игры на плохое поведение игрока, желательно приложить какие-то доказательства в виде скринов.
- Нельзя указывать свою личную информацию в профайле игры.
- Нужно уважать других участников игры.
- Не устанавливать неофициальные патчи.
- Использовать сложные и разные пароли.
- Даже во время игры не стоит отключать антивирус; пока вы играете, компьютер могут заразить.

## Как вести себя в случае фишинга

Воры и мошенники существовали всегда. Кража денег и документов для нас неудивительна. Но с появлением Интернета воры и мошенники активно перемещаются в Сеть. Так появилась новая угроза: интернет-мошенничество, или фишинг; главная цель мошенников — получение логинов и паролей, использующихся в дальнейшем для кражи денег и документов.

- Необходимо следить за своим аккаунтом. Если вы подозреваете, что ваша страничка была взломана, то необходимо заблокировать ее и сообщить об этом администраторам ресурса.

- Использовать только безопасные веб-сайты.
- Использовать сложные и разные пароли.
- Если страничку взломали, нужно срочно предупредить всех друзей в социальной сети об этом и о том, что от твоего имени возможна рассылка спама и ссылок на фишинговые сайты.
- Установить надежный пароль (PIN) на мобильный телефон.
- Отключить сохранение пароля в браузере.
- Не открывать подозрительные файлы и другие вложения в письмах, даже если они пришли от друзей, лучше уточнить у них, отправляли ли они эти файлы.

### Как соблюдать цифровую репутацию

Сетевой имидж пользователя формируется из информации о нем в Интернете. Данные о месте жительства, учебы, о финансовом положении, особенностях характера и рассказы о близких — все это накапливается и хранится в сети. Удалить эти сведения до конца невозможно.

Многие пользователи легкомысленно относятся к публикации личной информации в Интернете, не понимая возможных последствий. Порой невозможно догадаться о том, что фотография, размещенная 5 лет назад, стала причиной отказа принять вас на работу или учебу.

Комментарии, фотографии, видео и другие действия пользователя могут не исчезнуть даже после их удаления. Ведь неизвестно, кто сохранил эту информацию, попала ли она в поисковые системы и сохранилась ли, а главное — что подумают о человеке другие люди, которые найдут и увидят это. Найти информацию много лет спустя сможет любой — как из добрых побуждений, так и с намерением причинить вред.

- Прежде чем что-то публиковать и передавать у себя в блоге или в социальной сети, надо как следует подумать.

• В настройках профиля лучше установить ограничения на просмотр своего профиля и его содержимого и сделать его видимым только для друзей.

• Не следует размещать и указывать информацию, которая может кого-либо оскорблять или обижать.

## Авторское право

Современные школьники — активные пользователи цифрового пространства. Однако далеко не все знают, что пользование возможностями цифрового мира требует соблюдения прав на интеллектуальную собственность.

Согласно статье 1259 Гражданского кодекса Российской Федерации, к объектам авторских прав относятся:

• произведения науки, литературы и искусства: литературные, музыкальные, сценарные, хореографические, аудиовизуальные произведения; произведения живописи, скульптуры, графики, дизайна; произведения архитектуры, градостроительства и садово-паркового искусства, в том числе в виде проектов, чертежей, изображений и макетов; фотографии, географические и другие карты, планы, программы для ЭВМ и интернет-сайты;

• производные произведения, представляющие собой переработки другого произведения (например, экранизации, аранжировки, инсценировки, переводы);

• составные произведения, представляющие собой по подбору или расположению материала результат творческого труда.

Если вы поздравили своего друга с днем рождения, разместив в Интернете сочиненное вами стихотворение, то вы являетесь его автором, и никто не имеет права выдать это стихотворение за свое, что-то изменить, добавить, исправить в нем. Именно вам по закону принадлежат исключительное право на произведение, право авторства, право на имя, право на неприкосновенность произведения, право на его обнародование.

Из статьи 1270 Гражданского кодекса Российской Федерации следует, что использованием произведения

считается его воспроизведение, т. е. изготовление одного и более экземпляров произведения или его части в любой материальной форме, в том числе в форме звуко- или видеозаписи; его распространение и публичный показ. Сюда же относится импорт оригинала или экземпляров произведения для распространения в нашей стране, выдача произведения напрокат, его публичное исполнение, передача по радио и телевидению, перевод или другая переработка.

Срок действия авторского права — в течение всей жизни автора плюс 70 лет после его смерти, считая с 1 января года, следующего за годом смерти автора. После смерти автора его правами распоряжаются наследники или правопреемники, и в течение 70 лет необходимо испрашивать их согласие на использование произведения. После указанного срока оно становится общественным достоянием и может свободно использоваться кем угодно, в том числе в Интернете, без чьего-либо разрешения и без выплаты вознаграждения.

Объектами авторского права не являются:

- официальные документы государственных и муниципальных органов власти, международных организаций, государственные символы и знаки (флаги, гербы, ордена, деньги, марки);

- произведения народного творчества, не имеющие конкретных авторов;

- сообщения чисто информационного характера (новости дня, программы телепередач, расписания транспорта, прогнозы погоды и т. д.).

В Интернете большинство информационных ресурсов предоставляются для свободного доступа. Помещая какую-то информацию в Интернете, вы ее обнародуете для всех. Посмотреть ее может любой пользователь, но это не означает свободного использования.

Разместив на своем сайте чужие произведения без разрешения авторов, пользователь нарушает требования закона.

Без согласия автора или иного правообладателя и без выплаты гонорара в соответствии со статьей 1273

Гражданского кодекса Российской Федерации допускается:

- воспроизведение обнародованного произведения исключительно в личных целях, для себя (в том числе изготовление одного или нескольких экземпляров произведения или его части в любой материальной форме, его скачивание на жесткий диск своего компьютера);

- скачивание книг из Интернета для личного чтения и чтения членами своей семьи (нельзя размножать эту копию для продажи!).

Нельзя:

- копировать произведения архитектуры — здания и другие сооружения;

- копировать целиком базы данных или их существенные части;

- копировать компьютерные программы;

- полностью репродуцировать книги и ноты, т. е. факсимильно их копировать с помощью любых технических средств;

- делать видеозаписи аудиовизуального произведения для демонстрации кому-либо, кроме вашей семьи.

Без согласия автора или иного правообладателя и без выплаты вознаграждения в соответствии со статьей 1274 Гражданского кодекса Российской Федерации можно:

- цитировать его труд в оригинале и в переводе в научных, полемических, критических, информационных, учебных целях; использовать произведения и отрывки из них как иллюстрации в учебном издании, радио- и телепередачах или в своем блоге, но обязательно указать, кто автор и откуда взята цитата;

- воспроизводить в периодической печати, читать по радио или телевидению статьи по различным актуальным вопросам, опубликованные в печатной периодике, если это не было специально запрещено автором или иным правообладателем;

- воспроизводить в периодической печати, сообщать в радио- и телепередачах и Интернете публично произнесенные политические речи, обращения, доклады и т. п. в объеме, необходимом для информирования читателей, слушателей и зрителей;

- вести репортажи с выставок, концертов, конкурсов исполнителей и других культурных событий;

- ставить своими силами спектакль по пьесе автора в школе, больнице или тюрьме.

В российском законодательстве существует понятие «смежные права». Субъектами смежных прав являются исполнители, производители фонограмм, организации эфирного и кабельного вещания, которые заключили договор с автором, разрешившим им использовать свое произведение.

Смежные права тоже охраняются. В Уголовном кодексе Российской Федерации статья 146 «Нарушение авторских и смежных прав» предусматривает уголовную ответственность за присвоение авторства (плагиат); приобретение, хранение, перевозку контрафактных экземпляров произведений или фонограмм в целях сбыта, в том числе программного обеспечения, компьютерных игр, и наказание лишением свободы на срок до шести лет или возмещением материального ущерба.

В Интернете по объективным причинам сложно добиться максимального соблюдения авторского права. Тем не менее, согласно Федеральному закону № 149-ФЗ от 27 июля 2006 г. «Об информации, информационных технологиях и о защите информации», правообладатель, обнаружив сайт, на котором незаконно размещена информация, содержащая объекты его авторских и (или) смежных прав, может направить владельцу этого сайта заявление о нарушении своих прав. Владелец информационного ресурса обязан рассмотреть претензию в течение 24 часов и удалить незаконно размещенную информацию. Если же реакции на заявление нет, правообладатель может потребовать заблокировать сайт, обратившись через суд в Роскомнадзор.

# МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ ДЛЯ УЧИТЕЛЕЙ

Современные средства коммуникации стали неотъемлемой частью образовательного процесса в школе: педагоги активно используют компьютерные технологии и информационную поддержку.

Число пользователей Интернета с каждым днем неуклонно растет (причем самыми активными являются именно школьники), и становится все более актуальной проблема обеспечения информационной безопасности школьников в интернет-среде.

В связи с этим встает вопрос об обеспечении информационной безопасности (в том числе и психологической) школьников при работе в Интернете. Решать этот вопрос необходимо комплексно: обучать школьников компьютерной грамотности и в то же время формировать у них навыки соблюдения правил информационной (электронной) безопасности.

В процесс формирования безопасного поведения школьников в Интернете должны быть вовлечены все участники образовательного процесса: администрация школы, классные руководители, преподаватели информационных технологий, психологи, школьники и их родители.

Информационную безопасность школьников можно формировать на уроках информатики, основ безопасности жизнедеятельности, гражданского права, а также в рамках внеурочной деятельности.

Главная задача педагога — научить школьников правильно оценивать степень угрозы информации, которую они воспринимают или передают через Интернет.

При организации учебного процесса с помощью компьютерных технологий учитель должен рассказать

школьникам о рисках, возникающих при использовании Интернета:

- **контентных**, связанных с настройкой браузера и скачивания файлов;

- **электронных**, связанных с вредоносными программами, которые могут быть найдены и скачаны из Интернета;

- **коммуникационных**, связанных с взаимодействием и общением школьника с другими людьми в социальных сетях, с помощью мессенджера. Необходимо разъяснить школьникам, что при общении в сети Интернет можно столкнуться с преступниками и мошенниками. Отдельно необходимо объяснить опасность предоставления персональных данных на страницах в социальных сетях;

- **потребительских**, связанных с информацией, музыкой и покупкой вещей в Интернете. Необходимо предупредить школьников о том, что если для использования или покупки той или иной информации требуется оплата через мобильный телефон, то необходимо, во-первых, посоветоваться со взрослыми, а во-вторых, проверить этот номер в Интернете — безопасно ли отправлять на него смс-собщение. Сделать это можно на специальных сайтах: http://smsnumbers.ru, http://smscost.ru, http://smswm.ru;

- **психологических**, связанных с возникновением компьютерной и интернет-зависимости, психологической незащищенности.

Задача учителя — предостеречь школьников от посещения потенциально опасных сайтов:

- **суицид-сайтов**, на которых представлена информация о способах расстаться с жизнью;

- **сайтов-форумов** потенциальных самоубийц;

- **наркосайтов (**Интернет пестрит новостями о «пользе» употребления наркотиков, рецептами и советами по их изготовлению);

- **сайтов, разжигающих национальную рознь и расовое неприятие** (экстремизм, национализм, фашизм);
- **сайтов порнографической направленности**;
- **сайтов знакомств** (виртуальное общение разрушает коммуникативные навыки школьников, их способность к реальному общению);
- **сайтов сект** (виртуальный собеседник способен отрицательно повлиять на мировоззрение детей).

В образовательном процессе педагог должен демонстрировать только качественные образовательные ресурсы. При изучении раздела или темы необходимо снабдить учеников ссылками на традиционные бумажные и электронные учебники, учебные пособия, энциклопедии, справочники, словари, ресурсы электронных федеральных образовательных коллекций, цифровых хранилищ библиотек и музеев, образовательных сайтов, дидактические материалы педагога. Задача информационной деятельности педагогов и школьников заключается в совместном расширении и систематизации сети используемых информационных образовательных источников.

Организуя учебный процесс с использованием информационных источников Интернета, педагог должен учитывать и возрастные особенности школьников, используя специальные формы и методы обучения: если в 1 классе школьники пользуются преимущественно учебником и рабочей тетрадью, то одиннадцатиклассники в полном объеме используют мировые информационные ресурсы.

Педагог должен помочь школьникам найти дополнительные источники через библиотечные каталоги, поисковые системы Интернета, научить их отбирать и систематизировать полученную информацию. Необходимо научить школьников:

- анализировать информацию с позиции общечеловеческих ценностей;
- отделять факты от субъективных мнений;
- отделять эмоции от фактов;

- рассматривать проблему с разных сторон, а не только с позиции автора;
- устанавливать взаимосвязь явлений;
- связывать разнородные объекты;
- объединять противоположности, стараясь найти дополнительные аспекты рассмотрения проблемы;
- обобщать полученную информацию и делать выводы, принимать решения; оценивать полученную информацию по совокупности проведенного анализа;
- прогнозировать последствия принятого решения.

Этому необходимо обучать школьников в процессе познавательной деятельности по любому предмету школьной программы.

Организуя занятия в рамках внеучебной деятельности, необходимо не только учитывать возрастные особенности школьников, но и применять интересные интерактивные и игровые технологии и упражнения, направленные на развитие навыков безопасного поведения в Интернете. Например:

- для учащихся 1—4 классов провести занятие в интерактивной форме «Полезный и безопасный Интернет»;
- для учащихся 5—9 классов провести неделю «Безопасный Интернет»;
- для учащихся 10—11 классов организовать «Совет интернет-безопасности».

Чтобы педагог мог активно влиять на кибербезопасность каждого школьника индивидуально, необходимо знать уровень его компьютерной грамотности и зависимости, место и роль его родителей в достижении этой цели. Одна из форм изучения этой проблемы — анкетирование школьников и их родителей, а также педагогов. Анкеты разработаны факультетом психологии Московского государственного университета имени М. В. Ломоносова.

## АНКЕТА ДЛЯ ШКОЛЬНИКОВ

**Дорогие друзья!**

Приглашаем вас принять участие в исследовании, посвященном Интернету. Пожалуйста, ответьте на представленные ниже вопросы. Отвечайте не задумываясь — правильных и неправильных ответов нет, а есть разнообразие мнений. Ваше мнение нам очень важно.

**1.** Есть ли у вас дома компьютер, смартфон или планшет?

☐ Да

☐ Нет

**2.** Подключен ли компьютер к сети Интернет?

☐ Да

☐ Нет

**3.** Есть ли у вас в школе Интернет?

☐ Да

☐ Нет

☐ Не знаю

**4.** Пользуетесь ли вы Интернетом в школе?

☐ Да

☐ Нет

**5.** Установлены ли в ваших школьных компьютерах программы, ограничивающие доступ на какие-либо сайты?

☐ Да

☐ Нет

☐ Не знаю

**6.** Как часто вы пользуетесь Интернетом?

☐ 1—2 раза в неделю

☐ 1—2 раза в день

☐ 1 раз в месяц

☐ Я все время в Интернете

☐ Не пользуюсь Интернетом вообще

☐ Другое: _____

**7.** Сколько времени вы проводите в Интернете за один сеанс?

☐ 10—20 минут

☐ 1—3 часа

☐ 5—10 часов

☐ Другое: _____

**8.** Получаете ли вы удовольствие от работы в Интернете?

☐ Никогда

☐ Иногда

☐ Часто

☐ Всегда

**9.** Что вы обычно делаете в Интернете?

| | **Часто** | **Редко** | **Никогда** |
|---|---|---|---|
| Пользуюсь электронной почтой | | | |
| Общаюсь в «ВКонтакте», «Одноклассниках» и других социальных сетях | | | |
| Общаюсь по скайпу | | | |
| Веду виртуальный дневник (блог) | | | |
| Ищу информацию для учебы | | | |
| Ищу информацию для культурного и духовного развития | | | |
| Общаюсь в чатах | | | |
| Скачиваю программы, музыку, фото, видео | | | |
| Слушаю аудиозаписи | | | |
| Смотрю видеозаписи | | | |
| Узнаю о последних событиях и новостях в стране и мире | | | |
| Играю в онлайн-игры | | | |
| Принимаю участие в интернет-акциях, голосовании и др. | | | |
| Просматриваю запрещенные родителями сайты | | | |

Укажите, чем вы еще занимаетесь в Интернете:

_____

_____

_____

**10.** Как вы считаете, есть ли опасности в Интернете?

☐ Да

☐ Иногда

☐ Нет

☐ Не знаю

**11.** Как часто в Интернете вы сталкиваетесь с опасностями?

| | **Часто** | **Редко** | **Никогда** |
|---|---|---|---|
| Вирусы | | | |
| Мошенничество/кражи | | | |
| Преследование, оскорбление и унижение со стороны других пользователей | | | |
| Сексуальные домогательства | | | |
| Неэтичная и навязчивая реклама | | | |
| Порнография | | | |
| Психологическое давление | | | |
| Агрессия | | | |
| Экстремизм | | | |
| Призывы причинить вред себе и/или окружающим | | | |

Укажите, с чем еще вы сталкивались в Интернете:

_____

_____

_____

_____

_____

**12.** Часто ли вы в Интернете сталкиваетесь с информацией, которая раздражает и вызывает неприятные эмоции?

☐ Часто

☐ Редко

☐ Никогда

**13.** Как часто в Интернете вы оставляете малознакомым (едва знакомым) людям свои контактные данные?

| | **Часто** | **Редко** | **Никогда** |
|---|---|---|---|
| Адрес электронной почты | | | |
| Номер мобильного телефона | | | |
| Номер домашнего телефона | | | |
| Домашний адрес | | | |
| Номер школы и класса | | | |
| Свою фотографию и фотографии своих родственников | | | |

**14.** Вы пытаетесь встречаться с людьми, с которыми познакомились в Интернете?

☐ Часто

☐ Редко

☐ Никогда

**15.** Как вы считаете, приносит ли Интернет пользу?

| | **Часто** | **Редко** | **Никогда** |
|---|---|---|---|
| Физическому здоровью | | | |
| Психическому здоровью | | | |
| Морали (нравственности) | | | |
| Культурному уровню | | | |
| Успеваемости в школе | | | |

**16.** Какие сайты Интернета вы посещаете чаще всего?

☐ Игровые

☐ Сайты с музыкой и фильмами

☐ Сайты интернет-знакомств

☐ Сайты для детей

☐ Сайты для взрослых

☐ Другое: _____

**17.** Укажите названия своих любимых сайтов:

_____

_____

_____

_____

**18.** Укажите 5 причин, которые заставляют зайти в Интернет:

_____

_____

_____

_____

**19.** Укажите 5 причин, которые заставляют вас покинуть Интернет:

_____

_____

_____

_____

**20.** Как вы считаете, вредит ли Интернет?

| | **Часто** | **Редко** | **Никогда** |
|---|---|---|---|
| Физическому здоровью | | | |
| Психическому здоровью | | | |
| Морали (нравственности) | | | |
| Культурному уровню | | | |
| Успеваемости в школе | | | |

**21.** Рассказываете ли вы родителям о том, чем занимаетесь в Интернете?

☐ Всегда

☐ Иногда

☐ Редко

☐ Не рассказываю

**22.** Установлены ли на вашем домашнем компьютере программы, ограничивающие вход на какие-либо сайты?

☐ Да

☐ Нет

☐ Не знаю

**23.** Считаете ли вы, что Интернет — это свободное пространство, в котором по своему усмотрению можно делать все, что пожелаешь?

☐ Да

☐ Нет

☐ Не уверен(а)

☐ Считаю, что должны быть правила, регулирующие пользование Интернетом

**24.** Можете ли вы описать какой-либо неприятный, связанный с Интернетом случай, произошедший в вашей школе или с вами лично?

_____

_____

_____

_____

**25.** Как родители относятся к вашей деятельности в Интернете?

☐ Разрешают свободно пользоваться и не ограничивают во времени

☐ Устанавливают временной режим и следят за тем, какие сайты я посещаю

☐ Разрешают заходить в Интернет только в своем присутствии

☐ Запрещают пользоваться Интернетом вообще

☐ Другое: _____

_____

_____

**26.** Какой источник информации для вас сегодня самый главный? Обозначьте цифрами по степени значимости: 1 (самый главный); 2 (занимает по значимости второе место и т. д.).

☐ Учителя

☐ Родители (родственники)

☐ Друзья (одноклассники)

☐ Интернет

☐ Телевидение

☐ Книги

☐ Газеты/журналы

☐ Радио

☐ Другое: _____

**27.** Какие эмоции и чувства вы чаще всего испытываете, находясь в Интернете (укажите не менее трех)?

- ☐ Радость
- ☐ Страх
- ☐ Удивление
- ☐ Печаль
- ☐ Восторг
- ☐ Стыд
- ☐ Доверие
- ☐ Вина
- ☐ Интерес
- ☐ Разочарование
- ☐ Любопытство
- ☐ Уверенность
- ☐ Унижение
- ☐ Счастье
- ☐ Отвращение
- ☐ Удовольствие
- ☐ Обида
- ☐ Надежда
- ☐ Тревога
- ☐ Гнев

☐ Восхищение

☐ Другое: _____

**28.** Оцените уровень опасности.

| | **Очень опасно** | **Опасно** | **Скорее опасно** | **Не знаю** | **Скорее безопасно** | **Безопасно** | **Совершенно безопасно** |
|---|---|---|---|---|---|---|---|
| В стране | | | | | | | |
| В городе | | | | | | | |
| На улице | | | | | | | |
| В школе | | | | | | | |
| В Интернете | | | | | | | |
| Дома | | | | | | | |

**29.** Выскажите свое мнение по ряду вопросов, связанных с использованием Интернета. Если вы согласны с суждением, поставьте знак «+» в графе «Да», если не согласны — «+» в графе «Нет».

| | **Да** | **Нет** |
|---|---|---|
| Вы используете Интернет, чтобы уйти от проблем или избавиться от плохого настроения | | |
| Каждый раз вы проводите в Интернете больше времени, чем планировали | | |
| Вы чувствуете беспокойство или раздражение, когда вас отрывают от Интернета | | |
| Вы думаете об Интернете, когда находитесь вне Сети | | |
| Находясь вне Сети, вы испытываете подавленность или беспокойство | | |
| Вы можете лишиться отношений с кем-либо, перестать ходить в школу из-за Интернета | | |

**30.** По-вашему, Интернет — это _____

_____

_____

_____

_____

Укажите:

- свой возраст: _____
- пол: _____
- класс: _____
- профессию мамы: _____
- профессию папы: _____

**Спасибо за участие!**

## АНКЕТА ДЛЯ РОДИТЕЛЕЙ

**Уважаемые родители!**

Для изучения оценки рисков и опасностей Интернета ответьте на представленные ниже вопросы. Отвечайте не задумываясь — правильных и неправильных ответов нет, а есть разнообразие мнений. Ваше мнение нам очень важно.

**1.** Сколько лет вашим детям? Какого они пола?

| Возраст, лет | Девочка | Мальчик |
|---|---|---|
| Меньше 6 | | |
| 6—7 | | |
| 8—9 | | |
| 10—11 | | |
| 12—13 | | |
| 14—15 | | |
| 16—17 | | |
| У меня нет несовершеннолетних детей (младше 18 лет) | | |

*Если у вас есть дети младше 18 лет, переходите к вопросу 2; если нет — к вопросу 9.*

**2.** Использует ли ваш ребенок Интернет?

☐ Дома

☐ В школе

☐ У друзей дома

☐ Еще у кого-нибудь дома

☐ В интернет-кафе

☐ В библиотеке (другом публичном месте)

☐ Где-нибудь еще

☐ Ребенок не пользуется Интернетом

☐ Затрудняюсь ответить

*Если ребенок пользуется Интернетом, переходите к вопросу 3; если нет — к вопросу 7.*

**3.** Есть ли в вашей семье набор правил пользования ребенком приборами и электронными средствами информации и коммуникации?

☐ Да, для телевизора

☐ Да, для мобильного телефона

☐ Да, для электронных игровых консолей (Playstation, Xbox, GameCube, Gameboy)

☐ Да, для Интернета

☐ Да, для компьютера (помимо Интернета)

☐ Да, это является нормой для ребенка, но не для меня

☐ Нет, никаких правил нет

☐ Затрудняюсь ответить

*Если у вас есть набор правил для ребенка о пользовании Интернетом, переходите к вопросу 4; если нет — к вопросу 5.*

**4.** Какие правила вы устанавливаете для ребенка при пользовании Интернетом?

☐ Нельзя давать личную информацию в Интернете

☐ Есть сайты, на которые ребенок не должен заходить

☐ Ребенок должен рассказать мне, если он находит в Интернете то, что заставило его почувствовать себя неловко

☐ Ребенок не должен использовать грубые (нецензурные) слова в электронных письмах или чатах

☐ Ребенок не должен встречаться с теми, с кем познакомился в Интернете

☐ Ребенок не должен копировать документы, картинки

☐ Ребенок не должен общаться в чатах (с незнакомцами)

☐ Ребенок не должен скачивать музыку, фильмы

☐ Ребенок не должен скачивать программное обеспечение

☐ Устанавливается временной режим, сколько ребенок может находиться в Интернете

☐ Другие правила

☐ Затрудняюсь ответить

**5.** Нужно ли вам больше информации о том, как защитить своего ребенка от нелегального или негативного контента и контакта с людьми в Интернете?

☐ Да

☐ Нет

☐ Затрудняюсь ответить

**6.** Можете ли вы сказать, что ваши дети знают, как поступить в случае, если ситуация, связанная с Интернетом, заставляет их чувствовать себя неловко?

☐ Да

☐ Нет

☐ Затрудняюсь ответить

**7.** Откуда и от кого вы предпочли бы получить информацию о безопасном использовании Интернета?

☐ Школа

☐ Родительские (школьные) комитеты, собрания, другие информационные возможности для родителей

☐ Правительство, местные власти

☐ Информационные услуги провайдеров или телефонных компаний

☐ Производители программного обеспечения

☐ Поставщики (розничные продавцы) компьютеров

☐ Ваш работодатель

☐ Общественные или образовательные организации

☐ Средства массовой информации

☐ Правоохранительные органы

☐ Другие источники

☐ Я не хочу получать какую-либо информацию

☐ Затрудняюсь ответить

**8.** В какой форме вы хотели бы получать эту информацию?

☐ Письма

☐ Электронная почта

☐ Веб-сайты

☐ Смс и другие текстовые сообщения

☐ По телефону

☐ Газеты

☐ В компьютерных магазинах

☐ Из телепередач

☐ Из радиопередач

☐ В библиотеке

☐ На CD-дисках

☐ Из других медиаисточников

☐ Затрудняюсь ответить

**9.** Знаете ли вы, куда можно сообщить о незаконном или негативном контенте в Интернете?

☐ Да, на «горячую линию»

☐ Да, в правоохранительные органы

☐ Да, на специальные сервисы интернет-провайдеров

☐ Да, в школу

☐ Да, в родительский комитет

☐ Да, в общественные или образовательные организации

☐ Другое

☐ Нет, я не знаю

☐ Затрудняюсь ответить

Укажите:

- свой возраст: _____
- пол: _____
- профессию: _____

**Благодарим за участие!**

## АНКЕТА ДЛЯ ПЕДАГОГОВ

**Уважаемые педагоги!**

В целях оценки рисков и опасностей Интернета для школьников ответьте на представленные ниже вопросы. Отвечайте не задумываясь — правильных и неправильных ответов нет, а есть разнообразие мнений. Ваше мнение нам очень важно.

**1.** Есть ли у вас дома компьютер, подключенный к сети Интернет?

☐ Да

☐ Есть компьютер, не подключенный к сети Интернет

☐ Нет

**2.** Есть ли у вас в школе Интернет?

☐ Да

☐ Нет

☐ Не знаю

**3.** Доступен ли в вашей школе Интернет для школьников во внеурочное время?

☐ Да

☐ Нет

☐ Не знаю

**4.** Как часто вы сами пользуетесь Интернетом?

☐ 1—2 раза в неделю

☐ 1—2 раза в день

☐ 1 раз в месяц

☐ Я «живу» в Интернете

☐ Не пользуюсь Интернетом вообще

☐ Другое: _____

**5.** Сколько вы проводите в Интернете времени за один сеанс?

☐ 10—20 минут

☐ 1—3 часа

☐ 5—10 часов

☐ Другое: _____

**6.** Что вы обычно делаете в Интернете?

| | **Часто** | **Редко** | **Никогда** |
|---|---|---|---|
| Пользуюсь электронной почтой | | | |
| Общаюсь в «ВКонтакте», «Одноклассниках» и других социальных сетях | | | |
| Общаюсь с друзьями по ICQ | | | |
| Общаюсь по скайпу | | | |
| Веду виртуальный дневник (блог) | | | |
| Ищу информацию для работы | | | |
| Ищу информацию для культурного и духовного развития | | | |
| Общаюсь в чатах | | | |
| Скачиваю программы, музыку, фото, видео | | | |
| Слушаю аудиозаписи | | | |
| Смотрю видеозаписи | | | |
| Узнаю о последних событиях и новостях в стране и мире | | | |
| Играю в онлайн-игры | | | |
| Принимаю участие в интернет-акциях, голосовании и др. | | | |

Укажите, чем вы еще занимаетесь в Интернете:

_____

_____

_____

_____

**7.** По вашему мнению, что обычно делают в Интернете ваши ученики — пользователи Интернета?

| | **Часто** | **Редко** | **Никогда** |
|---|---|---|---|
| Пользуются электронной почтой | | | |
| Общаются в «ВКонтакте», «Одноклассниках» и других социальных сетях | | | |
| Общаются с друзьями по ICQ | | | |
| Общаются с друзьями по скайпу | | | |
| Ведут виртуальный дневник (блог) | | | |
| Ищут информацию для учебы | | | |
| Ищут информацию для культурного и духовного развития | | | |
| Общаются в чатах | | | |
| Скачивают программы, музыку, фото, видео | | | |
| Слушают аудиозаписи | | | |
| Смотрят видеозаписи | | | |
| Узнают о последних событиях и новостях в стране и мире | | | |
| Играют в онлайн-игры | | | |
| Принимают участие в интернет-акциях, голосовании и др. | | | |
| Просматривают запрещенные родителями сайты | | | |

Укажите, чем еще занимаются в Интернете ваши ученики:

_____

_____

_____

_____

_____

**8.** Можете ли вы сказать, что находиться в Интернете опасно?

☐ Да

☐ Иногда

☐ Нет

☐ Не знаю

**9.** Как часто вы и ваши ученики сталкивались в Интернете с опасностями?

| | **Часто** | **Редко** | **Никогда** |
|---|---|---|---|
| Вирусы | | | |
| Мошенничество/кражи | | | |
| Преследование, оскорбление и унижение со стороны других пользователей | | | |
| Сексуальные домогательства | | | |
| Неэтичная и навязчивая реклама | | | |
| Порнография | | | |
| Психологическое давление | | | |
| Агрессия | | | |
| Экстремизм | | | |
| Призывы причинить вред себе и/или окружающим | | | |

Укажите, с чем еще вы и ваши ученики сталкивались в Интернете:

_____

_____

_____

_____

_____

_____

**10.** Как часто вы оставляете малознакомым (едва знакомым) людям свои контактные данные?

| | **Часто** | **Редко** | **Никогда** |
|---|---|---|---|
| Адрес электронной почты | | | |
| Номер мобильного телефона | | | |
| Номер домашнего телефона | | | |
| Домашний адрес | | | |
| Номер школы и класса | | | |
| Свои фотографии и фотографии своих родственников | | | |

**11.** Школьники, пользуясь Интернетом, часто дают свои контактные данные малознакомым людям или встречаются с ними. Как вы к этому относитесь?

☐ Считаю это естественным и безопасным

☐ Считаю, что из-за этого могут быть иногда неприятности

☐ Считаю, что это опасно

☐ Другое: _____

**12.** Какие сайты вы посещаете в Интернете чаще всего?

| | Часто | Редко | Никогда |
|---|---|---|---|
| Игровые | | | |
| Сайты с музыкой и фильмами | | | |
| Сайты интернет-знакомств | | | |
| Сайты для детей | | | |
| Сайты для взрослых | | | |
| Другое | | | |

**13.** Знаете ли вы, какие сайты посещают ваши ученики?

| | Часто | Редко | Никогда |
|---|---|---|---|
| Игровые | | | |
| Сайты с музыкой и фильмами | | | |
| Сайты интернет-знакомств | | | |
| Сайты для детей | | | |
| Сайты для взрослых | | | |
| Другое | | | |

**14.** Укажите 5 причин, почему, на ваш взгляд, стоит заходить в Интернет:

_____

_____

_____

_____

_____

**15.** Укажите 5 причин, почему, на ваш взгляд, стоит покинуть Интернет:

_____

_____

_____

_____

_____

**16.** Как вы считаете, вредит ли ученикам Интернет?

| | **Часто** | **Редко** | **Никогда** |
|---|---|---|---|
| Их физическому здоровью | | | |
| Их психическому здоровью | | | |
| Их морали/нравственности | | | |
| Их культурному уровню | | | |
| Их успеваемости в школе | | | |

**17.** Сталкивались ли вы с жалобами родителей на проблемы компьютерной зависимости ваших учеников?

☐ Да, очень часто

☐ В редком случае

☐ Нет

☐ Другое: _____

**18.** Установлены ли на ваших школьных компьютерах программы, ограничивающие вход на какие-либо сайты?

☐ Да

☐ Нет

☐ Не знаю

**19.** Существует мнение, что виртуальное пространство Интернета в настоящее время сравнялось по степени опасности с реальной средой. Как вы к этому относитесь?

☐ Согласен(на)

☐ Считаю это большим преувеличением

☐ Виртуальное пространство в чем-то опасно, в чем-то безопасно

☐ Считаю Интернет абсолютно безопасной средой

☐ Не знаю

☐ Другое: _____

**20.** Считаете ли вы, что Интернет — это свободное пространство, в котором по своему усмотрению можно делать все, что пожелаешь?

☐ Да

☐ Нет

☐ Не уверен(а)

☐ Считаю, что должны быть правила, регулирующие пользование Интернетом

**21.** Можете ли вы описать какой-либо неприятный, связанный с Интернетом случай из вашей педагогической практики или произошедший с вами лично?

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

**22.** Каково, на ваш взгляд, должно быть отношение родителей к использованию детьми Интернета?

☐ Разрешать свободно пользоваться и не ограничивать во времени

☐ Устанавливать временной режим и следить за тем, какие сайты они посещают

☐ Разрешать заходить в Интернет только в своем присутствии

☐ Запрещать пользоваться Интернетом вообще

☐ Другое: _____

**23.** Какой источник информации для вас сегодня самый главный? Обозначьте цифрами по степени значимости: 1 (самый главный); 2 (занимает по значимости второе место) и т. д.

☐ Коллеги

☐ Друзья

☐ Родственники

☐ Интернет

☐ Телевидение

☐ Книги

☐ Газеты/журналы

☐ Радио

☐ Другое: _____

**24.** Какие эмоции и чувства вы чаще всего испытываете, находясь в Интернете (укажите не менее трех)?

☐ Радость

☐ Страх

☐ Удивление

☐ Печаль

☐ Восторг

☐ Стыд

☐ Доверие

☐ Вина

☐ Интерес

☐ Разочарование

☐ Любопытство

☐ Уверенность

☐ Унижение

☐ Счастье

☐ Отвращение

☐ Удовольствие

☐ Обида

☐ Надежда

☐ Тревога

☐ Гнев

☐ Восхищение

☐ Другое: _____

_____

**25.** Оцените уровень опасности.

| | **Очень опасно** | **Опасно** | **Скорее опасно** | **Не знаю** | **Скорее безопасно** | **Безопасно** | **Совершенно безопасно** |
|---|---|---|---|---|---|---|---|
| В стране | | | | | | | |
| В городе | | | | | | | |
| На улице | | | | | | | |
| В школе | | | | | | | |
| В Интернете | | | | | | | |
| Дома | | | | | | | |

**26.** По вашему мнению, Интернет — это _____

_____

_____

_____

_____

Укажите:

- свой возраст: _____
- пол: _____
- должность: _____
- стаж педагогической деятельности: _____

**Благодарим за участие!**

# Федеральный закон «О защите детей от информации, причиняющей вред их здоровью и развитию» (извлечения)

## Глава 1. Общие положения

### **СТАТЬЯ 1.** СФЕРА ДЕЙСТВИЯ НАСТОЯЩЕГО ФЕДЕРАЛЬНОГО ЗАКОНА

1. Настоящий Федеральный закон регулирует отношения, связанные с защитой детей от информации, причиняющей вред их здоровью и (или) развитию, в том числе от такой информации, содержащейся в информационной продукции.

2. Настоящий Федеральный закон не распространяется на отношения в сфере:

1) оборота информационной продукции, содержащей научную, научно-техническую, статистическую информацию;

2) распространения информации, недопустимость ограничения доступа к которой установлена Федеральным законом от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации» и другими федеральными законами;

3) оборота информационной продукции, имеющей значительную историческую, художественную или иную культурную ценность для общества;

4) рекламы.

### **СТАТЬЯ 2.** ОСНОВНЫЕ ПОНЯТИЯ, ИСПОЛЬЗУЕМЫЕ В НАСТОЯЩЕМ ФЕДЕРАЛЬНОМ ЗАКОНЕ

В настоящем Федеральном законе используются следующие основные понятия:

1) доступ детей к информации — возможность получения и использования детьми свободно распространяемой информации;

2) знак информационной продукции — графическое и (или) текстовое обозначение информационной продукции в соответствии с классификацией информаци-

онной продукции, предусмотренной частью 3 статьи 6 настоящего Федерального закона;

3) зрелищное мероприятие — демонстрация информационной продукции в месте, доступном для детей, и в месте, где присутствует значительное число лиц, не принадлежащих к обычному кругу семьи, в том числе посредством проведения театрально-зрелищных, культурно-просветительных и зрелищно-развлекательных мероприятий;

4) информационная безопасность детей — состояние защищенности детей, при котором отсутствует риск, связанный с причинением информацией вреда их здоровью и (или) физическому, психическому, духовному, нравственному развитию;

5) информационная продукция — предназначенные для оборота на территории Российской Федерации продукция средств массовой информации, печатная продукция, аудиовизуальная продукция на любых видах носителей, программы для электронных вычислительных машин (программы для ЭВМ) и базы данных, а также информация, распространяемая посредством зрелищных мероприятий, посредством информационно-телекоммуникационных сетей, в том числе сети «Интернет», и сетей подвижной радиотелефонной связи (в ред. Федерального закона от 28.07.2012 № 139-ФЗ);

6) информационная продукция для детей — информационная продукция, соответствующая по тематике, содержанию и художественному оформлению физическому, психическому, духовному и нравственному развитию детей;

7) информация, причиняющая вред здоровью и (или) развитию детей, — информация (в том числе содержащаяся в информационной продукции для детей), распространение которой среди детей запрещено или ограничено в соответствии с настоящим Федеральным законом;

8) информация порнографического характера — информация, представляемая в виде натуралистических изображения или описания половых органов человека и (или) полового сношения либо сопоставимого с поло-

вым сношением действия сексуального характера, в том числе такого действия, совершаемого в отношении животного;

9) классификация информационной продукции — распределение информационной продукции в зависимости от ее тематики, жанра, содержания и художественного оформления по возрастным категориям детей в порядке, установленном настоящим Федеральным законом;

10) места, доступные для детей, — общественные места, доступ ребенка в которые и (или) нахождение ребенка в которых не запрещены, в том числе общественные места, в которых ребенок имеет доступ к продукции средств массовой информации и (или) размещаемой в информационно-телекоммуникационных сетях информационной продукции;

11) натуралистические изображение или описание — изображение или описание в любой форме и с использованием любых средств человека, животного, отдельных частей тела человека и (или) животного, действия (бездействия), события, явления, их последствий с фиксированием внимания на деталях, анатомических подробностях и (или) физиологических процессах;

12) оборот информационной продукции — предоставление и (или) распространение информационной продукции, включая ее продажу (в том числе распространение по подписке), аренду, прокат, раздачу, выдачу из фондов общедоступных библиотек, публичный показ, публичное исполнение (в том числе посредством зрелищных мероприятий), распространение посредством эфирного или кабельного вещания, информационно-телекоммуникационных сетей, в том числе сети «Интернет», и сетей подвижной радиотелефонной связи (в ред. Федерального закона от 28.07.2012 № 139-ФЗ);

13) эксперт — лицо, отвечающее требованиям настоящего Федерального закона и привлекаемое для проведения экспертизы информационной продукции и дачи экспертного заключения или осуществления классификации информационной продукции и проведения ее экспертизы.

### **СТАТЬЯ 3.** ЗАКОНОДАТЕЛЬСТВО РОССИЙСКОЙ ФЕДЕРАЦИИ О ЗАЩИТЕ ДЕТЕЙ ОТ ИНФОРМАЦИИ, ПРИЧИНЯЮЩЕЙ ВРЕД ИХ ЗДОРОВЬЮ И (ИЛИ) РАЗВИТИЮ

Законодательство Российской Федерации о защите детей от информации, причиняющей вред их здоровью и (или) развитию, состоит из Конституции Российской Федерации, настоящего Федерального закона, других федеральных законов и принимаемых в соответствии с ними иных нормативных правовых актов.

### **СТАТЬЯ 5.** ВИДЫ ИНФОРМАЦИИ, ПРИЧИНЯЮЩЕЙ ВРЕД ЗДОРОВЬЮ И (ИЛИ) РАЗВИТИЮ ДЕТЕЙ

1. К информации, причиняющей вред здоровью и (или) развитию детей, относится:

1) информация, предусмотренная частью 2 настоящей статьи и запрещенная для распространения среди детей;

2) информация, которая предусмотрена частью 3 настоящей статьи с учетом положений статей 7—10 настоящего Федерального закона и распространение которой среди детей определенных возрастных категорий ограничено.

2. К информации, запрещенной для распространения среди детей, относится информация:

1) побуждающая детей к совершению действий, представляющих угрозу их жизни и (или) здоровью, в том числе к причинению вреда своему здоровью, самоубийству;

2) способная вызвать у детей желание употребить наркотические средства, психотропные и (или) одурманивающие вещества, табачные изделия, алкогольную и спиртосодержащую продукцию, принять участие в азартных играх, заниматься проституцией, бродяжничеством или попрошайничеством (в ред. Федерального закона от 29.06.2015 № 179-ФЗ);

3) обосновывающая или оправдывающая допустимость насилия и (или) жестокости либо побуждаю-

щая осуществлять насильственные действия по отношению к людям или животным, за исключением случаев, предусмотренных настоящим Федеральным законом;

4) отрицающая семейные ценности, пропагандирующая нетрадиционные сексуальные отношения и формирующая неуважение к родителям и (или) другим членам семьи (в ред. Федерального закона от 29.06.2013 № 135-ФЗ);

5) оправдывающая противоправное поведение;

6) содержащая нецензурную брань;

7) содержащая информацию порнографического характера;

8) о несовершеннолетнем, пострадавшем в результате противоправных действий (бездействия), включая фамилии, имена, отчества, фото- и видеоизображения такого несовершеннолетнего, его родителей и иных законных представителей, дату рождения такого несовершеннолетнего, аудиозапись его голоса, место его жительства или место временного пребывания, место его учебы или работы, иную информацию, позволяющую прямо или косвенно установить личность такого несовершеннолетнего (п. 8 введен Федеральным законом от 05.04.2013 № 50-ФЗ).

3. К информации, распространение которой среди детей определенных возрастных категорий ограничено, относится информация:

1) представляемая в виде изображения или описания жестокости, физического и (или) психического насилия, преступления или иного антиобщественного действия;

2) вызывающая у детей страх, ужас или панику, в том числе представляемая в виде изображения или описания в унижающей человеческое достоинство форме ненасильственной смерти, заболевания, самоубийства, несчастного случая, аварии или катастрофы и (или) их последствий;

3) представляемая в виде изображения или описания половых отношений между мужчиной и женщиной;

4) содержащая бранные слова и выражения, не относящиеся к нецензурной брани.

## Глава 2. Классификация информационной продукции

### **СТАТЬЯ 6.** ОСУЩЕСТВЛЕНИЕ КЛАССИФИКАЦИИ ИНФОРМАЦИОННОЙ ПРОДУКЦИИ

3. Классификация информационной продукции осуществляется в соответствии с требованиями настоящего Федерального закона по следующим категориям информационной продукции:

1) информационная продукция для детей, не достигших возраста шести лет;

2) информационная продукция для детей, достигших возраста шести лет;

3) информационная продукция для детей, достигших возраста двенадцати лет;

4) информационная продукция для детей, достигших возраста шестнадцати лет;

5) информационная продукция, запрещенная для детей (информационная продукция, содержащая информацию, предусмотренную частью 2 статьи 5 настоящего Федерального закона) (в ред. Федерального закона от 28.07.2012 № 139-ФЗ).

### **СТАТЬЯ 7.** ИНФОРМАЦИОННАЯ ПРОДУКЦИЯ ДЛЯ ДЕТЕЙ, НЕ ДОСТИГШИХ ВОЗРАСТА ШЕСТИ ЛЕТ

К информационной продукции для детей, не достигших возраста шести лет, может быть отнесена информационная продукция, содержащая информацию, не причиняющую вреда здоровью и (или) развитию детей (в том числе информационная продукция, содержащая оправданные ее жанром и (или) сюжетом эпизодические ненатуралистические изображение или описание физического и (или) психического насилия (за исключением сексуального насилия) при условии торжества добра над злом и выражения сострадания к жертве насилия и (или) осуждения насилия).

### **СТАТЬЯ 8.** ИНФОРМАЦИОННАЯ ПРОДУКЦИЯ ДЛЯ ДЕТЕЙ, ДОСТИГШИХ ВОЗРАСТА ШЕСТИ ЛЕТ

К допускаемой к обороту информационной продукции для детей, достигших возраста шести лет, может

быть отнесена информационная продукция, предусмотренная статьей 7 настоящего Федерального закона, а также информационная продукция, содержащая оправданные ее жанром и (или) сюжетом:

1) кратковременные и ненатуралистические изображение или описание заболеваний человека (за исключением тяжелых заболеваний) и (или) их последствий в форме, не унижающей человеческого достоинства;

2) ненатуралистические изображение или описание несчастного случая, аварии, катастрофы либо ненасильственной смерти без демонстрации их последствий, которые могут вызывать у детей страх, ужас или панику;

3) не побуждающие к совершению антиобщественных действий и (или) преступлений эпизодические изображение или описание этих действий и (или) преступлений при условии, что не обосновывается и не оправдывается их допустимость и выражается отрицательное, осуждающее отношение к лицам, их совершающим.

### **СТАТЬЯ 9.** ИНФОРМАЦИОННАЯ ПРОДУКЦИЯ ДЛЯ ДЕТЕЙ, ДОСТИГШИХ ВОЗРАСТА ДВЕНАДЦАТИ ЛЕТ

К допускаемой к обороту информационной продукции для детей, достигших возраста двенадцати лет, может быть отнесена информационная продукция, предусмотренная статьей 8 настоящего Федерального закона, а также информационная продукция, содержащая оправданные ее жанром и (или) сюжетом:

1) эпизодические изображение или описание жестокости и (или) насилия (за исключением сексуального насилия) без натуралистического показа процесса лишения жизни или нанесения увечий при условии, что выражается сострадание к жертве и (или) отрицательное, осуждающее отношение к жестокости, насилию (за исключением насилия, применяемого в случаях защиты прав граждан и охраняемых законом интересов общества или государства);

2) изображение или описание, не побуждающие к совершению антиобщественных действий (в том числе

к потреблению алкогольной и спиртосодержащей продукции, участию в азартных играх, занятию бродяжничеством или попрошайничеством), эпизодическое упоминание (без демонстрации) наркотических средств, психотропных и (или) одурманивающих веществ, табачных изделий при условии, что не обосновывается и не оправдывается допустимость антиобщественных действий, выражается отрицательное, осуждающее отношение к ним и содержится указание на опасность потребления указанных продукции, средств, веществ, изделий (в ред. Федерального закона от 29.06.2015 № 179-ФЗ);

3) не эксплуатирующие интереса к сексу и не носящие возбуждающего или оскорбительного характера эпизодические ненатуралистические изображение или описание половых отношений между мужчиной и женщиной, за исключением изображения или описания действий сексуального характера.

### **СТАТЬЯ 10.** ИНФОРМАЦИОННАЯ ПРОДУКЦИЯ ДЛЯ ДЕТЕЙ, ДОСТИГШИХ ВОЗРАСТА ШЕСТНАДЦАТИ ЛЕТ

К допускаемой к обороту информационной продукции для детей, достигших возраста шестнадцати лет, может быть отнесена информационная продукция, предусмотренная статьей 9 настоящего Федерального закона, а также информационная продукция, содержащая оправданные ее жанром и (или) сюжетом:

1) изображение или описание несчастного случая, аварии, катастрофы, заболевания, смерти без натуралистического показа их последствий, которые могут вызывать у детей страх, ужас или панику;

2) изображение или описание жестокости и (или) насилия (за исключением сексуального насилия) без натуралистического показа процесса лишения жизни или нанесения увечий при условии, что выражается сострадание к жертве и (или) отрицательное, осуждающее отношение к жестокости, насилию (за исключением насилия, применяемого в случаях защиты прав граждан и охраняемых законом интересов общества или государства);

3) информация о наркотических средствах или о психотропных и (или) одурманивающих веществах (без их демонстрации), об опасных последствиях их потребления с демонстрацией таких случаев при условии, что выражается отрицательное или осуждающее отношение к потреблению таких средств или веществ и содержится указание на опасность их потребления;

4) отдельные бранные слова и (или) выражения, не относящиеся к нецензурной брани;

5) не эксплуатирующие интереса к сексу и не носящие оскорбительного характера изображение или описание половых отношений между мужчиной и женщиной, за исключением изображения или описания действий сексуального характера.

## Глава 3. Требования к обороту информационной продукции

### **СТАТЬЯ 11.** ОБЩИЕ ТРЕБОВАНИЯ К ОБОРОТУ ИНФОРМАЦИОННОЙ ПРОДУКЦИИ

<...> 5. В присутствии родителей или иных законных представителей детей, достигших возраста шести лет, допускается оборот информационной продукции, предусмотренной статьей 9 настоящего Федерального закона.

6. До начала демонстрации посредством зрелищного мероприятия информационной продукции ей присваивается знак информационной продукции. В случае демонстрации нескольких видов информационной продукции для детей разных возрастных категорий указанный знак должен соответствовать информационной продукции для детей старшей возрастной категории. Указанный знак размещается на афишах и иных объявлениях о проведении зрелищного мероприятия, а также на входных билетах, приглашениях и иных документах, предоставляющих право его посещения.

7. Демонстрация посредством зрелищного мероприятия информационной продукции, содержащей инфор-

мацию, предусмотренную статьей 5 настоящего Федерального закона, предваряется непосредственно перед началом зрелищного мероприятия звуковым сообщением о недопустимости или об ограничении присутствия на такой демонстрации детей соответствующих возрастных категорий.

### **СТАТЬЯ 12.** ЗНАК ИНФОРМАЦИОННОЙ ПРОДУКЦИИ

1. Обозначение категории информационной продукции знаком информационной продукции и (или) текстовым предупреждением об ограничении распространения информационной продукции среди детей осуществляется с соблюдением требований настоящего Федерального закона ее производителем и (или) распространителем следующим образом:

1) применительно к категории информационной продукции для детей, не достигших возраста шести лет, — в виде цифры «0» и знака «плюс»;

2) применительно к категории информационной продукции для детей, достигших возраста шести лет, — в виде цифры «6» и знака «плюс» и (или) текстового предупреждения в виде словосочетания «для детей старше шести лет»;

3) применительно к категории информационной продукции для детей, достигших возраста двенадцати лет, — в виде цифры «12» и знака «плюс» и (или) текстового предупреждения в виде словосочетания «для детей старше 12 лет»;

4) применительно к категории информационной продукции для детей, достигших возраста шестнадцати лет, — в виде цифры «16» и знака «плюс» и (или) текстового предупреждения в виде словосочетания «для детей старше 16 лет»;

5) применительно к категории информационной продукции, запрещенной для детей, — в виде цифры «18» и знака «плюс» и (или) текстового предупреждения в виде словосочетания «запрещено для детей».

(Часть 1 в ред. Федерального закона от 28.07.2012 № 139-ФЗ.)

**СТАТЬЯ 13.** ДОПОЛНИТЕЛЬНЫЕ ТРЕБОВАНИЯ К РАСПРОСТРАНЕНИЮ ИНФОРМАЦИОННОЙ ПРОДУКЦИИ ПОСРЕДСТВОМ ТЕЛЕ- И РАДИОВЕЩАНИЯ

1. Информационная продукция, содержащая информацию, предусмотренную пунктами 1—5 части 2 статьи 5 настоящего Федерального закона, не подлежит распространению посредством теле- и радиовещания с 4 часов до 23 часов по местному времени, за исключением теле- и радиопрограмм, теле- и радиопередач, доступ к просмотру или прослушиванию которых осуществляется исключительно на платной основе с применением декодирующих технических устройств и с соблюдением требований частей 3 и 4 настоящей статьи.

2. Информационная продукция, содержащая информацию, предусмотренную пунктами 4 и 5 статьи 10 настоящего Федерального закона, не подлежит распространению посредством теле- и радиовещания с 7 часов до 21 часа по местному времени, за исключением теле- и радиопрограмм, теле- и радиопередач, доступ к просмотру или прослушиванию которых осуществляется исключительно на платной основе с применением декодирующих технических устройств и с соблюдением требований частей 3 и 4 настоящей статьи.

3. Распространение посредством телевизионного вещания информационной продукции, содержащей информацию, предусмотренную статьей 5 настоящего Федерального закона, сопровождается демонстрацией знака информационной продукции в углу кадра в порядке, установленном уполномоченным Правительством Российской Федерации федеральным органом исполнительной власти, в начале трансляции телепрограммы, телепередачи, а также при каждом возобновлении их трансляции (после прерывания рекламой и (или) иной информацией).

(Часть 3 в ред. Федерального закона от 28.07.2012 № 139-ФЗ.)

4. Распространение посредством радиовещания информационной продукции, содержащей информацию, предусмотренную статьей 5 настоящего Федерального закона, за исключением радиопередач, транслируемых в эфире без предварительной записи, сопровождается

сообщением об ограничении распространения такой информационной продукции среди детей в начале трансляции радиопередач в порядке, установленном уполномоченным Правительством Российской Федерации федеральным органом исполнительной власти.

(Часть 4 в ред. Федерального закона от 28.07.2012 № 139-ФЗ.)

5. При размещении анонсов или сообщений о распространении посредством теле- и радиовещания информационной продукции, запрещенной для детей, не допускается использование фрагментов указанной информационной продукции, содержащей информацию, причиняющую вред здоровью и (или) развитию детей.

(В ред. Федерального закона от 28.07.2012 № 139-ФЗ.)

### **СТАТЬЯ 14.** ОСОБЕННОСТИ РАСПРОСТРАНЕНИЯ ИНФОРМАЦИИ ПОСРЕДСТВОМ ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННЫХ СЕТЕЙ (В РЕД. ФЕДЕРАЛЬНОГО ЗАКОНА ОТ 28.07.2012 № 139-ФЗ)

1. Доступ к информации, распространяемой посредством информационно-телекоммуникационных сетей, в том числе сети «Интернет», в местах, доступных для детей, предоставляется лицом, организующим доступ к сети «Интернет» в таких местах (за исключением операторов связи, оказывающих эти услуги связи на основании договоров об оказании услуг связи, заключенных в письменной форме), другим лицам при условии применения административных и организационных мер, технических, программно-аппаратных средств защиты детей от информации, причиняющей вред их здоровью и (или) развитию.

2. Сайт в информационно-телекоммуникационной сети «Интернет», не зарегистрированный как средство массовой информации, может содержать знак информационной продукции (в том числе в машиночитаемом виде) и (или) текстовое предупреждение об ограничении ее распространения среди детей, соответствующие одной из категорий информационной продукции, установленных частью 3 статьи 6 настоящего Федерального закона. Классификация сайтов осуществляется их вла-

дельцами самостоятельно в соответствии с требованиями настоящего Федерального закона.

3. Аудиовизуальный сервис должен содержать знак информационной продукции (в том числе в машиночитаемом виде) и (или) текстовое предупреждение об ограничении распространения среди детей информационной продукции, соответствующие одной из категорий информационной продукции, установленных частью 3 статьи 6 настоящего Федерального закона. Классификация аудиовизуальных сервисов осуществляется их владельцами самостоятельно в соответствии с требованиями настоящего Федерального закона.

(Часть 3 введена Федеральным законом от 01.05.2017 № 87-ФЗ.)

### **СТАТЬЯ 15.** ДОПОЛНИТЕЛЬНЫЕ ТРЕБОВАНИЯ К ОБОРОТУ ОТДЕЛЬНЫХ ВИДОВ ИНФОРМАЦИОННОЙ ПРОДУКЦИИ ДЛЯ ДЕТЕЙ

1. В информационной продукции для детей, включая информационную продукцию, распространяемую посредством информационно-телекоммуникационных сетей, в том числе сети «Интернет», и сетей подвижной радиотелефонной связи, не допускается размещать объявления о привлечении детей к участию в создании информационной продукции, причиняющей вред их здоровью и (или) развитию.

(Часть 1 в ред. Федерального закона от 28.07.2012 № 139-ФЗ.)

2. Содержание и художественное оформление информационной продукции, предназначенной для обучения детей в дошкольных образовательных организациях, должны соответствовать содержанию и художественному оформлению информационной продукции для детей, не достигших возраста шести лет.

(В ред. Федерального закона от 02.07.2013 № 185-ФЗ.)

3. Содержание и художественное оформление печатных изданий, полиграфической продукции (в том числе тетрадей, дневников, обложек для книг, закладок для книг), аудиовизуальной продукции, иной информационной продукции, используемой в образова-

тельном процессе, должны соответствовать требованиям статей 7—10 настоящего Федерального закона.

### **СТАТЬЯ 16.** ДОПОЛНИТЕЛЬНЫЕ ТРЕБОВАНИЯ К ОБОРОТУ ИНФОРМАЦИОННОЙ ПРОДУКЦИИ, ЗАПРЕЩЕННОЙ ДЛЯ ДЕТЕЙ

1. Первая и последняя полосы газеты, обложка экземпляра печатной продукции, иной полиграфической продукции, запрещенной для детей, при распространении для неопределенного круга лиц в местах, доступных для детей, не должны содержать информацию, причиняющую вред здоровью и (или) развитию детей.

2. Информационная продукция, запрещенная для детей, в виде печатной продукции допускается к распространению в местах, доступных для детей, только в запечатанных упаковках.

3. Информационная продукция, запрещенная для детей, не допускается к распространению в предназначенных для детей образовательных организациях, детских медицинских, санаторно-курортных, физкультурно-спортивных организациях, организациях культуры, организациях отдыха и оздоровления детей или на расстоянии менее чем сто метров от границ территорий указанных организаций.

## Глава 4. Экспертиза информационной продукции

### **СТАТЬЯ 17.** ОБЩИЕ ТРЕБОВАНИЯ К ЭКСПЕРТИЗЕ ИНФОРМАЦИОННОЙ ПРОДУКЦИИ (В РЕД. ФЕДЕРАЛЬНОГО ЗАКОНА ОТ 28.07.2012 № 139-ФЗ)

1. Экспертиза информационной продукции проводится экспертом, экспертами и (или) экспертными организациями, аккредитованными уполномоченным Правительством Российской Федерации федеральным органом исполнительной власти, по инициативе органов государственной власти, органов местного самоуправления, юридических лиц, индивидуальных предпринимателей, общественных объединений, граждан на договорной основе. В случае несогласия с результатами проведенной экспертизы информационной про-

дукции заинтересованное лицо вправе оспорить экспертное заключение в судебном порядке.

2. Уполномоченный Правительством Российской Федерации федеральный орган исполнительной власти осуществляет в установленном им порядке аккредитацию экспертов и экспертных организаций на право проведения экспертизы информационной продукции, включая выдачу аттестатов аккредитации, приостановление или прекращение действия выданных аттестатов аккредитации, ведение реестра аккредитованных экспертов и экспертных организаций и контроль за деятельностью аккредитованных им экспертов и экспертных организаций.

3. Сведения, содержащиеся в реестре аккредитованных экспертов и экспертных организаций, являются открытыми и доступными для ознакомления с ними любых физических лиц и юридических лиц, за исключением случаев, если доступ к таким сведениям ограничен в соответствии с федеральными законами.

4. Уполномоченный Правительством Российской Федерации федеральный орган исполнительной власти размещает в информационно-телекоммуникационной сети «Интернет» на своем официальном сайте следующие сведения из реестра аккредитованных экспертов и экспертных организаций:

1) полное и (в случае, если имеется) сокращенное наименование, организационно-правовая форма юридического лица, адрес его места нахождения, адреса мест осуществления экспертной деятельности (в отношении аккредитованных экспертных организаций);

2) фамилия, имя и (в случае, если имеется) отчество индивидуального предпринимателя, адреса мест осуществления экспертной деятельности (в отношении аккредитованных экспертов, являющихся индивидуальными предпринимателями);

3) фамилия, имя и (в случае, если имеется) отчество физического лица, наименование и организационно-правовая форма экспертной организации, адреса мест осуществления экспертной деятельности (в отношении аккредитованных экспертов, являющихся работниками экспертных организаций);

4) номер и дата выдачи аттестата аккредитации;

5) номер и дата приказа (распоряжения должностного лица) уполномоченного Правительством Российской Федерации федерального органа исполнительной власти об аккредитации эксперта или экспертной организации;

6) вид информационной продукции, экспертизу которой вправе осуществлять аккредитованный эксперт или аккредитованная экспертная организация;

7) сведения о приостановлении или прекращении действия выданного аттестата аккредитации.

5. В качестве эксперта, экспертов для проведения экспертизы информационной продукции могут выступать лица, имеющие высшее профессиональное образование и обладающие специальными знаниями, в том числе в области педагогики, возрастной психологии, возрастной физиологии, детской психиатрии, за исключением лиц:

1) имеющих или имевших судимость за совершение тяжких и особо тяжких преступлений против личности, преступлений против половой неприкосновенности и половой свободы личности, против семьи и несовершеннолетних, умышленных преступлений против здоровья населения и общественной нравственности;

2) являющихся производителями, распространителями информационной продукции, переданной на экспертизу, или их представителями.

6. Порядок проведения экспертизы информационной продукции устанавливается уполномоченным Правительством Российской Федерации федеральным органом исполнительной власти с соблюдением требований настоящего Федерального закона.

7. Экспертиза информационной продукции может проводиться двумя и более экспертами одной специальности (комиссионная экспертиза) или разных специальностей (комплексная экспертиза).

8. Срок проведения экспертизы информационной продукции не может превышать тридцать дней с момента заключения договора о ее проведении.

9. Оплата услуг экспертов, экспертных организаций и возмещение понесенных ими в связи с прове-

дением экспертизы информационной продукции расходов осуществляются за счет заказчика экспертизы.

### **СТАТЬЯ 18.** ЭКСПЕРТНОЕ ЗАКЛЮЧЕНИЕ

1. По окончании экспертизы информационной продукции дается экспертное заключение.

2. В экспертном заключении указываются:

1) дата, время и место проведения экспертизы информационной продукции;

2) сведения об экспертной организации и эксперте (фамилия, имя, отчество, образование, специальность, стаж работы по специальности, наличие ученой степени, ученого звания, занимаемая должность, место работы);

3) вопросы, поставленные перед экспертом, экспертами;

4) объекты исследований и материалы, представленные для проведения экспертизы информационной продукции;

5) содержание и результаты исследований с указанием методик;

6) мотивированные ответы на поставленные перед экспертом, экспертами вопросы;

7) выводы о наличии или об отсутствии в информационной продукции информации, причиняющей вред здоровью и (или) развитию детей, о соответствии или о несоответствии информационной продукции определенной категории информационной продукции, о соответствии или о несоответствии информационной продукции знаку информационной продукции.

3. Экспертное заключение комиссионной экспертизы подписывается всеми экспертами, участвовавшими в проведении указанной экспертизы, если их мнения по поставленным вопросам совпадают. В случае возникновения разногласий каждый эксперт дает отдельное экспертное заключение по вопросам, вызвавшим разногласия. Каждый эксперт, участвовавший в проведении комплексной экспертизы, подписывает часть экспертного заключения, содержащую описание проведенных им исследований, и несет за нее ответственность.

4. Экспертное заключение составляется в трех экземплярах для передачи заказчику экспертизы инфор-

мационной продукции, для направления в течение двух рабочих дней со дня подписания экспертного заключения в уполномоченный Правительством Российской Федерации федеральный орган исполнительной власти и для хранения у эксперта или в экспертной организации в течение пяти лет.

(Часть 4 в ред. Федерального закона от 28.07.2012 № 139-ФЗ.)

5. Информация о проведенной экспертизе информационной продукции и ее результатах размещается уполномоченным Правительством Российской Федерации федеральным органом исполнительной власти в информационно-телекоммуникационной сети «Интернет» на своем официальном сайте в течение двух рабочих дней со дня получения экспертного заключения.

(Часть 5 введена Федеральным законом от 28.07.2012 № 139-ФЗ.)

6. Повторное проведение экспертизы конкретной информационной продукции допускается в порядке, установленном процессуальным законодательством, при рассмотрении судом споров, связанных с результатами проведенной экспертизы информационной продукции.

(Часть 6 введена Федеральным законом от 28.07.2012 № 139-ФЗ.)

### **СТАТЬЯ 19.** ПРАВОВЫЕ ПОСЛЕДСТВИЯ ЭКСПЕРТИЗЫ ИНФОРМАЦИОННОЙ ПРОДУКЦИИ

В срок не позднее чем пятнадцать дней со дня получения экспертного заключения федеральный орган исполнительной власти, уполномоченный Правительством Российской Федерации, принимает решение:

1) о несоответствии информационной продукции требованиям настоящего Федерального закона и вынесении предписания об устранении выявленного нарушения в случае, если в экспертном заключении содержится вывод о наличии в данной информационной продукции информации, причиняющей вред здоровью и (или) развитию детей, либо о несоответствии знака

информационной продукции определенной категории информационной продукции;

2) о соответствии информационной продукции требованиям настоящего Федерального закона и об отказе в вынесении указанного в пункте 1 настоящей части предписания.

## Глава 5. Государственный надзор и общественный контроль за соблюдением законодательства Российской Федерации о защите детей от информации, причиняющей вред их здоровью и (или) развитию (в ред. Федеральных законов от 28.07.2012 № 139-ФЗ, от 14.10.2014 № 307-ФЗ)

### **Статья 20.** Государственный надзор за соблюдением законодательства Российской Федерации о защите детей от информации, причиняющей вред их здоровью и (или) развитию (в ред. Федеральных законов от 28.07.2012 № 139-ФЗ, от 14.10.2014 № 307-ФЗ)

1. Государственный надзор за соблюдением законодательства Российской Федерации о защите детей от информации, причиняющей вред их здоровью и (или) развитию, осуществляют в пределах своей компетенции федеральный орган исполнительной власти, осуществляющий функции по контролю и надзору в сфере средств массовой информации, в том числе электронных, и массовых коммуникаций, информационных технологий и связи, федеральный орган исполнительной власти, осуществляющий федеральный государственный надзор в области защиты прав потребителей, и федеральный орган исполнительной власти, осуществляющий функции по контролю и надзору в сфере образования и науки.

(Часть 1 в ред. Федерального закона от 14.10.2014 № 307-ФЗ.)

2. Утратил силу. — Федеральный закон от 14.10.2014 № 307-ФЗ.

### **СТАТЬЯ 21.** ОБЩЕСТВЕННЫЙ КОНТРОЛЬ В СФЕРЕ ЗАЩИТЫ ДЕТЕЙ ОТ ИНФОРМАЦИИ, ПРИЧИНЯЮЩЕЙ ВРЕД ИХ ЗДОРОВЬЮ И (ИЛИ) РАЗВИТИЮ

1. Зарегистрированные в установленном федеральным законом порядке общественные объединения и иные некоммерческие организации в соответствии с их уставами, а также граждане вправе осуществлять в соответствии с законодательством Российской Федерации общественный контроль за соблюдением требований настоящего Федерального закона.

2. При осуществлении общественного контроля общественные объединения и иные некоммерческие организации, граждане вправе осуществлять мониторинг оборота информационной продукции и доступа детей к информации, в том числе посредством создания «горячих линий».

(Часть 2 в ред. Федерального закона от 28.07.2012 № 139-ФЗ.)

## Глава 6. Ответственность за правонарушения в сфере защиты детей от информации, причиняющей вред их здоровью и (или) развитию

### **СТАТЬЯ 22.** ОТВЕТСТВЕННОСТЬ ЗА ПРАВОНАРУШЕНИЯ В СФЕРЕ ЗАЩИТЫ ДЕТЕЙ ОТ ИНФОРМАЦИИ, ПРИЧИНЯЮЩЕЙ ВРЕД ИХ ЗДОРОВЬЮ И (ИЛИ) РАЗВИТИЮ

Нарушение законодательства Российской Федерации о защите детей от информации, причиняющей вред их здоровью и (или) развитию, влечет за собой ответственность в соответствии с законодательством Российской Федерации.

## Глава 7. Заключительные положения

### **СТАТЬЯ 23.** ПОРЯДОК ВСТУПЛЕНИЯ В СИЛУ НАСТОЯЩЕГО ФЕДЕРАЛЬНОГО ЗАКОНА

1. Настоящий Федеральный закон вступает в силу с 1 сентября 2012 года.

2. Положения части 1 статьи 12 настоящего Федерального закона не распространяются на печатную продукцию, выпущенную в оборот до дня вступления в силу настоящего Федерального закона.

# Федеральный закон «Об образовании в Российской Федерации» (извлечения)

## Глава 1. Общие положения

### **СТАТЬЯ 2.** ОСНОВНЫЕ ПОНЯТИЯ, ИСПОЛЬЗУЕМЫЕ В НАСТОЯЩЕМ ФЕДЕРАЛЬНОМ ЗАКОНЕ

<…> 15) Обучающийся — физическое лицо, осваивающее образовательную программу;

16) обучающийся с ограниченными возможностями здоровья — физическое лицо, имеющее недостатки в физическом и (или) психологическом развитии, подтвержденные психолого-медико-педагогической комиссией и препятствующие получению образования без создания специальных условий; <…>

21) педагогический работник — физическое лицо, которое состоит в трудовых, служебных отношениях с организацией, осуществляющей образовательную деятельность, и выполняет обязанности по обучению, воспитанию обучающихся и (или) организации образовательной деятельности; <…>

26) средства обучения и воспитания — приборы, оборудование, включая спортивное оборудование и инвентарь, инструменты (в том числе музыкальные), учебно-наглядные пособия, компьютеры, информационно-телекоммуникационные сети, аппаратно-программные и аудиовизуальные средства, печатные и электронные образовательные и информационные ресурсы и иные материальные объекты, необходимые для организации образовательной деятельности; <…>

31) участники образовательных отношений — обучающиеся, родители (законные представители) несовершеннолетних обучающихся, педагогические работники и их представители, организации, осуществляющие образовательную деятельность;

**СТАТЬЯ 16.** РЕАЛИЗАЦИЯ ОБРАЗОВАТЕЛЬНЫХ ПРОГРАММ С ПРИМЕНЕНИЕМ ЭЛЕКТРОННОГО ОБУЧЕНИЯ И ДИСТАНЦИОННЫХ ОБРАЗОВАТЕЛЬНЫХ ТЕХНОЛОГИЙ

1. Под электронным обучением понимается организация образовательной деятельности с применением содержащейся в базах данных и используемой при реализации образовательных программ информации и обеспечивающих ее обработку информационных технологий, технических средств, а также информационно-телекоммуникационных сетей, обеспечивающих передачу по линиям связи указанной информации, взаимодействие обучающихся и педагогических работников. Под дистанционными образовательными технологиями понимаются образовательные технологии, реализуемые в основном с применением информационно-телекоммуникационных сетей при опосредованном (на расстоянии) взаимодействии обучающихся и педагогических работников.

2. Организации, осуществляющие образовательную деятельность, вправе применять электронное обучение, дистанционные образовательные технологии при реализации образовательных программ в порядке, установленном федеральным органом исполнительной власти, осуществляющим функции по выработке государственной политики и нормативно-правовому регулированию в сфере образования.

3. При реализации образовательных программ с применением исключительно электронного обучения, дистанционных образовательных технологий в организации, осуществляющей образовательную деятельность, должны быть созданы условия для функционирования электронной информационно-образовательной среды, включающей в себя электронные информационные ресурсы, электронные образовательные ресурсы, совокупность информационных технологий, телекоммуникационных технологий, соответствующих технологических средств и обеспечивающей освоение обучающимися образовательных программ в полном объеме независимо от места нахождения обучающихся. Перечень профессий, специальностей и направлений подготовки, реализация образовательных программ по кото-

рым не допускается с применением исключительно электронного обучения, дистанционных образовательных технологий, утверждается федеральным органом исполнительной власти, осуществляющим функции по выработке государственной политики и нормативно-правовому регулированию в сфере образования.

4. При реализации образовательных программ с применением электронного обучения, дистанционных образовательных технологий местом осуществления образовательной деятельности является место нахождения организации, осуществляющей образовательную деятельность, или ее филиала независимо от места нахождения обучающихся.

5. При реализации образовательных программ с применением электронного обучения, дистанционных образовательных технологий организация, осуществляющая образовательную деятельность, обеспечивает защиту сведений, составляющих государственную или иную охраняемую законом тайну.

### **СТАТЬЯ 18.** ПЕЧАТНЫЕ И ЭЛЕКТРОННЫЕ ОБРАЗОВАТЕЛЬНЫЕ И ИНФОРМАЦИОННЫЕ РЕСУРСЫ

1. В организациях, осуществляющих образовательную деятельность, в целях обеспечения реализации образовательных программ формируются библиотеки, в том числе цифровые (электронные) библиотеки, обеспечивающие доступ к профессиональным базам данных, информационным справочным и поисковым системам, а также иным информационным ресурсам. Библиотечный фонд должен быть укомплектован печатными и (или) электронными учебными изданиями (включая учебники и учебные пособия), методическими и периодическими изданиями по всем входящим в реализуемые основные образовательные программы учебным предметам, курсам, дисциплинам (модулям).

### **СТАТЬЯ 35.** ПОЛЬЗОВАНИЕ УЧЕБНИКАМИ, УЧЕБНЫМИ ПОСОБИЯМИ, СРЕДСТВАМИ ОБУЧЕНИЯ И ВОСПИТАНИЯ

1. Обучающимся, осваивающим основные образовательные программы за счет бюджетных ассигнований федерального бюджета, бюджетов субъектов Россий-

ской Федерации и местных бюджетов в пределах федеральных государственных образовательных стандартов, образовательных стандартов, организациями, осуществляющими образовательную деятельность, бесплатно предоставляются в пользование на время получения образования учебники и учебные пособия, а также учебно-методические материалы, средства обучения и воспитания.

2. Обеспечение учебниками и учебными пособиями, а также учебно-методическими материалами, средствами обучения и воспитания организаций, осуществляющих образовательную деятельность по основным образовательным программам, в пределах федеральных государственных образовательных стандартов, образовательных стандартов осуществляется за счет бюджетных ассигнований федерального бюджета, бюджетов субъектов Российской Федерации и местных бюджетов.

3. Пользование учебниками и учебными пособиями обучающимися, осваивающими учебные предметы, курсы, дисциплины (модули) за пределами федеральных государственных образовательных стандартов, образовательных стандартов и (или) получающими платные образовательные услуги, осуществляется в порядке, установленном организацией, осуществляющей образовательную деятельность.

### **СТАТЬЯ 43.** ОБЯЗАННОСТИ И ОТВЕТСТВЕННОСТЬ ОБУЧАЮЩИХСЯ

1. Обучающиеся обязаны:

<…> 5) бережно относиться к имуществу организации, осуществляющей образовательную деятельность.

## Глава 11. Особенности реализации некоторых видов образовательных программ и получения образования отдельными категориями обучающихся

### **СТАТЬЯ 79.** ОРГАНИЗАЦИЯ ПОЛУЧЕНИЯ ОБРАЗОВАНИЯ ОБУЧАЮЩИМИСЯ С ОГРАНИЧЕННЫМИ ВОЗМОЖНОСТЯМИ ЗДОРОВЬЯ

<…> 3. Под специальными условиями для получения образования обучающимися с ограниченными возможностями здоровья в настоящем Федеральном за-

коне понимаются условия обучения, воспитания и развития таких обучающихся, включающие в себя использование специальных образовательных программ и методов обучения и воспитания, специальных учебников, учебных пособий и дидактических материалов, специальных технических средств обучения коллективного и индивидуального пользования, предоставление услуг ассистента (помощника), оказывающего обучающимся необходимую техническую помощь, проведение групповых и индивидуальных коррекционных занятий, обеспечение доступа в здания организаций, осуществляющих образовательную деятельность, и другие условия, без которых невозможно или затруднено освоение образовательных программ обучающимися с ограниченными возможностями здоровья. <...>

11. При получении образования обучающимся с ограниченными возможностями здоровья предоставляются бесплатно специальные учебники и учебные пособия, иная учебная литература, а также услуги сурдопереводчиков и тифлосурдопереводчиков. Указанная мера социальной поддержки является расходным обязательством субъекта Российской Федерации в отношении таких обучающихся, за исключением обучающихся за счет бюджетных ассигнований федерального бюджета. Для инвалидов, обучающихся за счет бюджетных ассигнований федерального бюджета, обеспечение этих мер социальной поддержки является расходным обязательством Российской Федерации.

## Федеральный закон «Об информации, информационных технологиях и о защите информации»

### **СТАТЬЯ 1.** СФЕРА ДЕЙСТВИЯ НАСТОЯЩЕГО ФЕДЕРАЛЬНОГО ЗАКОНА

1. Настоящий Федеральный закон регулирует отношения, возникающие при:

1) осуществлении права на поиск, получение, передачу, производство и распространение информации;

2) применении информационных технологий;

3) обеспечении защиты информации.

2. Положения настоящего Федерального закона не распространяются на отношения, возникающие при правовой охране результатов интеллектуальной деятельности и приравненных к ним средств индивидуализации, за исключением случаев, предусмотренных настоящим Федеральным законом.

(В ред. Федерального закона от 02.07.2013 № 187-ФЗ.)

### **СТАТЬЯ 2.** ОСНОВНЫЕ ПОНЯТИЯ, ИСПОЛЬЗУЕМЫЕ В НАСТОЯЩЕМ ФЕДЕРАЛЬНОМ ЗАКОНЕ

В настоящем Федеральном законе используются следующие основные понятия:

1) информация — сведения (сообщения, данные) независимо от формы их представления;

2) информационные технологии — процессы, методы поиска, сбора, хранения, обработки, предоставления, распространения информации и способы осуществления таких процессов и методов;

3) информационная система — совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств;

4) информационно-телекоммуникационная сеть — технологическая система, предназначенная для передачи по линиям связи информации, доступ к которой осуществляется с использованием средств вычислительной техники;

5) обладатель информации — лицо, самостоятельно создавшее информацию либо получившее на основании закона или договора право разрешать или ограничивать доступ к информации, определяемой по каким-либо признакам;

6) доступ к информации — возможность получения информации и ее использования;

7) конфиденциальность информации — обязательное для выполнения лицом, получившим доступ к определенной информации, требование не передавать такую информацию третьим лицам без согласия ее обладателя;

8) предоставление информации — действия, направленные на получение информации определенным кругом лиц или передачу информации определенному кругу лиц;

9) распространение информации — действия, направленные на получение информации неопределенным кругом лиц или передачу информации неопределенному кругу лиц;

10) электронное сообщение — информация, переданная или полученная пользователем информационно-телекоммуникационной сети;

11) документированная информация — зафиксированная на материальном носителе путем документирования информация с реквизитами, позволяющими определить такую информацию или в установленных законодательством Российской Федерации случаях ее материальный носитель;

11.1) электронный документ — документированная информация, представленная в электронной форме, то есть в виде, пригодном для восприятия человеком с использованием электронных вычислительных машин, а также для передачи по информационно-телекоммуникационным сетям или обработки в информационных системах (п. 11.1 введен Федеральным законом от 27.07.2010 № 227-ФЗ);

12) оператор информационной системы — гражданин или юридическое лицо, осуществляющие деятельность по эксплуатации информационной системы, в том числе по обработке информации, содержащейся в ее базах данных;

13) сайт в сети «Интернет» — совокупность программ для электронных вычислительных машин и иной информации, содержащейся в информационной системе, доступ к которой обеспечивается посредством информационно-телекоммуникационной сети «Интернет» (далее — сеть «Интернет») по доменным именам и (или) по сетевым адресам, позволяющим идентифицировать сайты в сети «Интернет» (п. 13 введен Федеральным законом от 28.07.2012 № 139-ФЗ, в ред. Федерального закона от 07.06.2013 № 112-ФЗ);

14) страница сайта в сети «Интернет» (далее также — интернет-страница) — часть сайта в сети «Интернет», доступ к которой осуществляется по указателю, состоящему из доменного имени и символов, определенных владельцем сайта в сети «Интернет» (п. 14 введен Федеральным законом от 28.07.2012 № 139-ФЗ);

15) доменное имя — обозначение символами, предназначенное для адресации сайтов в сети «Интернет» в целях обеспечения доступа к информации, размещенной в сети «Интернет» (п. 15 введен Федеральным законом от 28.07.2012 № 139-ФЗ);

16) сетевой адрес — идентификатор в сети передачи данных, определяющий при оказании телематических услуг связи абонентский терминал или иные средства связи, входящие в информационную систему (п. 16 введен Федеральным законом от 28.07.2012 № 139-ФЗ);

17) владелец сайта в сети «Интернет» — лицо, самостоятельно и по своему усмотрению определяющее порядок использования сайта в сети «Интернет», в том числе порядок размещения информации на таком сайте (п. 17 введен Федеральным законом от 28.07.2012 № 139-ФЗ);

18) провайдер хостинга — лицо, оказывающее услуги по предоставлению вычислительной мощности для размещения информации в информационной системе, постоянно подключенной к сети «Интернет» (п. 18 введен Федеральным законом от 28.07.2012 № 139-ФЗ);

19) единая система идентификации и аутентификации — федеральная государственная информационная система, порядок использования которой устанавливается Правительством Российской Федерации и которая

обеспечивает в случаях, предусмотренных законодательством Российской Федерации, санкционированный доступ к информации, содержащейся в информационных системах (п. 19 введен Федеральным законом от 07.06.2013 № 112-ФЗ);

20) поисковая система — информационная система, осуществляющая по запросу пользователя поиск в сети «Интернет» информации определенного содержания и предоставляющая пользователю сведения об указателе страницы сайта в сети «Интернет» для доступа к запрашиваемой информации, расположенной на сайтах в сети «Интернет», принадлежащих иным лицам, за исключением информационных систем, используемых для осуществления государственных и муниципальных функций, оказания государственных и муниципальных услуг, а также для осуществления иных публичных полномочий, установленных федеральными законами (п. 20 введен Федеральным законом от 13.07.2015 № 264-ФЗ).

### **СТАТЬЯ 3.** ПРИНЦИПЫ ПРАВОВОГО РЕГУЛИРОВАНИЯ ОТНОШЕНИЙ В СФЕРЕ ИНФОРМАЦИИ, ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ И ЗАЩИТЫ ИНФОРМАЦИИ

Правовое регулирование отношений, возникающих в сфере информации, информационных технологий и защиты информации, основывается на следующих принципах:

1) свобода поиска, получения, передачи, производства и распространения информации любым законным способом;

2) установление ограничений доступа к информации только федеральными законами;

3) открытость информации о деятельности государственных органов и органов местного самоуправления и свободный доступ к такой информации, кроме случаев, установленных федеральными законами;

4) равноправие языков народов Российской Федерации при создании информационных систем и их эксплуатации;

5) обеспечение безопасности Российской Федерации при создании информационных систем, их эксплуатации и защите содержащейся в них информации;

6) достоверность информации и своевременность ее предоставления;

7) неприкосновенность частной жизни, недопустимость сбора, хранения, использования и распространения информации о частной жизни лица без его согласия;

8) недопустимость установления нормативными правовыми актами каких-либо преимуществ применения одних информационных технологий перед другими, если только обязательность применения определенных информационных технологий для создания и эксплуатации государственных информационных систем не установлена федеральными законами.

### **СТАТЬЯ 4.** ЗАКОНОДАТЕЛЬСТВО РОССИЙСКОЙ ФЕДЕРАЦИИ ОБ ИНФОРМАЦИИ, ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЯХ И О ЗАЩИТЕ ИНФОРМАЦИИ

1. Законодательство Российской Федерации об информации, информационных технологиях и о защите информации основывается на Конституции Российской Федерации, международных договорах Российской Федерации и состоит из настоящего Федерального закона и других регулирующих отношения по использованию информации федеральных законов.

2. Правовое регулирование отношений, связанных с организацией и деятельностью средств массовой информации, осуществляется в соответствии с законодательством Российской Федерации о средствах массовой информации.

3. Порядок хранения и использования включенной в состав архивных фондов документированной информации устанавливается законодательством об архивном деле в Российской Федерации.

### **СТАТЬЯ 5.** ИНФОРМАЦИЯ КАК ОБЪЕКТ ПРАВОВЫХ ОТНОШЕНИЙ

1. Информация может являться объектом публичных, гражданских и иных правовых отношений. Ин-

формация может свободно использоваться любым лицом и передаваться одним лицом другому лицу, если федеральными законами не установлены ограничения доступа к информации либо иные требования к порядку ее предоставления или распространения.

2. Информация в зависимости от категории доступа к ней подразделяется на общедоступную информацию, а также на информацию, доступ к которой ограничен федеральными законами (информация ограниченного доступа).

3. Информация в зависимости от порядка ее предоставления или распространения подразделяется на:

1) информацию, свободно распространяемую;

2) информацию, предоставляемую по соглашению лиц, участвующих в соответствующих отношениях;

3) информацию, которая в соответствии с федеральными законами подлежит предоставлению или распространению;

4) информацию, распространение которой в Российской Федерации ограничивается или запрещается.

4. Законодательством Российской Федерации могут быть установлены виды информации в зависимости от ее содержания или обладателя.

### **СТАТЬЯ 6.** ОБЛАДАТЕЛЬ ИНФОРМАЦИИ

1. Обладателем информации может быть гражданин (физическое лицо), юридическое лицо, Российская Федерация, субъект Российской Федерации, муниципальное образование.

2. От имени Российской Федерации, субъекта Российской Федерации, муниципального образования правомочия обладателя информации осуществляются соответственно государственными органами и органами местного самоуправления в пределах их полномочий, установленных соответствующими нормативными правовыми актами.

3. Обладатель информации, если иное не предусмотрено федеральными законами, вправе:

1) разрешать или ограничивать доступ к информации, определять порядок и условия такого доступа;

2) использовать информацию, в том числе распространять ее, по своему усмотрению;

3) передавать информацию другим лицам по договору или на ином установленном законом основании;

4) защищать установленными законом способами свои права в случае незаконного получения информации или ее незаконного использования иными лицами;

5) осуществлять иные действия с информацией или разрешать осуществление таких действий.

4. Обладатель информации при осуществлении своих прав обязан:

1) соблюдать права и законные интересы иных лиц;

2) принимать меры по защите информации;

3) ограничивать доступ к информации, если такая обязанность установлена федеральными законами.

### **СТАТЬЯ 7.** ОБЩЕДОСТУПНАЯ ИНФОРМАЦИЯ

1. К общедоступной информации относятся общеизвестные сведения и иная информация, доступ к которой не ограничен.

2. Общедоступная информация может использоваться любыми лицами по их усмотрению при соблюдении установленных федеральными законами ограничений в отношении распространения такой информации.

3. Обладатель информации, ставшей общедоступной по его решению, вправе требовать от лиц, распространяющих такую информацию, указывать себя в качестве источника такой информации.

4. Информация, размещаемая ее обладателями в сети «Интернет» в формате, допускающем автоматизированную обработку без предварительных изменений человеком в целях повторного ее использования, является общедоступной информацией, размещаемой в форме открытых данных.

(Часть 4 введена Федеральным законом от 07.06.2013 № 112-ФЗ.)

5. Информация в форме открытых данных размещается в сети «Интернет» с учетом требований законодательства Российской Федерации о государственной тайне. В случае, если размещение информации в форме

открытых данных может привести к распространению сведений, составляющих государственную тайну, размещение указанной информации в форме открытых данных должно быть прекращено по требованию органа, наделенного полномочиями по распоряжению такими сведениями.

(Часть 5 введена Федеральным законом от 07.06.2013 № 112-ФЗ.)

6. В случае, если размещение информации в форме открытых данных может повлечь за собой нарушение прав обладателей информации, доступ к которой ограничен в соответствии с федеральными законами, или нарушение прав субъектов персональных данных, размещение указанной информации в форме открытых данных должно быть прекращено по решению суда. В случае, если размещение информации в форме открытых данных осуществляется с нарушением требований Федерального закона от 27 июля 2006 года № 152-ФЗ «О персональных данных», размещение информации в форме открытых данных должно быть приостановлено или прекращено по требованию уполномоченного органа по защите прав субъектов персональных данных.

(Часть 6 введена Федеральным законом от 07.06.2013 № 112-ФЗ.)

### **СТАТЬЯ 8.** ПРАВО НА ДОСТУП К ИНФОРМАЦИИ

1. Граждане (физические лица) и организации (юридические лица) (далее — организации) вправе осуществлять поиск и получение любой информации в любых формах и из любых источников при условии соблюдения требований, установленных настоящим Федеральным законом и другими федеральными законами.

2. Гражданин (физическое лицо) имеет право на получение от государственных органов, органов местного самоуправления, их должностных лиц в порядке, установленном законодательством Российской Федерации, информации, непосредственно затрагивающей его права и свободы.

3. Организация имеет право на получение от государственных органов, органов местного самоуправле-

ния информации, непосредственно касающейся прав и обязанностей этой организации, а также информации, необходимой в связи с взаимодействием с указанными органами при осуществлении этой организацией своей уставной деятельности.

4. Не может быть ограничен доступ к:

1) нормативным правовым актам, затрагивающим права, свободы и обязанности человека и гражданина, а также устанавливающим правовое положение организаций и полномочия государственных органов, органов местного самоуправления;

2) информации о состоянии окружающей среды;

3) информации о деятельности государственных органов и органов местного самоуправления, а также об использовании бюджетных средств (за исключением сведений, составляющих государственную или служебную тайну);

4) информации, накапливаемой в открытых фондах библиотек, музеев и архивов, а также в государственных, муниципальных и иных информационных системах, созданных или предназначенных для обеспечения граждан (физических лиц) и организаций такой информацией;

5) иной информации, недопустимость ограничения доступа к которой установлена федеральными законами.

5. Государственные органы и органы местного самоуправления обязаны обеспечивать доступ, в том числе с использованием информационно-телекоммуникационных сетей, в том числе сети «Интернет», к информации о своей деятельности на русском языке и государственном языке соответствующей республики в составе Российской Федерации в соответствии с федеральными законами, законами субъектов Российской Федерации и нормативными правовыми актами органов местного самоуправления. Лицо, желающее получить доступ к такой информации, не обязано обосновывать необходимость ее получения.

(В ред. Федерального закона от 27.07.2010 № 227-ФЗ.)

6. Решения и действия (бездействие) государственных органов и органов местного самоуправления, общественных объединений, должностных лиц, нарушающие право на доступ к информации, могут быть обжалованы в вышестоящий орган или вышестоящему должностному лицу либо в суд.

7. В случае, если в результате неправомерного отказа в доступе к информации, несвоевременного ее предоставления, предоставления заведомо недостоверной или не соответствующей содержанию запроса информации были причинены убытки, такие убытки подлежат возмещению в соответствии с гражданским законодательством.

8. Предоставляется бесплатно информация:

1) о деятельности государственных органов и органов местного самоуправления, размещенная такими органами в информационно-телекоммуникационных сетях;

2) затрагивающая права и установленные законодательством Российской Федерации обязанности заинтересованного лица;

3) иная установленная законом информация.

9. Установление платы за предоставление государственным органом или органом местного самоуправления информации о своей деятельности возможно только в случаях и на условиях, которые установлены федеральными законами.

### **СТАТЬЯ 9.** ОГРАНИЧЕНИЕ ДОСТУПА К ИНФОРМАЦИИ

1. Ограничение доступа к информации устанавливается федеральными законами в целях защиты основ конституционного строя, нравственности, здоровья, прав и законных интересов других лиц, обеспечения обороны страны и безопасности государства.

2. Обязательным является соблюдение конфиденциальности информации, доступ к которой ограничен федеральными законами.

2.1. Порядок идентификации информационных ресурсов в целях принятия мер по ограничению доступа к информационным ресурсам, требования к способам (методам) ограничения такого доступа, применяемым

в соответствии с настоящим Федеральным законом, а также требования к размещаемой информации об ограничении доступа к информационным ресурсам определяются федеральным органом исполнительной власти, осуществляющим функции по контролю и надзору в сфере средств массовой информации, массовых коммуникаций, информационных технологий и связи.

(Часть 2.1 введена Федеральным законом от 29.07.2017 № 276-ФЗ.)

3. Защита информации, составляющей государственную тайну, осуществляется в соответствии с законодательством Российской Федерации о государственной тайне.

4. Федеральными законами устанавливаются условия отнесения информации к сведениям, составляющим коммерческую тайну, служебную тайну и иную тайну, обязательность соблюдения конфиденциальности такой информации, а также ответственность за ее разглашение.

5. Информация, полученная гражданами (физическими лицами) при исполнении ими профессиональных обязанностей или организациями при осуществлении ими определенных видов деятельности (профессиональная тайна), подлежит защите в случаях, если на эти лица федеральными законами возложены обязанности по соблюдению конфиденциальности такой информации.

6. Информация, составляющая профессиональную тайну, может быть предоставлена третьим лицам в соответствии с федеральными законами и (или) по решению суда.

7. Срок исполнения обязанностей по соблюдению конфиденциальности информации, составляющей профессиональную тайну, может быть ограничен только с согласия гражданина (физического лица), предоставившего такую информацию о себе.

8. Запрещается требовать от гражданина (физического лица) предоставления информации о его частной жизни, в том числе информации, составляющей личную или семейную тайну, и получать такую ин-

формацию помимо воли гражданина (физического лица), если иное не предусмотрено федеральными законами.

9. Порядок доступа к персональным данным граждан (физических лиц) устанавливается федеральным законом о персональных данных.

### **СТАТЬЯ 10.** РАСПРОСТРАНЕНИЕ ИНФОРМАЦИИ ИЛИ ПРЕДОСТАВЛЕНИЕ ИНФОРМАЦИИ

1. В Российской Федерации распространение информации осуществляется свободно при соблюдении требований, установленных законодательством Российской Федерации.

2. Информация, распространяемая без использования средств массовой информации, должна включать в себя достоверные сведения о ее обладателе или об ином лице, распространяющем информацию, в форме и в объеме, которые достаточны для идентификации такого лица. Владелец сайта в сети «Интернет» обязан разместить на принадлежащем ему сайте информацию о своих наименовании, месте нахождения и адресе, адресе электронной почты для направления заявления, указанного в статье 15.7 настоящего Федерального закона, а также вправе предусмотреть возможность направления этого заявления посредством заполнения электронной формы на сайте в сети «Интернет».

(В ред. Федерального закона от 24.11.2014 № 364-ФЗ.)

3. При использовании для распространения информации средств, позволяющих определять получателей информации, в том числе почтовых отправлений и электронных сообщений, лицо, распространяющее информацию, обязано обеспечить получателю информации возможность отказа от такой информации.

4. Предоставление информации осуществляется в порядке, который устанавливается соглашением лиц, участвующих в обмене информацией.

5. Случаи и условия обязательного распространения информации или предоставления информации, в том числе предоставление обязательных экземпляров документов, устанавливаются федеральными законами.

6. Запрещается распространение информации, которая направлена на пропаганду войны, разжигание национальной, расовой или религиозной ненависти и вражды, а также иной информации, за распространение которой предусмотрена уголовная или административная ответственность.

### **СТАТЬЯ 10.1.** ОБЯЗАННОСТИ ОРГАНИЗАТОРА РАСПРОСТРАНЕНИЯ ИНФОРМАЦИИ В СЕТИ «ИНТЕРНЕТ»

(введена Федеральным законом от 05.05.2014 № 97-ФЗ)

1. Организатором распространения информации в сети «Интернет» является лицо, осуществляющее деятельность по обеспечению функционирования информационных систем и (или) программ для электронных вычислительных машин, которые предназначены и (или) используются для приема, передачи, доставки и (или) обработки электронных сообщений пользователей сети «Интернет».

2. Организатор распространения информации в сети «Интернет» обязан в установленном Правительством Российской Федерации порядке уведомить федеральный орган исполнительной власти, осуществляющий функции по контролю и надзору в сфере средств массовой информации, массовых коммуникаций, информационных технологий и связи, о начале осуществления деятельности, указанной в части 1 настоящей статьи.

3. Организатор распространения информации в сети «Интернет» обязан хранить на территории Российской Федерации:

1) информацию о фактах приема, передачи, доставки и (или) обработки голосовой информации, письменного текста, изображений, звуков, видео или иных электронных сообщений пользователей сети «Интернет» и информацию об этих пользователях в течение одного года с момента окончания осуществления таких действий;

2) текстовые сообщения пользователей сети «Интернет», голосовую информацию, изображения, звуки, видео, иные электронные сообщения пользователей се-

ти «Интернет» до шести месяцев с момента окончания их приема, передачи, доставки и (или) обработки. Порядок, сроки и объем хранения указанной в настоящем подпункте информации устанавливаются Правительством Российской Федерации.

(Пункт 3 в ред. Федерального закона от 06.07.2016 № 374-ФЗ.)

3.1. Организатор распространения информации в сети «Интернет» обязан предоставлять указанную в части 3 настоящей статьи информацию уполномоченным государственным органам, осуществляющим оперативно-разыскную деятельность или обеспечение безопасности Российской Федерации, в случаях, установленных федеральными законами.

(Пункт 3.1 введен Федеральным законом от 06.07.2016 № 374-ФЗ, в ред. Федерального закона от 29.07.2017 № 241-ФЗ.)

4. Организатор распространения информации в сети «Интернет» обязан обеспечивать реализацию установленных федеральным органом исполнительной власти в области связи по согласованию с уполномоченными государственными органами, осуществляющими оперативно-разыскную деятельность или обеспечение безопасности Российской Федерации, требований к оборудованию и программно-техническим средствам, используемым указанным организатором в эксплуатируемых им информационных системах, для проведения этими органами в случаях, установленных федеральными законами, мероприятий в целях реализации возложенных на них задач, а также принимать меры по недопущению раскрытия организационных и тактических приемов проведения данных мероприятий. Порядок взаимодействия организаторов распространения информации в сети «Интернет» с уполномоченными государственными органами, осуществляющими оперативно-разыскную деятельность или обеспечение безопасности Российской Федерации, устанавливается Правительством Российской Федерации.

4.1. Организатор распространения информации в сети «Интернет» обязан при использовании для приема, передачи, доставки и (или) обработки электрон-

ных сообщений пользователей сети «Интернет» дополнительного кодирования электронных сообщений и (или) при предоставлении пользователям сети «Интернет» возможности дополнительного кодирования электронных сообщений представлять в федеральный орган исполнительной власти в области обеспечения безопасности информацию, необходимую для декодирования принимаемых, передаваемых, доставляемых и (или) обрабатываемых электронных сообщений.

(Пункт 4.1 введен Федеральным законом от 06.07.2016 № 374-ФЗ.)

4.2. Организатор распространения информации в сети «Интернет» в случае осуществления деятельности по обеспечению функционирования информационных систем и (или) программ для электронных вычислительных машин, которые предназначены и (или) используются для обмена электронными сообщениями исключительно между пользователями этих информационных систем и (или) программ для электронных вычислительных машин, при котором отправитель электронного сообщения определяет получателя или получателей электронного сообщения, не предусматриваются размещение пользователями сети «Интернет» общедоступной информации в сети «Интернет» и передача электронных сообщений неопределенному кругу лиц (далее — организатор сервиса обмена мгновенными сообщениями), также обязан:

1) осуществлять идентификацию пользователей сети «Интернет», передачу электронных сообщений которых осуществляет организатор сервиса обмена мгновенными сообщениями (далее — пользователи сервиса обмена мгновенными сообщениями), по абонентскому номеру оператора подвижной радиотелефонной связи в порядке, установленном Правительством Российской Федерации, на основании договора об идентификации, заключенного организатором сервиса обмена мгновенными сообщениями с оператором подвижной радиотелефонной связи, за исключением случаев, предусмотренных настоящим Федеральным законом;

2) в течение суток с момента получения соответствующего требования уполномоченного федерального ор-

гана исполнительной власти ограничить возможность осуществления пользователем сервиса обмена мгновенными сообщениями, указанным в этом требовании, передачи электронных сообщений, содержащих информацию, распространение которой в Российской Федерации запрещено, а также информацию, распространяемую с нарушением требований законодательства Российской Федерации, в порядке, определенном Правительством Российской Федерации;

3) обеспечивать техническую возможность отказа пользователей сервиса обмена мгновенными сообщениями от получения электронных сообщений от других пользователей;

4) обеспечивать конфиденциальность передаваемых электронных сообщений;

5) обеспечивать возможность передачи электронных сообщений по инициативе государственных органов в соответствии с законодательством Российской Федерации;

6) не допускать передачу электронных сообщений пользователям сервиса обмена мгновенными сообщениями в случаях и в порядке, которые определены Правительством Российской Федерации.

(Часть 4.2 введена Федеральным законом от 29.07.2017 № 241-ФЗ.)

4.3. Организатор сервиса обмена мгновенными сообщениями, являющийся российским юридическим лицом или гражданином Российской Федерации, вправе осуществлять идентификацию пользователей сервиса обмена мгновенными сообщениями самостоятельно путем определения абонентского номера подвижной радиотелефонной связи пользователя сервиса обмена мгновенными сообщениями. Правительством Российской Федерации могут устанавливаться требования к порядку определения абонентского номера подвижной радиотелефонной связи пользователя сервиса обмена мгновенными сообщениями организатором сервиса обмена мгновенными сообщениями, являющимся российским юридическим лицом или гражданином Российской Федерации.

(Часть 4.3 введена Федеральным законом от 29.07.2017 № 241-ФЗ.)

4.4. Организатор сервиса обмена мгновенными сообщениями, являющийся российским юридическим лицом или гражданином Российской Федерации, обязан хранить сведения об идентификации абонентского номера подвижной радиотелефонной связи пользователя сервиса обмена мгновенными сообщениями (далее — идентификационные сведения об абонентском номере) только на территории Российской Федерации. Предоставление третьим лицам идентификационных сведений об абонентском номере может осуществляться только с согласия пользователя сервиса обмена мгновенными сообщениями, за исключением случаев, предусмотренных настоящим Федеральным законом и другими федеральными законами. Обязанность предоставить доказательство получения согласия пользователя сервиса обмена мгновенными сообщениями на предоставление третьим лицам идентификационных сведений об абонентском номере данного пользователя сервиса обмена мгновенными сообщениями возлагается на организатора сервиса обмена мгновенными сообщениями.

(Часть 4.4 введена Федеральным законом от 29.07.2017 № 241-ФЗ.)

5. Обязанности, предусмотренные настоящей статьей, не распространяются на операторов государственных информационных систем, операторов муниципальных информационных систем, операторов связи, оказывающих услуги связи на основании соответствующей лицензии, в части лицензируемой деятельности, а также не распространяются на граждан (физических лиц), осуществляющих указанную в части 1 настоящей статьи деятельность для личных, семейных и домашних нужд. Правительством Российской Федерации в целях применения положений настоящей статьи определяется перечень личных, семейных и домашних нужд при осуществлении деятельности, указанной в части 1 настоящей статьи.

6. Состав информации, подлежащей хранению в соответствии с частью 3 настоящей статьи, место и правила ее хранения, порядок ее предоставления уполномоченным государственным органам, осуществляющим оперативно-разыскную деятельность или обеспечение

безопасности Российской Федерации, а также порядок осуществления контроля за деятельностью организаторов распространения информации в сети «Интернет», связанной с хранением такой информации, и федеральный орган исполнительной власти, уполномоченный на осуществление этого контроля, определяются Правительством Российской Федерации.

### **СТАТЬЯ 10.3.** ОБЯЗАННОСТИ ОПЕРАТОРА ПОИСКОВОЙ СИСТЕМЫ

(введена Федеральным законом
от 13.07.2015 № 264-ФЗ)

1. Оператор поисковой системы, распространяющий в сети «Интернет» рекламу, которая направлена на привлечение внимания потребителей, находящихся на территории Российской Федерации, по требованию гражданина (физического лица) (далее в настоящей статье — заявитель) обязан прекратить выдачу сведений об указателе страницы сайта в сети «Интернет» (далее также — ссылка), позволяющих получить доступ к информации о заявителе, распространяемой с нарушением законодательства Российской Федерации, являющейся недостоверной, а также неактуальной, утратившей значение для заявителя в силу последующих событий или действий заявителя, за исключением информации о событиях, содержащих признаки уголовно наказуемых деяний, сроки привлечения к уголовной ответственности по которым не истекли, и информации о совершении гражданином преступления, по которому не снята или не погашена судимость.

2. Требование заявителя должно содержать:

1) фамилию, имя, отчество, паспортные данные, контактную информацию (номера телефона и (или) факса, адрес электронной почты, почтовый адрес);

2) информацию о заявителе, указанную в части 1 настоящей статьи, выдача ссылок на которую подлежит прекращению;

3) указатель страницы сайта в сети «Интернет», на которой размещена информация, указанная в части 1 настоящей статьи;

4) основание для прекращения выдачи ссылок поисковой системой;

5) согласие заявителя на обработку его персональных данных.

3. В случае обнаружения неполноты сведений, неточностей или ошибок в требовании заявителя оператор поисковой системы вправе направить заявителю в течение десяти рабочих дней с момента получения указанного требования уведомление об уточнении представленных сведений. Оператор поисковой системы также вправе направить заявителю уведомление о необходимости предоставления документа, удостоверяющего личность. Указанное уведомление может быть направлено заявителю однократно.

4. В течение десяти рабочих дней с момента получения уведомления, указанного в части 3 настоящей статьи, заявитель принимает меры, направленные на восполнение недостающих сведений, устранение неточностей и ошибок, и направляет оператору поисковой системы уточненные сведения, а также документ, удостоверяющий личность (в случае необходимости).

5. В течение десяти рабочих дней с момента получения требования заявителя или уточненных заявителем сведений (в случае направления заявителю уведомления, указанного в части 3 настоящей статьи) оператор поисковой системы обязан прекратить выдачу ссылок на информацию, указанную в требовании заявителя, при показе результатов поиска по запросам пользователей поисковой системы, содержащих имя и (или) фамилию заявителя, уведомить об этом заявителя или направить заявителю мотивированный отказ.

6. Оператор поисковой системы направляет заявителю уведомление об удовлетворении указанного в части 1 настоящей статьи требования заявителя или мотивированный отказ в его удовлетворении в той же форме, в которой было получено указанное требование.

7. Заявитель, считающий отказ оператора поисковой системы необоснованным, вправе обратиться в суд с исковым заявлением о прекращении выдачи ссылок на информацию, указанную в требовании заявителя.

8. Оператор поисковой системы обязан не раскрывать информацию о факте обращения к нему заявителя

с требованием, указанным в части 1 настоящей статьи, за исключением случаев, установленных федеральными законами.

**СТАТЬЯ 10.4.** ОСОБЕННОСТИ РАСПРОСТРАНЕНИЯ ИНФОРМАЦИИ НОВОСТНЫМ АГРЕГАТОРОМ

(введена Федеральным законом от 23.06.2016 № 208-ФЗ)

1. Владелец программы для электронных вычислительных машин, владелец сайта и (или) страницы сайта в сети «Интернет», которые используются для обработки и распространения новостной информации в сети «Интернет» на государственном языке Российской Федерации, государственных языках республик в составе Российской Федерации или иных языках народов Российской Федерации, на которых может распространяться реклама, направленная на привлечение внимания потребителей, находящихся на территории Российской Федерации, и доступ к которым в течение суток составляет более одного миллиона пользователей сети «Интернет» (далее — владелец новостного агрегатора), обязаны соблюдать требования законодательства Российской Федерации, в частности:

1) не допускать использование программы для электронных вычислительных машин, сайта и (или) страницы сайта в сети «Интернет», которые используются для обработки и распространения новостной информации в сети «Интернет» на государственном языке Российской Федерации, государственных языках республик в составе Российской Федерации или иных языках народов Российской Федерации, на которых может распространяться реклама, направленная на привлечение внимания потребителей, находящихся на территории Российской Федерации, и доступ к которым в течение суток составляет более одного миллиона пользователей сети «Интернет» (далее — новостной агрегатор), в целях совершения уголовно наказуемых деяний, разглашения сведений, составляющих государственную или иную специально охраняемую законом тайну, распространения материалов, содержащих публичные призывы к осуществлению террористической деятель-

ности или публично оправдывающих терроризм, других экстремистских материалов, а также материалов, пропагандирующих порнографию, культ насилия и жестокости, и материалов, содержащих нецензурную брань;

2) проверять достоверность распространяемых общественно значимых сведений до их распространения и незамедлительно прекратить их распространение на основании предписания, указанного в части 9 настоящей статьи;

3) не допускать использование новостного агрегатора в целях сокрытия или фальсификации общественно значимых сведений, распространения недостоверной общественно значимой новостной информации под видом достоверных сообщений, а также распространения информации с нарушением законодательства Российской Федерации;

4) не допускать распространение новостной информации с целью опорочить гражданина или отдельные категории граждан по признакам пола, возраста, расовой или национальной принадлежности, языка, отношения к религии, профессии, места жительства и работы, а также в связи с их политическими убеждениями;

5) не допускать распространение новостной информации о частной жизни гражданина с нарушением гражданского законодательства;

6) соблюдать запреты и ограничения, предусмотренные законодательством Российской Федерации о референдуме и законодательством Российской Федерации о выборах;

7) соблюдать требования законодательства Российской Федерации, регулирующие порядок распространения массовой информации;

8) соблюдать права и законные интересы граждан и организаций, в том числе честь, достоинство и деловую репутацию граждан, деловую репутацию организаций;

9) разместить на новостном агрегаторе адреса электронной почты для направления им юридически значимых сообщений, а также свои фамилию и инициалы

(для физического лица) или наименование (для юридического лица);

10) хранить в течение шести месяцев распространенную ими новостную информацию, сведения об источнике ее получения, а также сведения о сроках ее распространения;

11) обеспечить доступ федерального органа исполнительной власти, осуществляющего функции по контролю и надзору в сфере средств массовой информации, массовых коммуникаций, информационных технологий и связи, к информации, указанной в пункте 10 настоящей части, посредством системы взаимодействия указанного федерального органа исполнительной власти с владельцем новостного агрегатора, порядок функционирования которой устанавливается указанным федеральным органом исполнительной власти;

12) установить одну из предлагаемых федеральным органом исполнительной власти, осуществляющим функции по контролю и надзору в сфере средств массовой информации, массовых коммуникаций, информационных технологий и связи, предназначенных для определения количества пользователей информационным ресурсом в сети «Интернет» программ для электронных вычислительных машин.

(Пункт 12 введен Федеральным законом от 01.05.2017 № 87-ФЗ.)

2. Владелец новостного агрегатора не несет ответственность за распространение им новостной информации в случае, если она является дословным воспроизведением сообщений и материалов или их фрагментов, размещенных на официальном сайте государственного органа в сети «Интернет» или распространенных средством массовой информации, которое может быть установлено и привлечено к ответственности за нарушение законодательства Российской Федерации о средствах массовой информации.

(В ред. Федерального закона от 25.11.2017 № 327-ФЗ.)

3. Федеральный орган исполнительной власти, осуществляющий функции по контролю и надзору в сфере

средств массовой информации, массовых коммуникаций, информационных технологий и связи, ведет реестр новостных агрегаторов. В целях обеспечения формирования реестра новостных агрегаторов федеральный орган исполнительной власти, осуществляющий функции по контролю и надзору в сфере средств массовой информации, массовых коммуникаций, информационных технологий и связи:

1) организует мониторинг информационных ресурсов;

2) утверждает методику определения количества пользователей информационных ресурсов в сутки;

3) вправе запрашивать у владельца новостного агрегатора и иных лиц информацию, необходимую для ведения такого реестра. Указанные лица обязаны предоставлять запрашиваемую информацию не позднее чем в течение десяти дней со дня получения запроса федерального органа исполнительной власти, осуществляющего функции по контролю и надзору в сфере средств массовой информации, массовых коммуникаций, информационных технологий и связи.

4. В случае обнаружения в информационно-телекоммуникационных сетях, в том числе в сети «Интернет», информационного ресурса, на котором происходит обработка и распространение новостной информации в сети «Интернет» на государственном языке Российской Федерации, государственных языках республик в составе Российской Федерации или иных языках народов Российской Федерации, на котором может распространяться реклама, направленная на привлечение внимания потребителей, находящихся на территории Российской Федерации, и доступ к которому в течение суток составляет более одного миллиона пользователей сети «Интернет», включая рассмотрение соответствующих обращений органов государственной власти, органов местного самоуправления, граждан или организаций, федеральный орган исполнительной власти, осуществляющий функции по контролю и надзору в сфере средств массовой информации, массовых коммуникаций, информационных технологий и связи:

1) признает информационный ресурс новостным агрегатором и включает его в реестр новостных агрегаторов;

2) определяет провайдера хостинга или иное обеспечивающее размещение новостного агрегатора в сети «Интернет» лицо;

3) направляет провайдеру хостинга или указанному в пункте 2 настоящей части лицу уведомление в электронном виде на русском и английском языках о необходимости предоставления данных, позволяющих идентифицировать владельца новостного агрегатора;

4) фиксирует дату и время направления указанного в пункте 3 настоящей части уведомления провайдеру хостинга или указанному в пункте 2 настоящей части лицу в соответствующей информационной системе.

5. В течение трех рабочих дней с момента получения уведомления, указанного в пункте 3 части 4 настоящей статьи, провайдер хостинга или указанное в пункте 2 части 4 настоящей статьи лицо обязаны предоставить данные, позволяющие идентифицировать владельца новостного агрегатора.

6. После получения данных, указанных в пункте 3 части 4 настоящей статьи, федеральный орган исполнительной власти, осуществляющий функции по контролю и надзору в сфере средств массовой информации, массовых коммуникаций, информационных технологий и связи, направляет владельцу новостного агрегатора уведомление о включении его информационного ресурса в реестр новостных агрегаторов с указанием требований законодательства Российской Федерации, применимых к данным информационным ресурсам.

7. В случае, если доступ к новостному агрегатору на протяжении трех месяцев составляет в течение суток менее одного миллиона пользователей сети «Интернет», данный новостной агрегатор по заявлению его владельца исключается из реестра новостных агрегаторов, о чем владельцу новостного агрегатора направляется соответствующее уведомление. Данный новостной агрегатор может быть исключен из реестра новостных агрегаторов при отсутствии заявления его владельца,

если доступ к данному новостному агрегатору на протяжении шести месяцев составляет в течение суток менее одного миллиона пользователей сети «Интернет».

8. В случае обнаружения на новостном агрегаторе фактов фальсификации общественно значимых сведений, распространения недостоверной общественно значимой новостной информации под видом достоверных сообщений, а также распространения новостной информации с нарушением законодательства Российской Федерации уполномоченные государственные органы вправе обратиться в федеральный орган исполнительной власти, осуществляющий функции по контролю и надзору в сфере средств массовой информации, массовых коммуникаций, информационных технологий и связи, посредством заполнения электронной формы на официальном сайте федерального органа исполнительной власти, осуществляющего функции по контролю и надзору в сфере средств массовой информации, массовых коммуникаций, информационных технологий и связи, с приложением решения суда или решения указанного государственного органа с требованием принять меры по прекращению распространения такой информации. Форма и порядок направления данного требования и прилагаемых к нему документов определяются федеральным органом исполнительной власти, осуществляющим функции по контролю и надзору в сфере средств массовой информации, массовых коммуникаций, информационных технологий и связи.

9. В случае получения требования, указанного в части 8 настоящей статьи, и прилагаемых к нему документов федеральный орган исполнительной власти, осуществляющий функции по контролю и надзору в сфере средств массовой информации, массовых коммуникаций, информационных технологий и связи, в течение 24 часов с момента их получения рассматривает их и направляет владельцу новостного агрегатора предписание, в том числе посредством системы взаимодействия, указанной в пункте 11 части 1 настоящей статьи, о незамедлительном прекращении распространения информации, указанной в части 8 настоящей статьи.

10. Для целей настоящей статьи под новостной информацией понимается общедоступная информация, полученная из средств массовой информации, зарегистрированных в соответствии с Законом Российской Федерации от 27 декабря 1991 года № 2124-1 «О средствах массовой информации», а также иных источников.

11. Информационные ресурсы, которые зарегистрированы в соответствии с Законом Российской Федерации от 27 декабря 1991 года № 2124-1 «О средствах массовой информации» в качестве сетевых изданий, не являются новостными агрегаторами.

12. Владельцем новостного агрегатора может быть только российское юридическое лицо или гражданин Российской Федерации.

13. Нарушение владельцем новостного агрегатора требований настоящей статьи влечет за собой уголовную, административную или иную ответственность в соответствии с законодательством Российской Федерации.

### **СТАТЬЯ 10.5.** ОБЯЗАННОСТИ ВЛАДЕЛЬЦА АУДИОВИЗУАЛЬНОГО СЕРВИСА

(введена Федеральным законом от 01.05.2017 № 87-ФЗ)

1. Владелец сайта и (или) страницы сайта в сети «Интернет», и (или) информационной системы, и (или) программы для электронных вычислительных машин, которые используются для формирования и (или) организации распространения в сети «Интернет» совокупности аудиовизуальных произведений, доступ к которым предоставляется за плату и (или) при условии просмотра рекламы, направленной на привлечение внимания потребителей, находящихся на территории Российской Федерации, и доступ к которым в течение суток составляет более ста тысяч пользователей сети «Интернет», находящихся на территории Российской Федерации (далее — владелец аудиовизуального сервиса), обязан соблюдать требования законодательства Российской Федерации, в частности:

1) не допускать использование сайта и (или) страницы сайта в сети «Интернет», и (или) информационной системы, и (или) программы для электронных вычис-

лительных машин, которые используются для формирования и (или) организации распространения в сети «Интернет» совокупности аудиовизуальных произведений, доступ к которым предоставляется за плату и (или) при условии просмотра рекламы, направленной на привлечение внимания потребителей, находящихся на территории Российской Федерации, и доступ к которым в течение суток составляет более ста тысяч пользователей сети «Интернет», находящихся на территории Российской Федерации (далее — аудиовизуальный сервис), в целях совершения уголовно наказуемых деяний, разглашения сведений, составляющих государственную или иную специально охраняемую законом тайну, распространения материалов, содержащих публичные призывы к осуществлению террористической деятельности или публично оправдывающих терроризм, других экстремистских материалов, а также материалов, пропагандирующих порнографию, культ насилия и жестокости, и материалов, содержащих нецензурную брань;

2) осуществлять в соответствии с требованиями Федерального закона от 29 декабря 2010 года № 436-ФЗ «О защите детей от информации, причиняющей вред их здоровью и развитию» классификацию аудиовизуальных произведений до начала их распространения в случае, если классификация соответствующего аудиовизуального произведения не была осуществлена ранее его производителем или распространителем, а также обеспечивать обозначение категории данного аудиовизуального произведения соответствующим знаком информационной продукции и (или) текстовым предупреждением об ограничении распространения среди детей информационной продукции, причиняющей вред их здоровью и (или) развитию, за исключением аудиовизуальных произведений, размещаемых на таком аудиовизуальном сервисе его пользователями;

3) соблюдать запреты и ограничения, предусмотренные законодательством Российской Федерации о референдуме и законодательством Российской Федерации о выборах;

4) соблюдать требования законодательства Российской Федерации, регулирующие порядок распространения массовой информации;

5) не допускать распространения аудиовизуальным сервисом телеканалов или телепрограмм, не зарегистрированных в соответствии с Законом Российской Федерации от 27 декабря 1991 года № 2124-1 «О средствах массовой информации»;

6) разместить на аудиовизуальном сервисе адрес электронной почты для направления ему юридически значимых сообщений, а также свои фамилию и инициалы (для физического лица) или наименование (для юридического лица);

7) установить одну из предлагаемых федеральным органом исполнительной власти, осуществляющим функции по контролю и надзору в сфере средств массовой информации, массовых коммуникаций, информационных технологий и связи, предназначенных для определения количества пользователей информационным ресурсом в сети «Интернет» программ для электронных вычислительных машин.

2. Федеральный орган исполнительной власти, осуществляющий функции по контролю и надзору в сфере средств массовой информации, массовых коммуникаций, информационных технологий и связи, ведет реестр аудиовизуальных сервисов. В целях обеспечения формирования реестра аудиовизуальных сервисов федеральный орган исполнительной власти, осуществляющий функции по контролю и надзору в сфере средств массовой информации, массовых коммуникаций, информационных технологий и связи:

1) организует мониторинг информационных ресурсов;

2) утверждает методику определения количества пользователей информационных ресурсов в сутки;

3) вправе запрашивать у владельца аудиовизуального сервиса и иных лиц информацию, необходимую для ведения такого реестра. Указанные лица обязаны предоставлять запрашиваемую информацию не позднее чем в течение десяти дней со дня получения запроса федерального органа исполнительной власти, осущест-

вляющего функции по контролю и надзору в сфере средств массовой информации, массовых коммуникаций, информационных технологий и связи.

3. В случае обнаружения в сети «Интернет» информационного ресурса, который используется для формирования и (или) организации распространения в сети «Интернет» совокупности аудиовизуальных произведений, доступ к которым предоставляется за плату и (или) при условии просмотра рекламы, направленной на привлечение внимания потребителей, находящихся на территории Российской Федерации, и доступ к которым в течение суток составляет более ста тысяч пользователей сети «Интернет», находящихся на территории Российской Федерации, включая рассмотрение соответствующих обращений органов государственной власти, органов местного самоуправления, граждан или организаций, федеральный орган исполнительной власти, осуществляющий функции по контролю и надзору в сфере средств массовой информации, массовых коммуникаций, информационных технологий и связи:

1) признает информационный ресурс аудиовизуальным сервисом и включает его в реестр аудиовизуальных сервисов;

2) определяет провайдера хостинга или иное обеспечивающее размещение аудиовизуального сервиса в сети «Интернет» лицо;

3) направляет провайдеру хостинга или указанному в пункте 2 настоящей части лицу уведомление в электронном виде на русском и английском языках о необходимости предоставления данных, позволяющих идентифицировать владельца аудиовизуального сервиса;

4) фиксирует дату и время направления указанного в пункте 3 настоящей части уведомления провайдеру хостинга или указанному в пункте 2 настоящей части лицу в соответствующей информационной системе.

4. В течение трех рабочих дней с момента получения уведомления, указанного в пункте 3 части 3 настоящей статьи, провайдер хостинга или указанное в пункте 2 части 3 настоящей статьи лицо обязаны предоставить

данные, позволяющие идентифицировать владельца аудиовизуального сервиса.

5. После получения данных, указанных в пункте 3 части 3 настоящей статьи, федеральный орган исполнительной власти, осуществляющий функции по контролю и надзору в сфере средств массовой информации, массовых коммуникаций, информационных технологий и связи, направляет владельцу аудиовизуального сервиса уведомление о включении его информационного ресурса в реестр аудиовизуальных сервисов с указанием требований законодательства Российской Федерации, применимых к данным информационным ресурсам.

6. Владелец аудиовизуального сервиса, получивший указанное в части 5 настоящей статьи уведомление, обязан в течение двух месяцев со дня его получения предоставить в федеральный орган исполнительной власти, осуществляющий функции по контролю и надзору в сфере средств массовой информации, массовых коммуникаций, информационных технологий и связи, документы, свидетельствующие о соблюдении требований части 7 настоящей статьи.

7. Владельцем аудиовизуального сервиса может выступать российское юридическое лицо или гражданин Российской Федерации, не имеющий гражданства другого государства. Если иное не предусмотрено международным договором Российской Федерации, иностранное государство, международная организация, а также находящаяся под их контролем организация, иностранное юридическое лицо, российское юридическое лицо, доля иностранного участия в уставном капитале которого составляет более двадцати процентов, иностранный гражданин, лицо без гражданства, гражданин Российской Федерации, имеющий гражданство другого государства, их аффилированные лица, в совокупности или каждый в отдельности владеющие информационным ресурсом, который используется для распространения в сети «Интернет» совокупности аудиовизуальных произведений и количество пользователей которого на территории Российской Федерации составляет менее пятидесяти процентов от

общего количества пользователей такого информационного ресурса, вправе осуществлять владение, управление либо контроль прямо или косвенно в отношении более чем двадцати процентов долей (акций) в уставном капитале владельца аудиовизуального сервиса при условии согласования указанных владения, управления либо контроля с правительственной комиссией.

8. Правительственная комиссия принимает решение о согласовании владения, управления либо контроля, указанных в части 7 настоящей статьи, при условии, что такие владение, управление либо контроль в отношении владельца аудиовизуального сервиса будут способствовать развитию рынка аудиовизуальных сервисов в Российской Федерации.

9. Положение о правительственной комиссии, ее состав и порядок принятия ею решений утверждаются Правительством Российской Федерации.

10. Положения части 7 настоящей статьи не распространяются на хозяйственные общества, имеющие стратегическое значение для обеспечения обороны страны и безопасности государства и осуществляющие деятельность, указанную в пунктах 11—14, 34, 37 статьи 6 Федерального закона от 29 апреля 2008 года № 57-ФЗ «О порядке осуществления иностранных инвестиций в хозяйственные общества, имеющие стратегическое значение для обеспечения обороны страны и безопасности государства», и (или) лиц, входящих с такими хозяйственными обществами в одну группу лиц, в части соблюдения требований об ограничении владения, управления либо контроля в отношении владельца аудиовизуального сервиса.

11. Перечень документов, свидетельствующих о соблюдении владельцем аудиовизуального сервиса требований части 7 настоящей статьи, а также форма и порядок направления в федеральный орган исполнительной власти, осуществляющий функции по контролю и надзору в сфере средств массовой информации, массовых коммуникаций, информационных технологий и связи, таких документов утверждаются Правительством Российской Федерации.

12. В случае, если доступ к аудиовизуальному сервису на протяжении трех месяцев составляет в течение суток менее ста тысяч пользователей сети «Интернет», данный аудиовизуальный сервис по заявлению его владельца исключается из реестра аудиовизуальных сервисов, о чем владельцу аудиовизуального сервиса направляется соответствующее уведомление. Данный аудиовизуальный сервис может быть исключен из реестра аудиовизуальных сервисов при отсутствии заявления его владельца, если доступ к данному аудиовизуальному сервису на протяжении шести месяцев составляет в течение суток менее ста тысяч пользователей сети «Интернет».

13. В случае обнаружения на аудиовизуальном сервисе информации, распространяемой с нарушением законодательства Российской Федерации, федеральный орган исполнительной власти, осуществляющий функции по контролю и надзору в сфере средств массовой информации, массовых коммуникаций, информационных технологий и связи, направляет владельцу аудиовизуального сервиса требование принять меры по устранению выявленных нарушений законодательства Российской Федерации.

14. Федеральный орган исполнительной власти, осуществляющий функции по контролю и надзору в сфере средств массовой информации, массовых коммуникаций, информационных технологий и связи, обращается в суд с заявлением об ограничении доступа к аудиовизуальному сервису в случае:

1) установленного вступившим в законную силу постановлением по делу об административном правонарушении повторного в течение года неисполнения владельцем аудиовизуального сервиса требования принять меры по устранению выявленных нарушений законодательства Российской Федерации;

2) неисполнения владельцем аудиовизуального сервиса требований, предусмотренных частями 6 и 7 настоящей статьи.

15. На основании вступившего в законную силу решения суда до исполнения владельцем аудиовизуального сервиса требований, предусмотренных частями 6

и 7 настоящей статьи, доступ к аудиовизуальному сервису ограничивается оператором связи, оказывающим услуги по предоставлению доступа к сети «Интернет». Порядок взаимодействия федерального органа исполнительной власти, осуществляющего функции по контролю и надзору в сфере средств массовой информации, массовых коммуникаций, информационных технологий и связи, с оператором связи, владельцем аудиовизуального сервиса, а также порядок ограничения и возобновления доступа к аудиовизуальному сервису и порядок информирования о таком ограничении устанавливаются Правительством Российской Федерации.

16. Не являются аудиовизуальными сервисами:

1) информационные ресурсы, которые зарегистрированы в соответствии с Законом Российской Федерации от 27 декабря 1991 года № 2124-1 «О средствах массовой информации» в качестве сетевых изданий;

2) поисковые системы;

3) информационные ресурсы, на которых аудиовизуальные произведения размещаются преимущественно пользователями сети «Интернет». Порядок и критерии определения таких информационных ресурсов утверждаются федеральным органом исполнительной власти, осуществляющим функции по контролю и надзору в сфере средств массовой информации, массовых коммуникаций, информационных технологий и связи.

17. Нарушение владельцем аудиовизуального сервиса требований настоящей статьи влечет за собой уголовную, административную или иную ответственность в соответствии с законодательством Российской Федерации.

### **СТАТЬЯ 11.** ДОКУМЕНТИРОВАНИЕ ИНФОРМАЦИИ

1. Законодательством Российской Федерации или соглашением сторон могут быть установлены требования к документированию информации.

2. В государственных органах, органах местного самоуправления документирование информации осу-

ществляется в соответствии с правилами делопроизводства, установленными уполномоченным федеральным органом исполнительной власти в сфере архивного дела и делопроизводства.

(Часть 2 в ред. Федерального закона от 18.06.2017 № 127-ФЗ.)

3. Утратил силу. (Федеральный закон от 06.04.2011 № 65-ФЗ.)

4. В целях заключения гражданско-правовых договоров или оформления иных правоотношений, в которых участвуют лица, обменивающиеся электронными сообщениями, обмен электронными сообщениями, каждое из которых подписано электронной подписью или иным аналогом собственноручной подписи отправителя такого сообщения, в порядке, установленном федеральными законами, иными нормативными правовыми актами или соглашением сторон, рассматривается как обмен документами.

(В ред. Федерального закона от 06.04.2011 № 65-ФЗ.)

5. Право собственности и иные вещные права на материальные носители, содержащие документированную информацию, устанавливаются гражданским законодательством.

### **СТАТЬЯ 11.1.** ОБМЕН ИНФОРМАЦИЕЙ В ФОРМЕ ЭЛЕКТРОННЫХ ДОКУМЕНТОВ ПРИ ОСУЩЕСТВЛЕНИИ ПОЛНОМОЧИЙ ОРГАНОВ ГОСУДАРСТВЕННОЙ ВЛАСТИ И ОРГАНОВ МЕСТНОГО САМОУПРАВЛЕНИЯ

(введена Федеральным законом от 13.07.2015 № 263-ФЗ)

1. Органы государственной власти, органы местного самоуправления, а также организации, осуществляющие в соответствии с федеральными законами отдельные публичные полномочия, в пределах своих полномочий обязаны предоставлять по выбору граждан (физических лиц) и организаций информацию в форме электронных документов, подписанных усиленной квалифицированной электронной подписью, и (или) документов на бумажном носителе, за исключением случаев, если иной порядок предоставления такой информа-

ции установлен федеральными законами или иными нормативными правовыми актами Российской Федерации, регулирующими правоотношения в установленной сфере деятельности.

2. Информация, необходимая для осуществления полномочий органов государственной власти и органов местного самоуправления, организаций, осуществляющих в соответствии с федеральными законами отдельные публичные полномочия, может быть представлена гражданами (физическими лицами) и организациями в органы государственной власти, органы местного самоуправления, в организации, осуществляющие в соответствии с федеральными законами отдельные публичные полномочия, в форме электронных документов, подписанных электронной подписью, если иное не установлено федеральными законами, регулирующими правоотношения в установленной сфере деятельности.

3. Требования к осуществлению взаимодействия в электронной форме граждан (физических лиц) и организаций с органами государственной власти, органами местного самоуправления, с организациями, осуществляющими в соответствии с федеральными законами отдельные публичные полномочия, и порядок такого взаимодействия устанавливаются Правительством Российской Федерации в соответствии с Федеральным законом от 6 апреля 2011 года № 63-ФЗ «Об электронной подписи».

### **СТАТЬЯ 12.** ГОСУДАРСТВЕННОЕ РЕГУЛИРОВАНИЕ В СФЕРЕ ПРИМЕНЕНИЯ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ

1. Государственное регулирование в сфере применения информационных технологий предусматривает:

1) регулирование отношений, связанных с поиском, получением, передачей, производством и распространением информации с применением информационных технологий (информатизации), на основании принципов, установленных настоящим Федеральным законом;

2) развитие информационных систем различного назначения для обеспечения граждан (физических

лиц), организаций, государственных органов и органов местного самоуправления информацией, а также обеспечение взаимодействия таких систем;

3) создание условий для эффективного использования в Российской Федерации информационно-телекоммуникационных сетей, в том числе сети «Интернет» и иных подобных информационно-телекоммуникационных сетей;

4) обеспечение информационной безопасности детей.

(Пункт 4 введен Федеральным законом от 21.07.2011 № 252-ФЗ.)

2. Государственные органы, органы местного самоуправления в соответствии со своими полномочиями:

1) участвуют в разработке и реализации целевых программ применения информационных технологий;

2) создают информационные системы и обеспечивают доступ к содержащейся в них информации на русском языке и государственном языке соответствующей республики в составе Российской Федерации.

### **СТАТЬЯ 12.1.** ОСОБЕННОСТИ ГОСУДАРСТВЕННОГО РЕГУЛИРОВАНИЯ В СФЕРЕ ИСПОЛЬЗОВАНИЯ РОССИЙСКИХ ПРОГРАММ ДЛЯ ЭЛЕКТРОННЫХ ВЫЧИСЛИТЕЛЬНЫХ МАШИН И БАЗ ДАННЫХ

(введена Федеральным законом от 29.06.2015 № 188-ФЗ)

1. В целях расширения использования российских программ для электронных вычислительных машин и баз данных, подтверждения их происхождения из Российской Федерации, а также в целях оказания правообладателям программ для электронных вычислительных машин или баз данных мер государственной поддержки создается единый реестр российских программ для электронных вычислительных машин и баз данных (далее — реестр российского программного обеспечения).

2. Правила формирования и ведения реестра российского программного обеспечения, состав сведений, включаемых в реестр российского программного обеспечения, в том числе об основаниях возникновения исключительного права у правообладателя (правообладателей), условия включения таких сведений в реестр

российского программного обеспечения и исключения их из реестра российского программного обеспечения, порядок предоставления сведений, включаемых в реестр российского программного обеспечения, порядок принятия решения о включении таких сведений в реестр российского программного обеспечения устанавливаются Правительством Российской Федерации.

3. Уполномоченный Правительством Российской Федерации федеральный орган исполнительной власти в порядке и в соответствии с критериями, которые определяются Правительством Российской Федерации, может привлечь к формированию и ведению реестра российского программного обеспечения оператора реестра российского программного обеспечения — организацию, зарегистрированную на территории Российской Федерации.

4. Уполномоченный Правительством Российской Федерации федеральный орган исполнительной власти утверждает классификатор программ для электронных вычислительных машин и баз данных в целях ведения реестра российского программного обеспечения.

5. В реестр российского программного обеспечения включаются сведения о программах для электронных вычислительных машин и базах данных, которые соответствуют следующим требованиям:

1) исключительное право на программу для электронных вычислительных машин или базу данных на территории всего мира и на весь срок действия исключительного права принадлежит одному либо нескольким из следующих лиц (правообладателей):

а) Российской Федерации, субъекту Российской Федерации, муниципальному образованию;

б) российской некоммерческой организации, высший орган управления которой формируется прямо и (или) косвенно Российской Федерацией, субъектами Российской Федерации, муниципальными образованиями и (или) гражданами Российской Федерации и решения которой иностранное лицо не имеет возможности определять в силу особенностей отношений между таким иностранным лицом и российской некоммерческой организацией;

в) российской коммерческой организации, в которой суммарная доля прямого и (или) косвенного участия Российской Федерации, субъектов Российской Федерации, муниципальных образований, российских некоммерческих организаций, указанных в подпункте «б» настоящего пункта, граждан Российской Федерации составляет более пятидесяти процентов;

г) гражданину Российской Федерации;

2) программа для электронных вычислительных машин или база данных правомерно введена в гражданский оборот на территории Российской Федерации, экземпляры программы для электронных вычислительных машин или базы данных либо права использования программы для электронных вычислительных машин или базы данных свободно реализуются на всей территории Российской Федерации;

3) общая сумма выплат по лицензионным и иным договорам, предусматривающим предоставление прав на результаты интеллектуальной деятельности и средства индивидуализации, выполнение работ, оказание услуг в связи с разработкой, адаптацией и модификацией программы для электронных вычислительных машин или базы данных и для разработки, адаптации и модификации программы для электронных вычислительных машин или базы данных, в пользу иностранных юридических лиц и (или) физических лиц, контролируемых ими российских коммерческих организаций и (или) российских некоммерческих организаций, агентов, представителей иностранных лиц и контролируемых ими российских коммерческих организаций и (или) российских некоммерческих организаций составляет менее тридцати процентов от выручки правообладателя (правообладателей) программы для электронных вычислительных машин или базы данных от реализации программы для электронных вычислительных машин или базы данных, включая предоставление прав использования, независимо от вида договора за календарный год;

4) сведения о программе для электронных вычислительных машин или базе данных не составляют государственную тайну, и программа для электронных вы-

числительных машин или база данных не содержит сведений, составляющих государственную тайну.

6. Правительством Российской Федерации могут быть установлены дополнительные требования к программам для электронных вычислительных машин и базам данных, сведения о которых включены в реестр российского программного обеспечения.

7. Программы для электронных вычислительных машин и базы данных, сведения о которых включены в реестр российского программного обеспечения, признаются происходящими из Российской Федерации.

8. Для целей настоящей статьи доля участия одной организации в другой организации или гражданина Российской Федерации в организации определяется в соответствии с порядком, установленным главой 14.1 Налогового кодекса Российской Федерации.

9. Для целей настоящей статьи контролируемой иностранным лицом российской коммерческой организацией или российской некоммерческой организацией признается организация, решения которой иностранное лицо имеет возможность определять в силу преобладающего прямого и (или) косвенного участия в этой организации, участия в договоре (соглашении), предметом которого является управление этой организацией, или иных особенностей отношений между иностранным лицом и этой организацией и (или) иными лицами.

10. Решение об отказе во включении в реестр российского программного обеспечения программ для электронных вычислительных машин или баз данных может быть обжаловано правообладателем программы для электронных вычислительных машин или базы данных в суд в течение трех месяцев со дня получения такого решения.

### **СТАТЬЯ 13.** ИНФОРМАЦИОННЫЕ СИСТЕМЫ

1. Информационные системы включают в себя:

1) государственные информационные системы — федеральные информационные системы и региональные информационные системы, созданные на основании соответственно федеральных законов, законов

субъектов Российской Федерации, на основании правовых актов государственных органов;

2) муниципальные информационные системы, созданные на основании решения органа местного самоуправления;

3) иные информационные системы.

2. Если иное не установлено федеральными законами, оператором информационной системы является собственник используемых для обработки содержащейся в базах данных информации технических средств, который правомерно пользуется такими базами данных, или лицо, с которым этот собственник заключил договор об эксплуатации информационной системы. В случаях и в порядке, установленных федеральными законами, оператор информационной системы должен обеспечить возможность размещения информации в сети «Интернет» в форме открытых данных.

(В ред. Федерального закона от 07.06.2013 № 112-ФЗ.)

2.1. Технические средства информационных систем, используемых государственными органами, органами местного самоуправления, государственными и муниципальными унитарными предприятиями или государственными и муниципальными учреждениями, должны размещаться на территории Российской Федерации.

(Часть 2.1 введена Федеральным законом от 31.12.2014 № 531-ФЗ.)

2.2. В случае создания или модернизации информационной системы на основании концессионного соглашения или соглашения о государственно-частном партнерстве функции оператора информационной системы в пределах, в объемах и в сроки, которые предусмотрены соответствующим соглашением, осуществляются концессионером или частным партнером соответственно.

(Часть 2.2 введена Федеральным законом от 29.06.2018 № 173-ФЗ.)

3. Права обладателя информации, содержащейся в базах данных информационной системы, подлежат охране независимо от авторских и иных прав на такие базы данных.

4. Установленные настоящим Федеральным законом требования к государственным информационным системам распространяются на муниципальные информационные системы, если иное не предусмотрено законодательством Российской Федерации о местном самоуправлении.

5. Особенности эксплуатации государственных информационных систем и муниципальных информационных систем могут устанавливаться в соответствии с техническими регламентами, нормативными правовыми актами государственных органов, нормативными правовыми актами органов местного самоуправления, принимающих решения о создании таких информационных систем.

6. Порядок создания и эксплуатации информационных систем, не являющихся государственными информационными системами или муниципальными информационными системами, определяется операторами таких информационных систем в соответствии с требованиями, установленными настоящим Федеральным законом или другими федеральными законами.

7. Порядок осуществления контроля за соблюдением требований, предусмотренных частью 2.1 настоящей статьи и частью 6 статьи 14 настоящего Федерального закона, устанавливается Правительством Российской Федерации.

(Часть 7 введена Федеральным законом от 31.12.2014 № 531-ФЗ.)

### **СТАТЬЯ 14.** ГОСУДАРСТВЕННЫЕ ИНФОРМАЦИОННЫЕ СИСТЕМЫ

1. Государственные информационные системы создаются в целях реализации полномочий государственных органов и обеспечения обмена информацией между этими органами, а также в иных установленных федеральными законами целях.

2. Государственные информационные системы создаются, модернизируются и эксплуатируются с учетом требований, предусмотренных законодательством Российской Федерации о контрактной системе в сфере закупок товаров, работ, услуг для обеспечения государственных и муниципальных нужд либо законодательством

Российской Федерации о государственно-частном партнерстве, о муниципально-частном партнерстве, законодательством о концессионных соглашениях, а в случаях, если эксплуатация государственных информационных систем осуществляется без привлечения средств бюджетов бюджетной системы Российской Федерации, в соответствии с иными федеральными законами.

(В ред. федеральных законов от 28.12.2013 № 396-ФЗ, от 29.06.2018 № 173-ФЗ, от 19.07.2018 № 211-ФЗ.)

3. Государственные информационные системы создаются и эксплуатируются на основе статистической и иной документированной информации, предоставляемой гражданами (физическими лицами), организациями, государственными органами, органами местного самоуправления.

4. Перечни видов информации, предоставляемой в обязательном порядке, устанавливаются федеральными законами, условия ее предоставления — Правительством Российской Федерации или соответствующими государственными органами, если иное не предусмотрено федеральными законами. В случае, если при создании или эксплуатации государственных информационных систем предполагается осуществление или осуществляется обработка общедоступной информации, предусмотренной перечнями, утверждаемыми в соответствии со статьей 14 Федерального закона от 9 февраля 2009 года № 8-ФЗ «Об обеспечении доступа к информации о деятельности государственных органов и органов местного самоуправления», государственные информационные системы должны обеспечивать размещение такой информации в сети «Интернет» в форме открытых данных.

(В ред. Федерального закона от 07.06.2013 № 112-ФЗ.)

4.1. Правительство Российской Федерации определяет случаи, при которых доступ с использованием сети «Интернет» к информации, содержащейся в государственных информационных системах, предоставляется исключительно пользователям информации, прошедшим авторизацию в единой системе идентификации

и аутентификации, а также порядок использования единой системы идентификации и аутентификации.

(Часть 4.1 введена Федеральным законом от 07.06.2013 № 112-ФЗ.)

5. Если иное не установлено решением о создании государственной информационной системы, функции ее оператора осуществляются заказчиком, заключившим государственный контракт на создание такой информационной системы. При этом ввод государственной информационной системы в эксплуатацию осуществляется в порядке, установленном указанным заказчиком.

5.1. В случае создания или модернизации государственной информационной системы на основании концессионного соглашения или соглашения о государственно-частном партнерстве функции оператора данной системы в пределах, в объемах и в сроки, которые предусмотрены соответствующим соглашением, осуществляются концессионером или частным партнером.

(Часть 5.1 введена Федеральным законом от 29.06.2018 № 173-ФЗ.)

6. Правительство Российской Федерации утверждает требования к порядку создания, развития, ввода в эксплуатацию, эксплуатации и вывода из эксплуатации государственных информационных систем, дальнейшего хранения содержащейся в их базах данных информации, включающие в себя перечень, содержание и сроки реализации этапов мероприятий по созданию, развитию, вводу в эксплуатацию, эксплуатации и выводу из эксплуатации государственных информационных систем, дальнейшему хранению содержащейся в их базах данных информации.

(Часть 6 в ред. Федерального закона от 31.12.2014 № 531-ФЗ.)

7. Не допускается эксплуатация государственной информационной системы без надлежащего оформления прав на использование ее компонентов, являющихся объектами интеллектуальной собственности.

8. Технические средства, предназначенные для обработки информации, содержащейся в государственных информационных системах, в том числе программно-технические средства и средства защиты инфор-

мации, должны соответствовать требованиям законодательства Российской Федерации о техническом регулировании.

9. Информация, содержащаяся в государственных информационных системах, а также иные имеющиеся в распоряжении государственных органов сведения и документы являются государственными информационными ресурсами. Информация, содержащаяся в государственных информационных системах, является официальной. Государственные органы, определенные в соответствии с нормативным правовым актом, регламентирующим функционирование государственной информационной системы, обязаны обеспечить достоверность и актуальность информации, содержащейся в данной информационной системе, доступ к указанной информации в случаях и в порядке, предусмотренных законодательством, а также защиту указанной информации от неправомерных доступа, уничтожения, модифицирования, блокирования, копирования, предоставления, распространения и иных неправомерных действий.

(В ред. Федерального закона от 27.07.2010 № 227-ФЗ.)

### **СТАТЬЯ 14.1.** ПРИМЕНЕНИЕ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ В ЦЕЛЯХ ИДЕНТИФИКАЦИИ ГРАЖДАН РОССИЙСКОЙ ФЕДЕРАЦИИ

(введена Федеральным законом от 31.12.2017 № 482-ФЗ)

1. Государственные органы, банки и иные организации в случаях, определенных федеральными законами, после проведения идентификации при личном присутствии гражданина Российской Федерации с его согласия на безвозмездной основе размещают в электронной форме:

1) сведения, необходимые для регистрации гражданина Российской Федерации в единой системе идентификации и аутентификации, и иные сведения, если такие сведения предусмотрены федеральными законами, — в единой системе идентификации и аутентификации;

2) биометрические персональные данные гражданина Российской Федерации — в единой информационной системе персональных данных, обеспечивающей обработку, включая сбор и хранение биометрических персональных данных, их проверку и передачу информации о степени их соответствия предоставленным биометрическим персональным данным гражданина Российской Федерации (далее — единая биометрическая система).

2. Правительство Российской Федерации по согласованию с Центральным банком Российской Федерации устанавливает требования:

1) к фиксированию действий при размещении сведений, указанных в пунктах 1 и 2 части 1 настоящей статьи;

2) к проведению государственными органами и организациями, указанными в части 1 настоящей статьи, идентификации гражданина Российской Федерации, за исключением организаций, проводящих такую идентификацию в порядке, установленном Федеральным законом от 7 августа 2001 года № 115-ФЗ «О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма».

3. Федеральные законы, устанавливающие обязанность государственных органов и организаций по размещению сведений, указанных в пунктах 1 и 2 части 1 настоящей статьи, должны предусматривать осуществление контроля и надзора за соответствующими действиями, а также определение органа государственной власти или организации, уполномоченных на их осуществление.

4. Сведения, указанные в пунктах 1 и 2 части 1 настоящей статьи, размещаются соответственно в единой системе идентификации и аутентификации и в единой биометрической системе уполномоченным сотрудником государственного органа или организации и подписываются усиленной квалифицированной электронной подписью такого государственного органа или организации.

5. Форма согласия на обработку персональных данных и биометрических персональных данных, указанных в пунктах 1 и 2 части 1 настоящей статьи, утверждается Правительством Российской Федерации.

6. Порядок регистрации гражданина Российской Федерации в единой системе идентификации и аутентификации, включая состав сведений, необходимых для регистрации гражданина Российской Федерации в указанной системе, порядок и сроки проверки и обновления сведений, размещаемых в единой системе идентификации и аутентификации с использованием государственных информационных систем, устанавливаются Правительством Российской Федерации. Федеральные органы исполнительной власти, в том числе федеральный орган исполнительной власти, осуществляющий функции по выработке и реализации государственной политики и нормативно-правовому регулированию в сфере внутренних дел, органы государственных внебюджетных фондов направляют в единую систему идентификации и аутентификации сведения о гражданах Российской Федерации в целях их обновления в соответствии с указанным порядком.

7. В случаях, установленных федеральными законами, государственные органы и организации вправе обновлять информацию о гражданах Российской Федерации, идентифицированных в соответствии с частью 18 настоящей статьи, с использованием сведений, полученных из единой системы идентификации и аутентификации.

8. Состав сведений, размещаемых в единой биометрической системе, включая вид биометрических персональных данных, определяется Правительством Российской Федерации.

9. Обработка биометрических персональных данных в государственных органах, банках и иных организациях, указанных в абзаце первом части 1 настоящей статьи, в том числе с использованием единой биометрической системы, осуществляется в соответствии с требованиями к защите биометрических персональных данных, установленными в соответствии со статьей 19 Федерального закона от 27 июля 2006 года № 152-ФЗ «О персональных данных».

10. Контроль и надзор за выполнением организационных и технических мер по обеспечению безопасности персональных данных, установленных в соответствии

со статьей 19 Федерального закона от 27 июля 2006 года № 152-ФЗ «О персональных данных», при обработке персональных данных в единой биометрической системе, за исключением контроля и надзора за выполнением банками организационных и технических мер по обеспечению безопасности персональных данных при использовании единой биометрической системы, осуществляются федеральным органом исполнительной власти, уполномоченным в области обеспечения безопасности, и федеральным органом исполнительной власти, уполномоченным в области противодействия техническим разведкам и технической защиты информации, в пределах их полномочий, установленных законодательством Российской Федерации о персональных данных.

11. Контроль и надзор за выполнением банками организационных и технических мер по обеспечению безопасности персональных данных при использовании единой биометрической системы осуществляются Центральным банком Российской Федерации.

12. Правительство Российской Федерации определяет федеральный орган исполнительной власти, осуществляющий регулирование в сфере идентификации граждан Российской Федерации на основе биометрических персональных данных.

13. Федеральный орган исполнительной власти, осуществляющий регулирование в сфере идентификации граждан Российской Федерации на основе биометрических персональных данных:

1) определяет порядок обработки, включая сбор и хранение, параметров биометрических персональных данных в целях идентификации, порядок размещения и обновления биометрических персональных данных в единой биометрической системе, а также требования к информационным технологиям и техническим средствам, предназначенным для обработки биометрических персональных данных в целях проведения идентификации (в банковской сфере и иных сферах финансового рынка указанные требования устанавливаются по согласованию с Центральным банком Российской Федерации);

2) определяет формы подтверждения соответствия информационных технологий и технических средств, предназначенных для обработки биометрических персональных данных в целях проведения идентификации, требованиям, определенным в соответствии с пунктом 1 настоящей части, и публикует перечень технологий и средств, имеющих подтверждение соответствия (в банковской сфере и иных сферах финансового рынка формы подтверждения соответствия устанавливаются по согласованию с Центральным банком Российской Федерации);

3) разрабатывает и утверждает методики проверки соответствия предоставленных биометрических персональных данных физического лица его биометрическим персональным данным, содержащимся в единой биометрической системе, а также определяет степень взаимного соответствия указанных биометрических персональных данных, достаточную для проведения идентификации, предусмотренной настоящим Федеральным законом.

14. Центральный банк Российской Федерации совместно с оператором единой биометрической системы определяет перечень угроз безопасности, актуальных при обработке, включая сбор и хранение, биометрических персональных данных, их проверке и передаче информации о степени их соответствия предоставленным биометрическим персональным данным гражданина Российской Федерации в государственных органах, банках и иных организациях, указанных в абзаце первом части 1 настоящей статьи, в единой биометрической системе с учетом оценки возможного вреда, проведенной в соответствии с законодательством Российской Федерации о персональных данных, и согласовывает указанный перечень с федеральным органом исполнительной власти, уполномоченным в области обеспечения безопасности, и федеральным органом исполнительной власти, уполномоченным в области противодействия техническим разведкам и технической защиты информации.

15. Государственные органы, банки и иные организации, указанные в абзаце первом части 1 настоящей

статьи, оператор единой биометрической системы при обработке, включая сбор и хранение, биометрических персональных данных, их проверке и определении степени их соответствия предоставленным биометрическим персональным данным гражданина Российской Федерации:

1) осуществляют свои функции в соответствии с законодательством Российской Федерации о персональных данных и требованиями настоящего Федерального закона;

2) осуществляют обработку, включая сбор и хранение, биометрических персональных данных с применением информационных технологий и технических средств, имеющих подтверждение соответствия требованиям, установленным в соответствии с настоящим Федеральным законом;

3) обеспечивают проверку соответствия предоставленных биометрических персональных данных гражданина Российской Федерации его биометрическим персональным данным согласно методикам, утвержденным в соответствии с настоящим Федеральным законом.

16. Оператор единой биометрической системы:

1) осуществляет передачу информации о результатах проверки соответствия предоставленных биометрических персональных данных гражданина Российской Федерации его биометрическим персональным данным, содержащимся в единой биометрической системе, в государственные органы, банки и иные организации, указанные в абзаце первом части 1 настоящей статьи;

2) предоставляет в федеральный орган исполнительной власти, осуществляющий функции по выработке и реализации государственной политики и нормативно-правовому регулированию в сфере внутренних дел, и федеральный орган исполнительной власти в области обеспечения безопасности в целях обеспечения обороны страны, безопасности государства, охраны правопорядка и противодействия терроризму сведения, содержащиеся в единой биометрической системе, в порядке, установленном Правительством Российской Федерации.

17. Функции оператора единой биометрической системы возлагаются Правительством Российской Федерации на оператора, занимающего существенное положение в сети связи общего пользования на территориях не менее чем двух третей субъектов Российской Федерации.

18. Идентификация гражданина Российской Федерации с применением информационных технологий осуществляется без его личного присутствия в случаях, установленных федеральными законами, путем предоставления государственным органам и организациям:

1) сведений о гражданине Российской Федерации, размещенных в единой системе идентификации и аутентификации, в порядке, установленном Правительством Российской Федерации;

2) информации о степени соответствия предоставленных биометрических персональных данных гражданина Российской Федерации его биометрическим персональным данным, содержащимся в единой биометрической системе.

19. При предоставлении биометрических персональных данных физического лица по каналам связи в целях проведения его идентификации без личного присутствия посредством сети «Интернет» должны применяться шифровальные (криптографические) средства, позволяющие обеспечить безопасность передаваемых данных от угроз безопасности, актуальных при обработке биометрических персональных данных, определенных в соответствии с частью 14 настоящей статьи, и имеющие подтверждение соответствия требованиям, установленным в соответствии со статьей 19 Федерального закона от 27 июля 2006 года № 152-ФЗ «О персональных данных». Государственный орган, банк или иная организация, указанные в абзаце первом части 1 настоящей статьи, обязаны предложить использовать указанные средства физическим лицам, обратившимся к ним в целях проведения идентификации без личного присутствия, и указать страницу сайта в сети «Интернет», с которой предоставляются эти средства.

20. В случае, если физическое лицо для предоставления своих биометрических персональных данных в

целях проведения идентификации без личного присутствия посредством сети «Интернет» использует мобильный телефон, смартфон или планшетный компьютер и отказывается от использования шифровальных (криптографических) средств, указанных в части 19 настоящей статьи, государственный орган, банк или иная организация, указанные в абзаце первом части 1 настоящей статьи, обязаны отказать такому лицу в проведении указанной идентификации.

21. В случае, если физическое лицо при предоставлении своих биометрических персональных данных в целях проведения идентификации без личного присутствия посредством сети «Интернет» использует иные устройства, в том числе персональный компьютер, и отказывается от применения шифровальных (криптографических) средств, указанных в части 19 настоящей статьи, государственный орган, банк или иная организация, указанные в абзаце первом части 1 настоящей статьи, уведомляет его о рисках, связанных с таким отказом. После подтверждения физическим лицом своего решения государственный орган, банк или иная организация, указанные в абзаце первом части 1 настоящей статьи, может провести соответствующую идентификацию физического лица посредством сети «Интернет» без использования им указанных шифровальных (криптографических) средств.

22. Государственные органы, банки и иные организации при проведении идентификации гражданина Российской Федерации с применением информационных технологий в соответствии с частью 18 настоящей статьи вправе подтверждать достоверность сведений, предусмотренных пунктом 1 части 18 настоящей статьи, с использованием информационных систем государственных органов, в том числе федерального органа исполнительной власти, осуществляющего функции по выработке и реализации государственной политики и нормативно-правовому регулированию в сфере внутренних дел, Пенсионного фонда Российской Федерации, Федерального фонда обязательного медицинского страхования и (или) государственной информационной системы, определенной Правительством Российской Федерации.

23. Согласие гражданина Российской Федерации на обработку персональных данных, содержащихся в единой системе идентификации и аутентификации, и биометрических персональных данных для проведения его идентификации с применением информационных технологий в соответствии с частью 18 настоящей статьи может быть подписано его простой электронной подписью, ключ к которой получен в соответствии с правилами использования простой электронной подписи при обращении за получением государственных и муниципальных услуг в электронной форме, установленными Правительством Российской Федерации. Указанное согласие, подписанное простой электронной подписью, признается электронным документом, равнозначным документу на бумажном носителе, подписанному собственноручной подписью данного гражданина Российской Федерации.

24. Размер и порядок взимания оператором единой биометрической системы платы за предоставление государственным органам и организациям сведений, указанных в пункте 2 части 18 настоящей статьи, определяются федеральным органом исполнительной власти, осуществляющим функции по выработке и реализации государственной политики и нормативно-правовому регулированию в сфере информационных технологий, по согласованию с оператором единой биометрической системы и иными государственными органами и организациями в случаях, установленных федеральными законами.

### **СТАТЬЯ 15.** ИСПОЛЬЗОВАНИЕ ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННЫХ СЕТЕЙ

1. На территории Российской Федерации использование информационно-телекоммуникационных сетей осуществляется с соблюдением требований законодательства Российской Федерации в области связи, настоящего Федерального закона и иных нормативных правовых актов Российской Федерации.

2. Регулирование использования информационно-телекоммуникационных сетей, доступ к которым не ограничен определенным кругом лиц, осуществляется

в Российской Федерации с учетом общепринятой международной практики деятельности саморегулируемых организаций в этой области. Порядок использования иных информационно-телекоммуникационных сетей определяется владельцами таких сетей с учетом требований, установленных настоящим Федеральным законом.

3. Использование на территории Российской Федерации информационно-телекоммуникационных сетей в хозяйственной или иной деятельности не может служить основанием для установления дополнительных требований или ограничений, касающихся регулирования указанной деятельности, осуществляемой без использования таких сетей, а также для несоблюдения требований, установленных федеральными законами.

4. Федеральными законами может быть предусмотрена обязательная идентификация личности, организаций, использующих информационно-телекоммуникационную сеть при осуществлении предпринимательской деятельности. При этом получатель электронного сообщения, находящийся на территории Российской Федерации, вправе провести проверку, позволяющую установить отправителя электронного сообщения, а в установленных федеральными законами или соглашением сторон случаях обязан провести такую проверку.

5. Передача информации посредством использования информационно-телекоммуникационных сетей осуществляется без ограничений при условии соблюдения установленных федеральными законами требований к распространению информации и охране объектов интеллектуальной собственности. Передача информации может быть ограничена только в порядке и на условиях, которые установлены федеральными законами.

6. Особенности подключения государственных информационных систем к информационно-телекоммуникационным сетям могут быть установлены нормативным правовым актом Президента Российской Федерации или нормативным правовым актом Правительства Российской Федерации.

**СТАТЬЯ 15.1.** 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

(введена Федеральным законом от 28.07.2012 № 139-ФЗ)

1. В целях ограничения доступа к сайтам в сети «Интернет», содержащим информацию, распространение которой в Российской Федерации запрещено, создается 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» (далее — реестр).

2. В реестр включаются:

1) доменные имена и (или) указатели страниц сайтов в сети «Интернет», содержащих информацию, распространение которой в Российской Федерации запрещено;

2) сетевые адреса, позволяющие идентифицировать сайты в сети «Интернет», содержащие информацию, распространение которой в Российской Федерации запрещено.

3. Создание, формирование и ведение реестра осуществляются федеральным органом исполнительной власти, осуществляющим функции по контролю и надзору в сфере средств массовой информации, массовых коммуникаций, информационных технологий и связи, в порядке, установленном Правительством Российской Федерации.

4. Федеральный орган исполнительной власти, осуществляющий функции по контролю и надзору в сфере средств массовой информации, массовых коммуникаций, информационных технологий и связи, в порядке и в соответствии с критериями, которые определяются Правительством Российской Федерации, может при-

влечь к формированию и ведению реестра оператора реестра — организацию, зарегистрированную на территории Российской Федерации.

5. Основаниями для включения в реестр сведений, указанных в части 2 настоящей статьи, являются:

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 (подпункт «б» в ред. Федерального закона от 19.12.2016 № 442-ФЗ);

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 (подпункт «г» введен Федеральным законом от 05.04.2013 № 50-ФЗ);

д) информации, нарушающей требования Федерального закона от 29 декабря 2006 года № 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 № 138-ФЗ «О лотереях» о запрете деятельности по организации и проведению азартных игр и лотерей с использованием сети «Интернет» и иных средств связи (подпункт «д» введен Федеральным законом от 21.07.2014 № 222-ФЗ);

е) информации, содержащей предложения о розничной продаже дистанционным способом алкогольной продукции, и (или) спиртосодержащей пищевой продукции, и (или) этилового спирта, и (или) спиртосодержащей непищевой продукции, розничная продажа которой ограничена или запрещена законодательством о государственном регулировании производства и оборота этилового спирта, алкогольной и спиртосодержащей продукции и об ограничении потребления (распития) алкогольной продукции (подпункт «е» введен Федеральным законом от 29.07.2017 № 278-ФЗ);

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

3) постановление судебного пристава-исполнителя об ограничении доступа к информации, распространяемой в сети «Интернет», порочащей честь, достоинство или деловую репутацию гражданина либо деловую репутацию юридического лица.

(Пункт 3 введен Федеральным законом от 23.04.2018 № 102-ФЗ.)

6. Решение о включении в 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, может быть обжаловано владельцем сайта в сети «Интернет», провайдером хостинга, оператором связи, оказывающим услуги по предоставлению доступа к информационно-телекоммуникационной сети «Интернет», в суд в течение трех месяцев со дня принятия такого решения.

7. В течение суток с момента получения от оператора реестра уведомления о включении доменного имени и (или) указателя страницы сайта в сети «Интернет» в реестр провайдер хостинга обязан проинформировать об этом обслуживаемого им владельца сайта в сети «Интернет» и уведомить его о необходимости незамедли-

тельного удаления интернет-страницы, содержащей информацию, распространение которой в Российской Федерации запрещено.

8. В течение суток с момента получения от провайдера хостинга уведомления о включении доменного имени и (или) указателя страницы сайта в сети «Интернет» в реестр владелец сайта в сети «Интернет» обязан удалить интернет-страницу, содержащую информацию, распространение которой в Российской Федерации запрещено. В случае отказа или бездействия владельца сайта в сети «Интернет» провайдер хостинга обязан ограничить доступ к такому сайту в сети «Интернет» в течение суток.

9. В случае непринятия провайдером хостинга и (или) владельцем сайта в сети «Интернет» мер, указанных в частях 7 и 8 настоящей статьи, сетевой адрес, позволяющий идентифицировать сайт в сети «Интернет», содержащий информацию, распространение которой в Российской Федерации запрещено, включается в реестр.

10. В течение суток с момента включения в реестр сетевого адреса, позволяющего идентифицировать сайт в сети «Интернет», содержащий информацию, распространение которой в Российской Федерации запрещено, оператор связи, оказывающий услуги по предоставлению доступа к информационно-телекоммуникационной сети «Интернет», обязан ограничить доступ к такому сайту в сети «Интернет».

11. Федеральный орган исполнительной власти, осуществляющий функции по контролю и надзору в сфере средств массовой информации, массовых коммуникаций, информационных технологий и связи, или привлеченный им в соответствии с частью 4 настоящей статьи оператор реестра исключает из реестра доменное имя, указатель страницы сайта в сети «Интернет» или сетевой адрес, позволяющий идентифицировать сайт в сети «Интернет», на основании обращения владельца сайта в сети «Интернет», провайдера хостинга или оператора связи, оказывающего услуги по предоставлению доступа к информационно-телекоммуникационной се-

ти «Интернет», не позднее чем в течение трех дней со дня такого обращения после принятия мер по удалению информации, распространение которой в Российской Федерации запрещено, либо на основании вступившего в законную силу решения суда об отмене решения федерального органа исполнительной власти, осуществляющего функции по контролю и надзору в сфере средств массовой информации, массовых коммуникаций, информационных технологий и связи, о включении в реестр доменного имени, указателя страницы сайта в сети «Интернет» или сетевого адреса, позволяющего идентифицировать сайт в сети «Интернет».

12. Порядок взаимодействия оператора реестра с провайдером хостинга и порядок получения доступа к содержащейся в реестре информации оператором связи, оказывающим услуги по предоставлению доступа к информационно-телекоммуникационной сети «Интернет», устанавливаются уполномоченным Правительством Российской Федерации федеральным органом исполнительной власти.

13. Порядок ограничения доступа к сайтам в сети «Интернет», предусмотренный настоящей статьей, не применяется к информации, порядок ограничения доступа к которой предусмотрен статьей 15.3 настоящего Федерального закона.

(Часть 13 введена Федеральным законом от 28.12.2013 № 398-ФЗ.)

14. Федеральный орган исполнительной власти, осуществляющий функции по контролю и надзору в сфере средств массовой информации, массовых коммуникаций, информационных технологий и связи, или привлеченный им в соответствии с частью 4 настоящей статьи оператор реестра в течение суток с момента получения решений, указанных в подпунктах «а» и «в» пункта 1 части 5 настоящей статьи, уведомляет по системе взаимодействия об этом федеральный орган исполнительной власти в сфере внутренних дел.

(Часть 14 введена Федеральным законом от 07.06.2017 № 109-ФЗ.)

**СТАТЬЯ 15.2.** ПОРЯДОК ОГРАНИЧЕНИЯ ДОСТУПА К ИНФОРМАЦИИ, РАСПРОСТРАНЯЕМОЙ С НАРУШЕНИЕМ АВТОРСКИХ И (ИЛИ) СМЕЖНЫХ ПРАВ

(в ред. Федерального закона от 24.11.2014 № 364-ФЗ)

(введена Федеральным законом от 02.07.2013 № 187-ФЗ)

1. Правообладатель в случае обнаружения в информационно-телекоммуникационных сетях, в том числе в сети «Интернет», объектов авторских и (или) смежных прав (кроме фотографических произведений и произведений, полученных способами, аналогичными фотографии), распространяемых в таких сетях, или информации, необходимой для их получения с использованием информационно-телекоммуникационных сетей, которые распространяются без его разрешения или иного законного основания, вправе обратиться в федеральный орган исполнительной власти, осуществляющий функции по контролю и надзору в сфере средств массовой информации, массовых коммуникаций, информационных технологий и связи, с заявлением о принятии мер по ограничению доступа к информационным ресурсам, распространяющим такие объекты или информацию, на основании вступившего в силу судебного акта. Форма указанного заявления утверждается федеральным органом исполнительной власти, осуществляющим функции по контролю и надзору в сфере средств массовой информации, массовых коммуникаций, информационных технологий и связи.

(В ред. Федерального закона от 24.11.2014 № 364-ФЗ.)

2. Федеральный орган исполнительной власти, осуществляющий функции по контролю и надзору в сфере средств массовой информации, массовых коммуникаций, информационных технологий и связи, на основании вступившего в силу судебного акта в течение трех рабочих дней:

1) определяет провайдера хостинга или иное лицо, обеспечивающее размещение в информационно-телекоммуникационной сети, в том числе в сети «Интернет», указанного информационного ресурса, обслужи-

вающего владельца сайта в сети «Интернет», на котором размещена информация, содержащая объекты авторских и (или) смежных прав (кроме фотографических произведений и произведений, полученных способами, аналогичными фотографии), или информация, необходимая для их получения с использованием информационно-телекоммуникационных сетей, без разрешения правообладателя или иного законного основания (в ред. Федерального закона от 24.11.2014 № 364-ФЗ);

2) направляет провайдеру хостинга или иному указанному в пункте 1 настоящей части лицу в электронном виде уведомление на русском и английском языках о нарушении исключительных прав на объекты авторских и (или) смежных прав (кроме фотографических произведений и произведений, полученных способами, аналогичными фотографии), распространяемые в информационно-телекоммуникационных сетях, в том числе в сети «Интернет», с указанием наименования произведения, его автора, правообладателя, доменного имени и сетевого адреса, позволяющих идентифицировать сайт в сети «Интернет», на котором размещена информация, содержащая объекты авторских и (или) смежных прав (кроме фотографических произведений и произведений, полученных способами, аналогичными фотографии), или информация, необходимая для их получения с использованием информационно-телекоммуникационных сетей, без разрешения правообладателя или иного законного основания, а также указателей страниц сайта в сети «Интернет», позволяющих идентифицировать такую информацию, и с требованием принять меры по ограничению доступа к такой информации (в ред. Федерального закона от 24.11.2014 № 364-ФЗ);

3) фиксирует дату и время направления уведомления провайдеру хостинга или иному указанному в пункте 1 настоящей части лицу в соответствующей информационной системе.

3. В течение одного рабочего дня с момента получения уведомления, указанного в пункте 2 части 2 настоящей статьи, провайдер хостинга или иное указанное в пункте 1 части 2 настоящей статьи лицо обязаны проинформировать об этом обслуживаемого ими владельца

информационного ресурса и уведомить его о необходимости незамедлительно ограничить доступ к незаконно размещенной информации.

(В ред. Федерального закона от 24.11.2014 № 364-ФЗ.)

4. В течение одного рабочего дня с момента получения от провайдера хостинга или иного указанного в пункте 1 части 2 настоящей статьи лица уведомления о необходимости ограничить доступ к незаконно размещенной информации владелец информационного ресурса обязан удалить незаконно размещенную информацию или принять меры по ограничению доступа к ней. В случае отказа или бездействия владельца информационного ресурса провайдер хостинга или иное указанное в пункте 1 части 2 настоящей статьи лицо обязаны ограничить доступ к соответствующему информационному ресурсу не позднее истечения трех рабочих дней с момента получения уведомления, указанного в пункте 2 части 2 настоящей статьи.

(Часть 4 в ред. Федерального закона от 24.11.2014 № 364-ФЗ.)

5. В случае непринятия провайдером хостинга или иным указанным в пункте 1 части 2 настоящей статьи лицом и (или) владельцем информационного ресурса мер, указанных в частях 3 и 4 настоящей статьи, доменное имя сайта в сети «Интернет», его сетевой адрес, указатели страниц сайта в сети «Интернет», позволяющие идентифицировать информацию, содержащую объекты авторских и (или) смежных прав (кроме фотографических произведений и произведений, полученных способами, аналогичными фотографии), или информацию, необходимую для их получения с использованием информационно-телекоммуникационных сетей, и размещенную без разрешения правообладателя или иного законного основания, а также иные сведения об этом сайте и информация направляются по системе взаимодействия операторам связи для принятия мер по ограничению доступа к данному информационному ресурсу, в том числе к сайту в сети «Интернет», или к размещенной на нем информации.

(В ред. Федерального закона от 24.11.2014 № 364-ФЗ.)

6. Федеральный орган исполнительной власти, осуществляющий функции по контролю и надзору в сфере средств массовой информации, массовых коммуникаций, информационных технологий и связи, на основании вступившего в силу судебного акта в течение трех рабочих дней со дня получения судебного акта об отмене ограничения доступа к информационному ресурсу, содержащему объекты авторских и (или) смежных прав (кроме фотографических произведений и произведений, полученных способами, аналогичными фотографии), распространяемые в информационно-телекоммуникационных сетях, в том числе в сети «Интернет», или информацию, необходимую для их получения с использованием информационно-телекоммуникационных сетей, которые распространяются без разрешения правообладателя или иного законного основания, уведомляет провайдера хостинга или иное указанное в пункте 1 части 2 настоящей статьи лицо и операторов связи об отмене мер по ограничению доступа к данному информационному ресурсу. В течение одного рабочего дня со дня получения от указанного федерального органа исполнительной власти уведомления об отмене мер по ограничению доступа к информационному ресурсу провайдер хостинга обязан проинформировать об этом владельца информационного ресурса и уведомить о возможности снятия ограничения доступа.

(В ред. Федерального закона от 24.11.2014 № 364-ФЗ.)

7. В течение суток с момента получения по системе взаимодействия сведений об информационном ресурсе, содержащем объекты авторских и (или) смежных прав (кроме фотографических произведений и произведений, полученных способами, аналогичными фотографии), распространяемые в информационно-телекоммуникационных сетях, в том числе в сети «Интернет», или информацию, необходимую для их получения с использованием информационно-телекоммуникационных сетей, которые используются без разрешения правообладателя или иного законного основания, оператор связи, оказывающий услуги по предоставлению доступа к информационно-телекоммуникационной сети «Ин-

тернет», обязан ограничить доступ к незаконно размещенной информации в соответствии с вступившим в законную силу судебным актом. В случае отсутствия у оператора связи технической возможности ограничить доступ к незаконно размещенной информации оператор связи обязан ограничить доступ к такому информационному ресурсу.

(Часть 7 в ред. Федерального закона от 24.11.2014 № 364-ФЗ.)

8. Порядок функционирования информационной системы взаимодействия устанавливается федеральным органом исполнительной власти, осуществляющим функции по контролю и надзору в сфере средств массовой информации, массовых коммуникаций, информационных технологий и связи.

9. Предусмотренный настоящей статьей порядок не применяется к информации, подлежащей включению в реестр в соответствии со статьей 15.1 настоящего Федерального закона.

### **СТАТЬЯ 15.3.** ПОРЯДОК ОГРАНИЧЕНИЯ ДОСТУПА К ИНФОРМАЦИИ, РАСПРОСТРАНЯЕМОЙ С НАРУШЕНИЕМ ЗАКОНА

(введена Федеральным законом от 28.12.2013 № 398-ФЗ)

1. В случае обнаружения в информационно-телекоммуникационных сетях, в том числе в сети «Интернет», информации, содержащей призывы к массовым беспорядкам, осуществлению экстремистской деятельности, участию в массовых (публичных) мероприятиях, проводимых с нарушением установленного порядка, информационных материалов иностранной или международной неправительственной организации, деятельность которой признана нежелательной на территории Российской Федерации в соответствии с Федеральным законом от 28 декабря 2012 года № 272-ФЗ «О мерах воздействия на лиц, причастных к нарушениям основополагающих прав и свобод человека, прав и свобод граждан Российской Федерации», сведений, позволяющих получить доступ к указанным информации или материалам (далее — распространяемая с наруше-

нием закона информация), включая случай поступления уведомления о распространяемой с нарушением закона информации от федеральных органов государственной власти, органов государственной власти субъектов Российской Федерации, органов местного самоуправления, организаций или граждан, Генеральный прокурор Российской Федерации или его заместители обращаются в федеральный орган исполнительной власти, осуществляющий функции по контролю и надзору в сфере средств массовой информации, массовых коммуникаций, информационных технологий и связи, с требованием о принятии мер по ограничению доступа к информационным ресурсам, распространяющим такую информацию.

(Часть 1 в ред. Федерального закона от 25.11.2017 № 327-ФЗ.)

2. Федеральный орган исполнительной власти, осуществляющий функции по контролю и надзору в сфере средств массовой информации, массовых коммуникаций, информационных технологий и связи, на основании обращения, указанного в части 1 настоящей статьи, незамедлительно:

1) направляет по системе взаимодействия операторам связи требование о принятии мер по ограничению доступа к информационному ресурсу, в том числе к сайту в сети «Интернет», на котором размещена распространяемая с нарушением закона информация. Данное требование должно содержать доменное имя сайта в сети «Интернет», сетевой адрес, указатели страниц сайта в сети «Интернет», позволяющие идентифицировать такую информацию (в ред. Федерального закона от 25.11.2017 № 327-ФЗ);

2) определяет провайдера хостинга или иное лицо, обеспечивающее размещение в информационно-телекоммуникационной сети, в том числе в сети «Интернет», указанного информационного ресурса, обслуживающего владельца сайта в сети «Интернет», на котором размещена распространяемая с нарушением закона информация (в ред. Федерального закона от 25.11.2017 № 327-ФЗ);

3) направляет провайдеру хостинга или иному указанному в пункте 2 настоящей части лицу уведомление

в электронном виде на русском и английском языках о нарушении порядка распространения информации с указанием доменного имени и сетевого адреса, позволяющих идентифицировать сайт в сети «Интернет», на котором размещена распространяемая с нарушением закона информация, а также указателей страниц сайта в сети «Интернет», позволяющих идентифицировать такую информацию, и с требованием принять меры по удалению такой информации (в ред. Федерального закона от 25.11.2017 № 327-ФЗ);

4) фиксирует дату и время направления уведомления провайдеру хостинга или иному указанному в пункте 2 настоящей части лицу в соответствующей информационной системе.

3. После получения по системе взаимодействия требования федерального органа исполнительной власти, осуществляющего функции по контролю и надзору в сфере средств массовой информации, массовых коммуникаций, информационных технологий и связи, о принятии мер по ограничению доступа оператор связи, оказывающий услуги по предоставлению доступа к информационно-телекоммуникационной сети «Интернет», обязан незамедлительно ограничить доступ к информационному ресурсу, в том числе к сайту в сети «Интернет», на котором размещена распространяемая с нарушением закона информация.

(В ред. Федерального закона от 25.11.2017 № 327-ФЗ.)

4. В течение суток с момента получения уведомления, указанного в пункте 3 части 2 настоящей статьи, провайдер хостинга или иное указанное в пункте 2 части 2 настоящей статьи лицо обязаны проинформировать об этом обслуживаемого ими владельца информационного ресурса и уведомить его о необходимости незамедлительно удалить распространяемую с нарушением закона информацию.

(В ред. Федерального закона от 25.11.2017 № 327-ФЗ.)

5. В случае, если владелец информационного ресурса удалил распространяемую с нарушением закона информацию, он направляет уведомление об этом в федеральный орган исполнительной власти, осуществ-

ляющий функции по контролю и надзору в сфере средств массовой информации, массовых коммуникаций, информационных технологий и связи. Такое уведомление может быть направлено также в электронном виде.

(В ред. Федерального закона от 25.11.2017 № 327-ФЗ.)

6. После получения уведомления, указанного в части 5 настоящей статьи, и проверки его достоверности федеральный орган исполнительной власти, осуществляющий функции по контролю и надзору в сфере средств массовой информации, массовых коммуникаций, информационных технологий и связи, обязан незамедлительно уведомить по системе взаимодействия оператора связи, оказывающего услуги по предоставлению доступа к информационно-телекоммуникационной сети «Интернет», о возобновлении доступа к информационному ресурсу, в том числе к сайту в сети «Интернет».

7. После получения уведомления, указанного в части 6 настоящей статьи, оператор связи незамедлительно возобновляет доступ к информационному ресурсу, в том числе к сайту в сети «Интернет».

### **СТАТЬЯ 15.4.** ПОРЯДОК ОГРАНИЧЕНИЯ ДОСТУПА К ИНФОРМАЦИОННОМУ РЕСУРСУ ОРГАНИЗАТОРА РАСПРОСТРАНЕНИЯ ИНФОРМАЦИИ В СЕТИ «ИНТЕРНЕТ»

(введена Федеральным законом от 05.05.2014 № 97-ФЗ)

1. В случае установления факта неисполнения организатором распространения информации в сети «Интернет» обязанностей, предусмотренных статьей 10.1 настоящего Федерального закона, в его адрес (адрес его филиала или представительства) уполномоченным федеральным органом исполнительной власти направляется уведомление, в котором указывается срок исполнения таких обязанностей, составляющий не менее чем пятнадцать дней.

(В ред. Федерального закона от 29.07.2017 № 241-ФЗ.)

2. В случае неисполнения организатором распространения информации в сети «Интернет» в указанный

в уведомлении срок обязанностей, предусмотренных статьей 10.1 настоящего Федерального закона, доступ к информационным системам и (или) программам для электронных вычислительных машин, которые предназначены и (или) используются для приема, передачи, доставки и (или) обработки электронных сообщений пользователей сети «Интернет» и функционирование которых обеспечивается данным организатором, до исполнения таких обязанностей ограничивается оператором связи, оказывающим услуги по предоставлению доступа к сети «Интернет», на основании вступившего в законную силу решения суда.

(В ред. Федерального закона от 29.07.2017 № 241-ФЗ.)

3. Порядок взаимодействия уполномоченного федерального органа исполнительной власти с организатором распространения информации в сети «Интернет», порядок направления указанного в части 1 настоящей статьи уведомления, порядок ограничения и возобновления доступа к указанным в части 2 настоящей статьи информационным системам и (или) программам и порядок информирования граждан (физических лиц) о таком ограничении устанавливаются Правительством Российской Федерации.

### **СТАТЬЯ 15.5.** ПОРЯДОК ОГРАНИЧЕНИЯ ДОСТУПА К ИНФОРМАЦИИ, ОБРАБАТЫВАЕМОЙ С НАРУШЕНИЕМ ЗАКОНОДАТЕЛЬСТВА РОССИЙСКОЙ ФЕДЕРАЦИИ В ОБЛАСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ

(введена Федеральным законом от 21.07.2014 № 242-ФЗ)

1. В целях ограничения доступа к информации в сети «Интернет», обрабатываемой с нарушением законодательства Российской Федерации в области персональных данных, создается автоматизированная информационная система «Реестр нарушителей прав субъектов персональных данных» (далее — реестр нарушителей).

2. В реестр нарушителей включаются:

1) доменные имена и (или) указатели страниц сайтов в сети «Интернет», содержащих информацию, обрабатываемую с нарушением законодательства Российской Федерации в области персональных данных;

2) сетевые адреса, позволяющие идентифицировать сайты в сети «Интернет», содержащие информацию, обрабатываемую с нарушением законодательства Российской Федерации в области персональных данных;

3) указание на вступивший в законную силу судебный акт;

4) информация об устранении нарушения законодательства Российской Федерации в области персональных данных;

5) дата направления операторам связи данных об информационном ресурсе для ограничения доступа к этому ресурсу.

3. Создание, формирование и ведение реестра нарушителей осуществляются федеральным органом исполнительной власти, осуществляющим функции по контролю и надзору в сфере средств массовой информации, массовых коммуникаций, информационных технологий и связи, в порядке, установленном Правительством Российской Федерации.

4. Федеральный орган исполнительной власти, осуществляющий функции по контролю и надзору в сфере средств массовой информации, массовых коммуникаций, информационных технологий и связи, в соответствии с критериями, определенными Правительством Российской Федерации, может привлечь к формированию и ведению реестра нарушителей оператора такого реестра — организацию, зарегистрированную на территории Российской Федерации.

5. Основанием для включения в реестр нарушителей информации, указанной в части 2 настоящей статьи, является вступивший в законную силу судебный акт.

6. Субъект персональных данных вправе обратиться в федеральный орган исполнительной власти, осуществляющий функции по контролю и надзору в сфере средств массовой информации, массовых коммуникаций, информационных технологий и связи, с заявлением о принятии мер по ограничению доступа к информации, обрабатываемой с нарушением законодательства Российской Федерации в области персональных данных, на основании вступившего в законную силу судебного акта. Форма указанного заявления утверждается

федеральным органом исполнительной власти, осуществляющим функции по контролю и надзору в сфере средств массовой информации, массовых коммуникаций, информационных технологий и связи.

7. В течение трех рабочих дней со дня получения вступившего в законную силу судебного акта федеральный орган исполнительной власти, осуществляющий функции по контролю и надзору в сфере средств массовой информации, массовых коммуникаций, информационных технологий и связи, на основании указанного решения суда:

1) определяет провайдера хостинга или иное лицо, обеспечивающее обработку информации в информационно-телекоммуникационной сети, в том числе в сети «Интернет», с нарушением законодательства Российской Федерации в области персональных данных;

2) направляет провайдеру хостинга или иному указанному в пункте 1 настоящей части лицу в электронном виде уведомление на русском и английском языках о нарушении законодательства Российской Федерации в области персональных данных с информацией о вступившем в законную силу судебном акте, доменном имени и сетевом адресе, позволяющих идентифицировать сайт в сети «Интернет», на котором осуществляется обработка информации с нарушением законодательства Российской Федерации в области персональных данных, а также об указателях страниц сайта в сети «Интернет», позволяющих идентифицировать такую информацию, и с требованием принять меры по устранению нарушения законодательства Российской Федерации в области персональных данных, указанные в решении суда;

3) фиксирует дату и время направления уведомления провайдеру хостинга или иному указанному в пункте 1 настоящей части лицу в реестре нарушителей.

8. В течение одного рабочего дня с момента получения уведомления, указанного в пункте 2 части 7 настоящей статьи, провайдер хостинга или иное указанное в пункте 1 части 7 настоящей статьи лицо обязаны проинформировать об этом обслуживаемого ими владельца информационного ресурса и уведомить его о необходимости незамедлительно принять меры по устранению

нарушения законодательства Российской Федерации в области персональных данных, указанного в уведомлении, или принять меры по ограничению доступа к информации, обрабатываемой с нарушением законодательства Российской Федерации в области персональных данных.

9. В течение одного рабочего дня с момента получения от провайдера хостинга или иного указанного в пункте 1 части 7 настоящей статьи лица уведомления о необходимости устранения нарушения законодательства Российской Федерации в области персональных данных владелец информационного ресурса обязан принять меры по устранению указанного в уведомлении нарушения. В случае отказа или бездействия владельца информационного ресурса провайдер хостинга или иное указанное в пункте 1 части 7 настоящей статьи лицо обязаны ограничить доступ к соответствующему информационному ресурсу не позднее истечения трех рабочих дней с момента получения уведомления, указанного в пункте 2 части 7 настоящей статьи.

10. В случае непринятия провайдером хостинга или иным указанным в пункте 1 части 7 настоящей статьи лицом и (или) владельцем информационного ресурса мер, указанных в частях 8 и 9 настоящей статьи, доменное имя сайта в сети «Интернет», его сетевой адрес, указатели страниц сайта в сети «Интернет», позволяющие идентифицировать информацию, обрабатываемую с нарушением законодательства Российской Федерации в области персональных данных, а также иные сведения об этом сайте и информация направляются по автоматизированной информационной системе операторам связи для принятия мер по ограничению доступа к данному информационному ресурсу, в том числе к сетевому адресу, доменному имени, указателю страниц сайта в сети «Интернет».

11. Федеральный орган исполнительной власти, осуществляющий функции по контролю и надзору в сфере средств массовой информации, массовых коммуникаций, информационных технологий и связи, или привлеченный им в соответствии с частью 4 настоящей статьи оператор реестра нарушителей исключает из такого реестра доменное имя, указатель страницы сайта

в сети «Интернет» или сетевой адрес, позволяющие идентифицировать сайт в сети «Интернет», на основании обращения владельца сайта в сети «Интернет», провайдера хостинга или оператора связи не позднее чем в течение трех дней со дня такого обращения после принятия мер по устранению нарушения законодательства Российской Федерации в области персональных данных или на основании вступившего в законную силу решения суда об отмене ранее принятого судебного акта.

12. Порядок взаимодействия оператора реестра нарушителей с провайдером хостинга и порядок получения доступа к содержащейся в таком реестре информации оператором связи устанавливаются уполномоченным Правительством Российской Федерации федеральным органом исполнительной власти.

### **СТАТЬЯ 15.6.** ПОРЯДОК ОГРАНИЧЕНИЯ ДОСТУПА К САЙТАМ В СЕТИ «ИНТЕРНЕТ», НА КОТОРЫХ НЕОДНОКРАТНО И НЕПРАВОМЕРНО РАЗМЕЩАЛАСЬ ИНФОРМАЦИЯ, СОДЕРЖАЩАЯ ОБЪЕКТЫ АВТОРСКИХ И (ИЛИ) СМЕЖНЫХ ПРАВ, ИЛИ ИНФОРМАЦИЯ, НЕОБХОДИМАЯ ДЛЯ ИХ ПОЛУЧЕНИЯ С ИСПОЛЬЗОВАНИЕМ ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННЫХ СЕТЕЙ, В ТОМ ЧИСЛЕ СЕТИ «ИНТЕРНЕТ»

(введена Федеральным законом от 24.11.2014 № 364-ФЗ)

1. В течение суток с момента поступления по системе взаимодействия в адрес федерального органа исполнительной власти, осуществляющего функции по контролю и надзору в сфере средств массовой информации, массовых коммуникаций, информационных технологий и связи, вступившего в законную силу соответствующего решения Московского городского суда указанный орган:

1) направляет операторам связи по системе взаимодействия требование о принятии мер по постоянному ограничению доступа к сайту в сети «Интернет», на котором неоднократно и неправомерно размещалась информация, содержащая объекты авторских и (или) смежных прав, или информация, необходимая для их получения с использованием информационно-телекоммуникационных сетей, в том числе сети «Интернет»;

2) направляет в порядке, установленном федеральным органом исполнительной власти, осуществляющим функции по контролю и надзору в сфере средств массовой информации, массовых коммуникаций, информационных технологий и связи, операторам поисковых систем, распространяющим в сети «Интернет» рекламу, которая направлена на привлечение внимания потребителей, находящихся на территории Российской Федерации, в электронном виде требование о прекращении выдачи сведений о доменном имени и об указателях страниц сайтов в сети «Интернет», на которых неоднократно и неправомерно размещалась информация, содержащая объекты авторских и (или) смежных прав, или информация, необходимая для их получения с использованием информационно-телекоммуникационных сетей, в том числе сети «Интернет».

(Часть 1 в ред. Федерального закона от 01.07.2017 № 156-ФЗ.)

2. В течение суток с момента получения указанного в пункте 1 части 1 настоящей статьи требования оператор связи, оказывающий услуги по предоставлению доступа к информационно-телекоммуникационной сети «Интернет», обязан ограничить доступ к соответствующему сайту в сети «Интернет». Снятие ограничения доступа к такому сайту в сети «Интернет» не допускается.

(В ред. Федерального закона от 01.07.2017 № 156-ФЗ.)

2.1. В течение суток с момента получения указанного в пункте 2 части 1 настоящей статьи требования оператор поисковой системы, распространяющий в сети «Интернет» рекламу, которая направлена на привлечение внимания потребителей, находящихся на территории Российской Федерации, обязан прекратить выдачу сведений о доменном имени и об указателях страниц сайтов в сети «Интернет», доступ к которым ограничен на основании соответствующего решения Московского городского суда.

(Часть 2.1 введена Федеральным законом от 01.07.2017 № 156-ФЗ.)

3. Сведения о сайтах в сети «Интернет», доступ к которым ограничен на основании решения Московского городского суда, размещаются на официальном сайте

федерального органа исполнительной власти, осуществляющего функции по контролю и надзору в сфере средств массовой информации, массовых коммуникаций, информационных технологий и связи, в информационно-телекоммуникационной сети «Интернет».

### **СТАТЬЯ 15.6-1.** ПОРЯДОК ОГРАНИЧЕНИЯ ДОСТУПА К КОПИЯМ ЗАБЛОКИРОВАННЫХ САЙТОВ

(введена Федеральным законом от 01.07.2017 № 156-ФЗ)

1. Размещение в информационно-телекоммуникационных сетях, в том числе в сети «Интернет», сайта, сходного до степени смешения с сайтом в сети «Интернет», доступ к которому ограничен по решению Московского городского суда в связи с неоднократным и неправомерным размещением информации, содержащей объекты авторских и (или) смежных прав, или информации, необходимой для их получения с использованием информационно-телекоммуникационных сетей, в том числе сети «Интернет» (далее — копия заблокированного сайта), не допускается.

2. В случае поступления от федеральных органов исполнительной власти или правообладателей информации об обнаружении в информационно-телекоммуникационных сетях, в том числе в сети «Интернет», указанного в части 1 настоящей статьи сайта федеральный орган исполнительной власти, осуществляющий функции по выработке и реализации государственной политики и нормативно-правовому регулированию в сфере массовых коммуникаций и средств массовой информации, в течение суток:

1) в порядке, установленном Правительством Российской Федерации, принимает мотивированное решение о признании сайта в сети «Интернет» копией заблокированного сайта;

2) направляет в порядке, установленном федеральным органом исполнительной власти, осуществляющим функции по выработке и реализации государственной политики и нормативно-правовому регулированию в сфере массовых коммуникаций и средств массовой информации, владельцу копии заблокированного сайта в электронном виде на русском и англий-

ском языках мотивированное решение о признании сайта в сети «Интернет» копией заблокированного сайта;

3) направляет по системе взаимодействия в федеральный орган исполнительной власти, осуществляющий функции по контролю и надзору в сфере средств массовой информации, массовых коммуникаций, информационных технологий и связи, мотивированное решение о признании сайта в сети «Интернет» копией заблокированного сайта.

3. В течение суток с момента поступления по системе взаимодействия мотивированного решения федерального органа исполнительной власти, осуществляющего функции по выработке и реализации государственной политики и нормативно-правовому регулированию в сфере массовых коммуникаций и средств массовой информации, о признании сайта в сети «Интернет» копией заблокированного сайта, федеральный орган исполнительной власти, осуществляющий функции по контролю и надзору в сфере средств массовой информации, массовых коммуникаций, информационных технологий и связи:

1) определяет провайдера хостинга или иное обеспечивающее размещение копии заблокированного сайта в сети «Интернет» лицо;

2) направляет провайдеру хостинга или указанному в пункте 1 настоящей части лицу уведомление в электронном виде на русском и английском языках о принятом федеральным органом исполнительной власти, осуществляющим функции по выработке и реализации государственной политики и нормативно-правовому регулированию в сфере массовых коммуникаций и средств массовой информации, мотивированном решении о признании сайта в сети «Интернет» копией заблокированного сайта;

3) фиксирует дату и время направления предусмотренного пунктом 2 настоящей части уведомления провайдеру хостинга или указанному в пункте 1 настоящей части лицу в соответствующей информационной системе;

4) направляет по системе взаимодействия операторам связи требование о принятии мер по ограничению доступа к копии заблокированного сайта;

5) направляет в порядке, установленном федеральным органом исполнительной власти, осуществляющим функции по контролю и надзору в сфере средств массовой информации, массовых коммуникаций, информационных технологий и связи, операторам поисковых систем, распространяющим в сети «Интернет» рекламу, которая направлена на привлечение внимания потребителей, находящихся на территории Российской Федерации, в электронном виде требование о прекращении выдачи сведений о доменном имени и об указателях страниц копии заблокированного сайта.

4. В течение суток с момента получения указанного в пункте 4 части 3 настоящей статьи требования оператор связи, оказывающий услуги по предоставлению доступа к информационно-телекоммуникационной сети, в том числе сети «Интернет», обязан ограничить доступ к копии заблокированного сайта.

5. В течение суток с момента получения указанного в пункте 5 части 3 настоящей статьи требования оператор поисковой системы, распространяющий в сети «Интернет» рекламу, которая направлена на привлечение внимания потребителей, находящихся на территории Российской Федерации, обязан прекратить выдачу сведений о доменном имени и об указателях страниц копии заблокированного сайта.

6. Сведения о копиях заблокированных сайтов размещаются на официальном сайте федерального органа исполнительной власти, осуществляющего функции по контролю и надзору в сфере средств массовой информации, массовых коммуникаций, информационных технологий и связи, в сети «Интернет».

### **СТАТЬЯ 15.7.** ВНЕСУДЕБНЫЕ МЕРЫ ПО ПРЕКРАЩЕНИЮ НАРУШЕНИЯ АВТОРСКИХ И (ИЛИ) СМЕЖНЫХ ПРАВ В ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННЫХ СЕТЯХ, В ТОМ ЧИСЛЕ В СЕТИ «ИНТЕРНЕТ», ПРИНИМАЕМЫЕ ПО ЗАЯВЛЕНИЮ ПРАВООБЛАДАТЕЛЯ

(введена Федеральным законом от 24.11.2014 № 364-ФЗ)

1. Правообладатель в случае обнаружения в информационно-телекоммуникационных сетях, в том числе в сети «Интернет», сайта в сети «Интернет», на кото-

ром без его разрешения или иного законного основания размещена информация, содержащая объекты авторских и (или) смежных прав, или информация, необходимая для их получения с использованием информационно-телекоммуникационных сетей, в том числе сети «Интернет», вправе направить владельцу сайта в сети «Интернет» в письменной или электронной форме заявление о нарушении авторских и (или) смежных прав (далее — заявление). Заявление может быть направлено лицом, уполномоченным правообладателем в соответствии с законодательством Российской Федерации.

2. Заявление должно содержать:

1) сведения о правообладателе или лице, уполномоченном правообладателем (если заявление направляется таким лицом) (далее — заявитель):

а) для физического лица — фамилию, имя, отчество, паспортные данные (серия и номер, кем выдан, дата выдачи), контактную информацию (номера телефона и (или) факса, адрес электронной почты);

б) для юридического лица — наименование, место нахождения и адрес, контактную информацию (номера телефона и (или) факса, адрес электронной почты);

2) информацию об объекте авторских и (или) смежных прав, размещенном на сайте в сети «Интернет» без разрешения правообладателя или иного законного основания;

3) указание на доменное имя и (или) сетевой адрес сайта в сети «Интернет», на котором без разрешения правообладателя или иного законного основания размещена информация, содержащая объект авторских и (или) смежных прав, или информация, необходимая для его получения с использованием информационно-телекоммуникационных сетей, в том числе сети «Интернет»;

4) указание на наличие у правообладателя прав на объект авторских и (или) смежных прав, размещенный на сайте в сети «Интернет» без разрешения правообладателя или иного законного основания;

5) указание на отсутствие разрешения правообладателя на размещение на сайте в сети «Интернет» инфор-

мации, содержащей объект авторских и (или) смежных прав, или информации, необходимой для его получения с использованием информационно-телекоммуникационных сетей, в том числе сети «Интернет»;

6) согласие заявителя на обработку его персональных данных (для заявителя — физического лица).

3. В случае, если заявление подается уполномоченным лицом, к заявлению прикладывается копия документа (в письменной или электронной форме), подтверждающего его полномочия.

4. В случае обнаружения неполноты сведений, неточностей или ошибок в заявлении владелец сайта в сети «Интернет» вправе направить заявителю в течение двадцати четырех часов с момента получения заявления уведомление об уточнении представленных сведений. Указанное уведомление может быть направлено заявителю однократно.

5. В течение двадцати четырех часов с момента получения уведомления, указанного в части 4 настоящей статьи, заявитель принимает меры, направленные на восполнение недостающих сведений, устранение неточностей и ошибок, и направляет владельцу сайта в сети «Интернет» уточненные сведения.

6. В течение двадцати четырех часов с момента получения заявления или уточненных заявителем сведений (в случае направления заявителю уведомления, указанного в части 4 настоящей статьи) владелец сайта в сети «Интернет» удаляет указанную в части 1 настоящей статьи информацию.

7. При наличии у владельца сайта в сети «Интернет» доказательств, подтверждающих правомерность размещения на принадлежащем ему сайте в сети «Интернет» информации, содержащей объект авторских и (или) смежных прав, или информации, необходимой для его получения с использованием информационно-телекоммуникационных сетей, в том числе сети «Интернет», владелец сайта в сети «Интернет» вправе не принимать предусмотренные частью 6 настоящей статьи меры и обязан направить заявителю соответствующее уведомление с приложением указанных доказательств.

8. Правила настоящей статьи в равной степени распространяются на правообладателя и на лицензиата, получившего исключительную лицензию на объект авторских и (или) смежных прав.

**СТАТЬЯ 15.8.** МЕРЫ, НАПРАВЛЕННЫЕ НА ПРОТИВОДЕЙСТВИЕ ИСПОЛЬЗОВАНИЮ НА ТЕРРИТОРИИ РОССИЙСКОЙ ФЕДЕРАЦИИ ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННЫХ СЕТЕЙ И ИНФОРМАЦИОННЫХ РЕСУРСОВ, ПОСРЕДСТВОМ КОТОРЫХ ОБЕСПЕЧИВАЕТСЯ ДОСТУП К ИНФОРМАЦИОННЫМ РЕСУРСАМ И ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННЫМ СЕТЯМ, ДОСТУП К КОТОРЫМ ОГРАНИЧЕН НА ТЕРРИТОРИИ РОССИЙСКОЙ ФЕДЕРАЦИИ

(введена Федеральным законом от 29.07.2017 № 276-ФЗ)

1. Владельцам информационно-телекоммуникационных сетей, информационных ресурсов (сайт в сети «Интернет» и (или) страница сайта в сети «Интернет», информационная система, программа для электронных вычислительных машин), посредством которых обеспечивается доступ к информационным ресурсам, информационно-телекоммуникационным сетям, доступ к которым ограничен на территории Российской Федерации в соответствии с настоящим Федеральным законом (далее также — владелец программно-аппаратных средств доступа к информационным ресурсам, информационно-телекоммуникационным сетям, доступ к которым ограничен), запрещается предоставлять возможность использования на территории Российской Федерации принадлежащих им информационно-телекоммуникационных сетей и информационных ресурсов для получения доступа к информационным ресурсам, информационно-телекоммуникационным сетям, доступ к которым ограничен на территории Российской Федерации в соответствии с настоящим Федеральным законом.

2. В целях противодействия использованию на территории Российской Федерации информационно-телекоммуникационных сетей, информационных ресурсов, посредством которых обеспечивается доступ к информационным ресурсам, информационно-телекоммуникационным сетям, доступ к которым ограничен на

территории Российской Федерации в соответствии с настоящим Федеральным законом (далее также — программно-аппаратные средства доступа к информационным ресурсам, информационно-телекоммуникационным сетям, доступ к которым ограничен), для получения доступа к информационным ресурсам, информационно-телекоммуникационным сетям, доступ к которым ограничен на территории Российской Федерации в соответствии с настоящим Федеральным законом, федеральный орган исполнительной власти, осуществляющий функции по контролю и надзору в сфере средств массовой информации, массовых коммуникаций, информационных технологий и связи:

1) осуществляет создание и эксплуатацию федеральной государственной информационной системы, содержащей перечень информационных ресурсов, информационно-телекоммуникационных сетей, доступ к которым ограничен на территории Российской Федерации в соответствии с настоящим Федеральным законом (далее — федеральная государственная информационная система информационных ресурсов информационно-телекоммуникационных сетей, доступ к которым ограничен);

2) в порядке, установленном Правительством Российской Федерации, взаимодействует с федеральными органами исполнительной власти, осуществляющими оперативно-разыскную деятельность или обеспечение безопасности Российской Федерации, в целях получения информации о программно-аппаратных средствах доступа к информационным ресурсам, информационно-телекоммуникационным сетям, доступ к которым ограничен;

3) на основании обращения федерального органа исполнительной власти, осуществляющего оперативно-разыскную деятельность или обеспечение безопасности Российской Федерации, определяет провайдера хостинга или иное лицо, обеспечивающее размещение в сети «Интернет» программно-аппаратных средств доступа к информационным ресурсам, информационно-телекоммуникационным сетям, доступ к которым ограничен;

4) направляет провайдеру хостинга или иному указанному в пункте 3 настоящей части лицу уведомление в электронном виде на русском и английском языках о необходимости предоставления данных, позволяющих идентифицировать владельца программно-аппаратных средств доступа к информационным ресурсам, информационно-телекоммуникационным сетям, доступ к которым ограничен, или о необходимости уведомления владельца программно-аппаратных средств доступа к информационным ресурсам, информационно-телекоммуникационным сетям, доступ к которым ограничен, о необходимости размещения указанных данных на сайте в сети «Интернет» такого владельца;

5) фиксирует дату и время направления указанного в пункте 4 настоящей части уведомления в федеральной государственной информационной системе информационных ресурсов, информационно-телекоммуникационных сетей, доступ к которым ограничен.

3. В течение трех рабочих дней со дня получения уведомления, указанного в пункте 4 части 2 настоящей статьи, провайдер хостинга или иное указанное в пункте 3 части 2 настоящей статьи лицо обязаны предоставить информацию о совершении действий, предусмотренных таким уведомлением.

4. В течение трех рабочих дней со дня получения данных, позволяющих идентифицировать владельца программно-аппаратных средств доступа к информационным ресурсам, информационно-телекоммуникационным сетям, доступ к которым ограничен, или самостоятельного выявления таких данных федеральным органом исполнительной власти, осуществляющим функции по контролю и надзору в сфере средств массовой информации, массовых коммуникаций, информационных технологий и связи, указанный федеральный орган исполнительной власти направляет этому владельцу на русском и английском языках требование о необходимости подключения такого владельца к федеральной государственной информационной системе информационных ресурсов, информационно-телекоммуникационных сетей, доступ к которым ограничен.

5. В течение тридцати рабочих дней со дня направления требования, указанного в части 4 настоящей статьи, владелец программно-аппаратных средств доступа к информационным ресурсам, информационно-телекоммуникационным сетям, доступ к которым ограничен, обязан подключиться к федеральной государственной информационной системе информационных ресурсов, информационно-телекоммуникационных сетей, доступ к которым ограничен, в порядке, установленном федеральным органом исполнительной власти, осуществляющим функции по контролю и надзору в сфере средств массовой информации, массовых коммуникаций, информационных технологий и связи.

6. По требованию федерального органа исполнительной власти, осуществляющего функции по контролю и надзору в сфере средств массовой информации, массовых коммуникаций, информационных технологий и связи, к федеральной государственной информационной системе информационных ресурсов, информационно-телекоммуникационных сетей, доступ к которым ограничен, также обязан подключиться оператор поисковой системы, распространяющий в сети «Интернет» рекламу, которая направлена на привлечение внимания потребителей, находящихся на территории Российской Федерации, в течение тридцати рабочих дней со дня получения указанного требования.

7. Владелец программно-аппаратных средств доступа к информационным ресурсам, информационно-телекоммуникационным сетям, доступ к которым ограничен, обязан:

1) в течение трех рабочих дней после предоставления ему доступа к федеральной государственной информационной системе информационных ресурсов, информационно-телекоммуникационных сетей, доступ к которым ограничен, обеспечить соблюдение запрета предоставлять возможность использования на территории Российской Федерации программно-аппаратных средств доступа к информационным ресурсам, информационно-телекоммуникационным сетям, доступ к которым ограничен, для получения доступа к информационным ресурсам, информационно-телекоммуника-

ционным сетям, доступ к которым ограничен на территории Российской Федерации в соответствии с настоящим Федеральным законом;

2) соблюдать установленный федеральным органом исполнительной власти, осуществляющим функции по контролю и надзору в сфере средств массовой информации, массовых коммуникаций, информационных технологий и связи, режим обработки и использования информации, размещенной в федеральной государственной информационной системе информационных ресурсов, информационно-телекоммуникационных сетей, доступ к которым ограничен.

8. В течение трех рабочих дней со дня получения доступа к федеральной государственной информационной системе информационных ресурсов, информационно-телекоммуникационных сетей, доступ к которым ограничен, оператор поисковой системы, распространяющий в сети «Интернет» рекламу, которая направлена на привлечение внимания потребителей, находящихся на территории Российской Федерации, обязан прекратить на территории Российской Федерации выдачу по запросам пользователей указанной поисковой системы сведений об информационных ресурсах, информационно-телекоммуникационных сетях, доступ к которым ограничен на территории Российской Федерации в соответствии с настоящим Федеральным законом.

9. Порядок взаимодействия федерального органа исполнительной власти, осуществляющего функции по контролю и надзору в сфере средств массовой информации, массовых коммуникаций, информационных технологий и связи, с лицами, указанными в частях 5 и 6 настоящей статьи, при предоставлении доступа к федеральной государственной информационной системе информационных ресурсов, информационно-телекоммуникационных сетей, доступ к которым ограничен, порядок доступа к указанной системе и к информации, размещенной в ней, режим обработки и использования такой информации, требования к технологическим, программным, лингвистическим, правовым и организационным средствам обеспечения пользования ука-

занной системой устанавливаются федеральным органом исполнительной власти, осуществляющим функции по контролю и надзору в сфере средств массовой информации, массовых коммуникаций, информационных технологий и связи.

10. В случае неисполнения владельцем программно-аппаратных средств доступа к информационным ресурсам, информационно-телекоммуникационным сетям, доступ к которым ограничен, обязанностей, предусмотренных частями 5 и 7 настоящей статьи, федеральный орган исполнительной власти, осуществляющий функции по контролю и надзору в сфере средств массовой информации, массовых коммуникаций, информационных технологий и связи, принимает решение об ограничении доступа к принадлежащим такому владельцу программно-аппаратным средствам доступа к информационным ресурсам, информационно-телекоммуникационным сетям, доступ к которым ограничен.

11. В течение суток с момента принятия указанного в части 10 настоящей статьи решения федеральный орган исполнительной власти, осуществляющий функции по контролю и надзору в сфере средств массовой информации, массовых коммуникаций, информационных технологий и связи, направляет по системе взаимодействия операторам связи, оказывающим услуги по предоставлению доступа к сети «Интернет», информацию, необходимую для ограничения доступа к соответствующим программно-аппаратным средствам доступа к информационным ресурсам, информационно-телекоммуникационным сетям, доступ к которым ограничен.

12. Операторы связи, оказывающие услуги по предоставлению доступа к сети «Интернет», в течение суток с момента получения по системе взаимодействия информации, указанной в части 11 настоящей статьи, обязаны в соответствии с полученной информацией ограничить на территории Российской Федерации доступ к соответствующим программно-аппаратным средствам доступа к информационным ресурсам, информационно-телекоммуникационным сетям, доступ к которым ограничен.

13. В случае, если владелец программно-аппаратных средств доступа к информационным ресурсам, информационно-телекоммуникационным сетям, доступ к которым ограничен, обеспечил исполнение обязанностей, предусмотренных частями 5 и 7 настоящей статьи, он направляет уведомление об этом в федеральный орган исполнительной власти, осуществляющий функции по контролю и надзору в сфере средств массовой информации, массовых коммуникаций, информационных технологий и связи. Такое уведомление может быть направлено также в электронном виде.

14. После получения уведомления, указанного в части 13 настоящей статьи, и проверки его достоверности федеральный орган исполнительной власти, осуществляющий функции по контролю и надзору в сфере средств массовой информации, массовых коммуникаций, информационных технологий и связи, обязан в течение суток уведомить по системе взаимодействия операторов связи, оказывающих услуги по предоставлению доступа к сети «Интернет», о необходимости возобновления доступа к информационно-телекоммуникационным сетям, информационным ресурсам, доступ к которым был ограничен на основании решения указанного федерального органа исполнительной власти в соответствии с частью 10 настоящей статьи.

15. Операторы связи, оказывающие услуги по предоставлению доступа к сети «Интернет», в течение суток с момента получения по системе взаимодействия уведомления, указанного в части 14 настоящей статьи, обязаны прекратить ограничение доступа к информационно-телекоммуникационным сетям, информационным ресурсам, доступ к которым был ограничен на основании решения федерального органа исполнительной власти, осуществляющего функции по контролю и надзору в сфере средств массовой информации, массовых коммуникаций, информационных технологий и связи, в соответствии с частью 10 настоящей статьи.

16. Порядок контроля за обеспечением ограничения доступа к программно-аппаратным средствам доступа к информационным ресурсам, информационно-телекоммуникационным сетям, доступ к которым

ограничен, и порядок контроля за прекращением на территории Российской Федерации выдачи операторами поисковых систем, распространяющими в сети «Интернет» рекламу, которая направлена на привлечение внимания потребителей, находящихся на территории Российской Федерации, сведений об информационных ресурсах, информационно-телекоммуникационных сетях, доступ к которым ограничен на территории Российской Федерации в соответствии с настоящим Федеральным законом, утверждаются федеральным органом исполнительной власти, осуществляющим функции по контролю и надзору в сфере средств массовой информации, массовых коммуникаций, информационных технологий и связи.

17. Положения настоящей статьи не распространяются на операторов государственных информационных систем, государственные органы и органы местного самоуправления, а также на случаи использования программно-аппаратных средств доступа к информационным ресурсам, информационно-телекоммуникационным сетям, доступ к которым ограничен, при условии, что круг пользователей таких программно-аппаратных средств их владельцами заранее определен и использование таких программно-аппаратных средств осуществляется в технологических целях обеспечения деятельности лица, осуществляющего их использование.

### **СТАТЬЯ 16.** ЗАЩИТА ИНФОРМАЦИИ

1. Защита информации представляет собой принятие правовых, организационных и технических мер, направленных на:

1) обеспечение защиты информации от неправомерного доступа, уничтожения, модифицирования, блокирования, копирования, предоставления, распространения, а также от иных неправомерных действий в отношении такой информации;

2) соблюдение конфиденциальности информации ограниченного доступа;

3) реализацию права на доступ к информации.

2. Государственное регулирование отношений в сфере защиты информации осуществляется путем установ-

ления требований о защите информации, а также ответственности за нарушение законодательства Российской Федерации об информации, информационных технологиях и о защите информации.

3. Требования о защите общедоступной информации могут устанавливаться только для достижения целей, указанных в пунктах 1 и 3 части 1 настоящей статьи.

4. Обладатель информации, оператор информационной системы в случаях, установленных законодательством Российской Федерации, обязаны обеспечить:

1) предотвращение несанкционированного доступа к информации и (или) передачи ее лицам, не имеющим права на доступ к информации;

2) своевременное обнаружение фактов несанкционированного доступа к информации;

3) предупреждение возможности неблагоприятных последствий нарушения порядка доступа к информации;

4) недопущение воздействия на технические средства обработки информации, в результате которого нарушается их функционирование;

5) возможность незамедлительного восстановления информации, модифицированной или уничтоженной вследствие несанкционированного доступа к ней;

6) постоянный контроль за обеспечением уровня защищенности информации;

7) нахождение на территории Российской Федерации баз данных информации, с использованием которых осуществляются сбор, запись, систематизация, накопление, хранение, уточнение (обновление, изменение), извлечение персональных данных граждан Российской Федерации. (Пункт 7 введен Федеральным законом от 21.07.2014 № 242-ФЗ.)

5. Требования о защите информации, содержащейся в государственных информационных системах, устанавливаются федеральным органом исполнительной власти в области обеспечения безопасности и федеральным органом исполнительной власти, уполномоченным в области противодействия техническим разведкам и технической защиты информации, в пределах их пол-

номочий. При создании и эксплуатации государственных информационных систем используемые в целях защиты информации методы и способы ее защиты должны соответствовать указанным требованиям.

6. Федеральными законами могут быть установлены ограничения использования определенных средств защиты информации и осуществления отдельных видов деятельности в области защиты информации.

### **СТАТЬЯ 17.** ОТВЕТСТВЕННОСТЬ ЗА ПРАВОНАРУШЕНИЯ В СФЕРЕ ИНФОРМАЦИИ, ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ И ЗАЩИТЫ ИНФОРМАЦИИ

1. Нарушение требований настоящего Федерального закона влечет за собой дисциплинарную, гражданско-правовую, административную или уголовную ответственность в соответствии с законодательством Российской Федерации.

1.1. Лица, виновные в нарушении требований статьи 14.1 настоящего Федерального закона в части обработки, включая сбор и хранение, биометрических персональных данных, несут административную, гражданскую и уголовную ответственность в соответствии с законодательством Российской Федерации.

(Часть 1.1 введена Федеральным законом от 31.12.2017 № 482-ФЗ.)

2. Лица, права и законные интересы которых были нарушены в связи с разглашением информации ограниченного доступа или иным неправомерным использованием такой информации, вправе обратиться в установленном порядке за судебной защитой своих прав, в том числе с исками о возмещении убытков, компенсации морального вреда, защите чести, достоинства и деловой репутации. Требование о возмещении убытков не может быть удовлетворено в случае предъявления его лицом, не принимавшим мер по соблюдению конфиденциальности информации или нарушившим установленные законодательством Российской Федерации требования о защите информации, если принятие этих мер и соблюдение таких требований являлись обязанностями данного лица.

3. В случае, если распространение определенной информации ограничивается или запрещается федеральными законами, гражданско-правовую ответственность за распространение такой информации не несет лицо, оказывающее услуги:

1) либо по передаче информации, предоставленной другим лицом, при условии ее передачи без изменений и исправлений;

2) либо по хранению информации и обеспечению доступа к ней при условии, что это лицо не могло знать о незаконности распространения информации.

4. Провайдер хостинга, оператор связи и владелец сайта в сети «Интернет» не несут ответственность перед правообладателем и перед пользователем за ограничение доступа к информации и (или) ограничение ее распространения в соответствии с требованиями настоящего Федерального закона.

(Часть 4 введена Федеральным законом от 02.07.2013 № 187-ФЗ, в ред. Федерального закона от 24.11.2014 № 364-ФЗ.)

### **СТАТЬЯ 18.** О ПРИЗНАНИИ УТРАТИВШИМИ СИЛУ ОТДЕЛЬНЫХ ЗАКОНОДАТЕЛЬНЫХ АКТОВ (ПОЛОЖЕНИЙ ЗАКОНОДАТЕЛЬНЫХ АКТОВ) РОССИЙСКОЙ ФЕДЕРАЦИИ

Со дня вступления в силу настоящего Федерального закона признать утратившими силу:

1) Федеральный закон от 20 февраля 1995 года № 24-ФЗ «Об информации, информатизации и защите информации» (Собрание законодательства Российской Федерации, 1995, № 8, ст. 609);

2) Федеральный закон от 4 июля 1996 года № 85-ФЗ «Об участии в международном информационном обмене» (Собрание законодательства Российской Федерации, 1996, № 28, ст. 3347);

3) статью 16 Федерального закона от 10 января 2003 года № 15-ФЗ «О внесении изменений и дополнений в некоторые законодательные акты Российской Федерации в связи с принятием Федерального закона „О лицензировании отдельных видов деятельности“» (Собрание законодательства Российской Федерации, 2003, № 2, ст. 167);

4) статью 21 Федерального закона от 30 июня 2003 года № 86-ФЗ «О внесении изменений и дополнений в некоторые законодательные акты Российской Федерации, признании утратившими силу отдельных законодательных актов Российской Федерации, предоставлении отдельных гарантий сотрудникам органов внутренних дел, органов по контролю за оборотом наркотических средств и психотропных веществ и упраздняемых федеральных органов налоговой полиции в связи с осуществлением мер по совершенствованию государственного управления» (Собрание законодательства Российской Федерации, 2003, № 27, ст. 2700);

5) статью 39 Федерального закона от 29 июня 2004 года № 58-ФЗ «О внесении изменений в некоторые законодательные акты Российской Федерации и признании утратившими силу некоторых законодательных актов Российской Федерации в связи с осуществлением мер по совершенствованию государственного управления» (Собрание законодательства Российской Федерации, 2004, № 27, ст. 2711).

## Европейская конвенция по киберпреступлениям (преступлениям в киберпространстве). Будапешт, 23 ноября 2001 г.

### Преамбула

Государства — члены Совета Европы и другие подписавшие настоящую Конвенцию Государства,

Считая, что цель Совета Европы состоит в достижении большего единства между его членами;

Признавая ценность создания механизма сотрудничества с другими Государствами — членами настоящей Конвенции;

Убежденные в необходимости осуществлять общую политику в вопросах уголовного права, целью которой является защита общества от киберпреступлений, в том числе путем принятия соответствующих законодательных актов, а также путем расширения международного сотрудничества;

Ощущая глубокие изменения, вызванные распространением цифровых технологий, конвергенцией и продолжающейся глобализацией компьютерных сетей;

Обеспокоенные опасностью того, что компьютерные сети и электронная информация могут также использоваться для совершения преступлений, и что доказательства, касающиеся таких преступлений, могут сохраняться и передаваться по этим сетям;

Признавая необходимость сотрудничества между Государствами — членами Конвенции и частными лицами и организациями в борьбе против киберпреступлений и потребность защищать законные интересы в использовании и развитии информационных технологий;

Считая, что эффективная борьба против киберпреступлений требует наличия четкого, быстрого и эффективного механизма международного сотрудничества в вопросах, связанных с преступностью;

Разделяя убеждение в том, что настоящая Конвенция является необходимым условием для того, чтобы предотвратить правонарушения, направленные против

конфиденциальности, целостности и доступности компьютерных систем, сетей и данных, а также неправомерное использование указанных систем, сетей и данных через придание этим действиям статуса преступления в терминах, предусмотренных настоящей Конвенцией, а также путем применения властных полномочий, достаточных для эффективного противодействия указанным правонарушениям путем облегчения обнаружения, расследования и судебного преследования указанных правонарушений;

Помня о необходимости четкого баланса между интересами законности и уважением к фундаментальным правам человека, закрепленным в Конвенции Совета Европы 1950 г. «О защите прав и основных свобод человека», в Международном пакте ООН о гражданских и политических правах 1966 г., равно как и в других применимых в данном случае международных соглашениях о правах человека, которые подтверждают право каждого не подвергаться преследованию за свое мнение, равно как и право на свободу самовыражения, включая свободу искать, получать и распространять информацию и идеи, независимо от государственных границ, а также право на защиту от вмешательства в частную жизнь;

Признавая защиту личных данных, как это указано, например, в Конвенции Совета Европы 1981 г. о защите личности в связи с автоматической обработкой персональных данных;

Принимая во внимание Конвенцию Организации Объединенных Наций 1989 г. о правах ребенка и составленный Международной организацией труда список недопустимых форм детского труда (1999 г.);

Принимая во внимание действующие конвенции Совета Европы о сотрудничестве в борьбе с уголовными преступлениями, а также соглашения схожего характера, заключенные между государствами — членами Совета Европы и другими государствами; подчеркивая также, что настоящая Конвенция призвана дополнить указанные конвенции, с тем чтобы повысить эффективность расследования и разбирательства уголовных дел, связанных с компьютерными системами и данными,

а также сделать возможным сбор доказательств по уголовным преступлениям в электронной форме;

Приветствуя недавние шаги, направленные на дальнейшее расширение международного взаимопонимания и сотрудничества в сфере борьбы с киберпреступлениями, включая действия Организации Объединенных Наций, ОБСЕ, Европейского Союза и Большой Восьмерки;

Напоминая о Рекомендациях Комитета министров: № R (85) 10, касающейся практического применения Европейской Конвенции об оказании содействия в расследовании уголовных дел в отношении судебных поручений по вопросам перехвата телекоммуникаций; № R (88) 2 о борьбе с пиратством в области авторских и смежных прав; № R (87) 15, регламентирующей использование персональных данных органами полиции; № R (95) 4 о защите персональных данных в сфере телекоммуникационных услуг, с особой ссылкой на телефонные услуги; а также № R (89) 9 о преступлениях, связанных с компьютерами, в которой национальным законодательным органам даются указания по определению отдельных компьютерных преступлений, и № R (95) 13 по вопросам уголовного процессуального законодательства, связанным с информационными технологиями;

Принимая во внимание Резолюцию № 1, принятую на 21-й Конференции министров юстиции государств — членов Совета Европы (Прага, июнь 1997 г.), в которой Совету министров рекомендуется поддержать работу по сближению норм национального уголовного законодательства в разных странах и внедрению эффективных методов расследования такого рода правонарушений, проводимую Европейским комитетом по проблемам преступности (CDPC), так же как и Резолюцию № 3, принятую на 23-й Конференции министров юстиции государств — членов Совета Европы (Лондон, июнь 2000 г.), которая призвала участвующие в переговорах стороны прилагать все свои усилия к выработке решений, которые позволили бы наибольшему числу Государств присоединиться к Конвенции, а также подтвердила потребность в быстром и эффективном механизме

международного сотрудничества, который должным образом учитывал бы специфику борьбы с киберпреступлениями;

Проявляя уважение к Плану действий, принятому главами государств и правительств Совета Европы по случаю их второй встречи на высшем уровне (Страсбург, 10—11 октября 1997 г.), нацеленному на поиск общих рекомендаций в связи с развитием новых информационных технологий, которые основывались бы на стандартах и ценностях Совета Европы;

Согласились о нижеследующем:

## Глава I. Употребление терминов

### **СТАТЬЯ 1.** ОПРЕДЕЛЕНИЯ

В целях настоящей Конвенции:

(a) «компьютерная система» означает любое устройство или совокупность соединенных между собой или связанных устройств, одно либо более из которых осуществляет автоматическую обработку данных в соответствии с программой;

(b) «компьютерные данные» означает любое представление фактов, сведений или понятий в форме, пригодной для обработки с помощью компьютерных систем, в том числе программы, предназначенные для выполнения компьютерной системой определенных действий;

(c) «поставщик услуг» означает:

(i) любую государственную или частную организацию, предоставляющую своим пользователям возможность обмениваться данными (коммуникационные услуги) посредством компьютерной системы;

(ii) любую иную организацию, которая обрабатывает или хранит компьютерные данные по поручению организации, предоставляющей коммуникационные услуги, либо пользователей таких услуг;

(d) «данные трафика» означают любые компьютерные данные, связанные с операциями по передаче данных посредством компьютерной системы, которые созданы компьютерной системой, являвшейся звеном в цепочке передачи данных, и указывают на источник

сообщения, его назначение, маршрут, время, дату, размер, длительность или тип лежащей в его основе услуги.

## Глава II. Меры, которые предстоит принять на национальном уровне

## Раздел 1. Материальное уголовное право

### Часть 1. Преступления против конфиденциальности, целостности и доступности компьютерных данных и систем

#### **СТАТЬЯ 2.** НЕЗАКОННЫЙ ДОСТУП

Каждая из Сторон должна принять такие меры законодательного и иного характера, которые могут понадобиться для того, чтобы установить в своем внутреннем законодательстве в качестве уголовно наказуемого деяния противоправный умышленный доступ к компьютерной системе в целом или любой ее части. Любая из Сторон может потребовать, чтобы деяние считалось преступлением, если оно совершено с нарушением мер безопасности, с намерением получения компьютерных данных или с любым другим нечестным умыслом, или же в отношении компьютерной системы, которая связана с другой компьютерной системой.

#### **СТАТЬЯ 3.** НЕЗАКОННЫЙ ПЕРЕХВАТ

Каждая из Сторон должна принять такие меры законодательного и иного характера, которые могут понадобиться для того, чтобы установить в своем внутреннем законодательстве в качестве уголовно наказуемого деяния осуществляемый техническими средствами противоправный умышленный перехват не предназначенных для общественности передач компьютерных данных на компьютерную систему, с нее либо в ее пределах, включая исходящие от компьютерной системы электромагнитные излучения, несущие в себе подобные компьютерные данные. Любая из Сторон может потребовать, чтобы деяние считалось преступлением, если оно совершено с нечестным намерением, или в отно-

шении компьютерной системы, которая связана с другой компьютерной системой.

### **СТАТЬЯ 4.** ВМЕШАТЕЛЬСТВО В ДАННЫЕ

1. Каждая из Сторон должна принять такие меры законодательного и иного характера, которые могут понадобиться для того, чтобы установить в своем внутреннем законодательстве в качестве уголовно наказуемого деяния противоправное умышленное повреждение, стирание, порчу, изменение или подавление компьютерных данных.

2. Любая из Сторон может сохранить за собой право требовать, чтобы описанное в пункте 1 поведение считалось преступлением только в том случае, если в его результате был нанесен серьезный ущерб.

### **СТАТЬЯ 5.** ВМЕШАТЕЛЬСТВО В СИСТЕМУ

Каждая из Сторон должна принять такие меры законодательного и иного характера, которые могут понадобиться для того, чтобы установить в своем внутреннем законодательстве в качестве уголовно наказуемого деяния противоправное умышленное создание серьезных препятствий функционированию компьютерной системы путем ввода, передачи, повреждения, удаления, порчи, изменения или подавления компьютерных данных.

### **СТАТЬЯ 6.** НЕНАДЛЕЖАЩЕЕ ИСПОЛЬЗОВАНИЕ УСТРОЙСТВ

1. Каждая из Сторон должна принять такие меры законодательного и иного характера, которые могут понадобиться для того, чтобы установить в своем внутреннем законодательстве в качестве уголовно наказуемого деяния противоправное умышленное:

(a) производство, продажу, приобретение с целью использования, импорт, распространение или предоставление каким-либо иным образом:

(i) устройства, в том числе компьютерной программы, разработанного или приспособленного прежде всего для совершения любого из преступлений, предусмотренных статьями 2—5;

(ii) компьютерного пароля, кода доступа или аналогичных данных, с помощью которых можно осуществить доступ к компьютерной системе в целом или отдельной ее части с намерением использования ее в целях совершения любого из преступлений, предусмотренных статьями 2—5; и

(b) обладание одним из предметов, указанных выше в пунктах (a)(i) или (ii), с намерением использовать его в целях совершения любого из преступлений, предусмотренных статьями 2—5. Любая из Сторон может установить в законе, что уголовная ответственность наступает при условии обладания определенным количеством такого рода предметов.

2. Данная статья не может толковаться в смысле наложения уголовной ответственности в случаях, когда производство, продажа, приобретение с целью использования, импорт, распределение или предоставление каким-либо иным образом предмета, упомянутого в пункте 1 данной статьи, либо владение таким предметом имеет место не с целью совершения преступления, предусмотренного статьями 2—5 данной Конвенции, а осуществляется, например, для санкционированного тестирования или защиты компьютерной системы.

3. Каждая из Сторон может сохранить за собой право не применять пункт 1 данной статьи при условии, что действие этой оговорки не будет распространяться на продажу, распространение или предоставление каким-либо иным образом предметов, упомянутых в пункте 1(a)(ii) данной статьи.

### Часть 2. Преступления, связанные с компьютерами

#### **СТАТЬЯ 7.** ПОДЛОГ КОМПЬЮТЕРНЫХ ДАННЫХ

Каждая из Сторон должна принять такие меры законодательного и иного характера, которые могут понадобиться для того, чтобы установить в своем внутреннем законодательстве в качестве уголовно наказуемого деяния противоправное умышленное введение, изменение, стирание или подавление компьютерных данных, имеющее результатом недостоверные данные, с намерением, чтобы такие данные считались подлинными

или над ними совершались действия, как если бы они были подлинными, вне зависимости от того, действительно ли эти данные являются удобочитаемыми и разборчивыми. Для наступления уголовной ответственности любая из Сторон может потребовать наличия намерения ввести в заблуждение или схожего нечестного умысла.

### **СТАТЬЯ 8.** КОМПЬЮТЕРНОЕ МОШЕННИЧЕСТВО

Каждая из Сторон должна принять такие меры законодательного и иного характера, которые могут понадобиться для того, чтобы установить в своем внутреннем законодательстве в качестве уголовно наказуемого деяния противоправное умышленное причинение материального ущерба другому лицу путем:

(a) любого ввода, изменения, стирания или подавления компьютерных данных;

(b) любого вмешательства в функционирование компьютерной системы с обманным или нечестным намерением противоправного получения экономической выгоды для себя самого или для другого лица.

## Часть 3. Правонарушения, связанные с содержанием

### **СТАТЬЯ 9.** ПРЕСТУПЛЕНИЯ, СВЯЗАННЫЕ С ДЕТСКОЙ ПОРНОГРАФИЕЙ

1. Каждая из Сторон должна принять такие меры законодательного и иного характера, которые могут понадобиться для того, чтобы установить в своем внутреннем законодательстве в качестве уголовно наказуемого деяния противоправное умышленное поведение следующего характера:

(a) изготовление материалов, связанных с детской порнографией, с целью распространения их через компьютерную систему;

(b) предложение или предоставление материалов, связанных с детской порнографией, через компьютерную систему;

(c) распространение или передача материалов, связанных с детской порнографией, через компьютерную систему;

(d) получение материалов, связанных с детской порнографией, через компьютерную систему для самого себя или для другого лица;

(e) обладание материалами, связанными с детской порнографией, в компьютерной системе или на носителе компьютерных данных.

2. В целях вышеприведенного пункта 1 под «материалами, связанными с детской порнографией» понимаются любые материалы порнографического характера, которые наглядно показывают:

(a) несовершеннолетнего, принимающего участие в сексуально откровенном действии;

(b) лицо, выступающее в роли несовершеннолетнего, принимающее участие в сексуально откровенном действии;

(c) реалистические изображения, представляющие несовершеннолетнего, принимающего участие в сексуально откровенном действии.

3. В целях вышеприведенного пункта 2 под «несовершеннолетними» понимаются все люди моложе 18 лет. В то же время любая из Сторон может снизить возрастной предел до 16 лет.

4. Каждая из Сторон может сохранить за собой право не применять, полностью или частично, пункты 1(d), 1(e), 2(b) и 2(c).

### Часть 4. Преступления, связанные с нарушениями авторского права и смежных прав

#### **СТАТЬЯ 10.** НАРУШЕНИЯ, СВЯЗАННЫЕ С НАРУШЕНИЯМИ АВТОРСКОГО ПРАВА И СМЕЖНЫХ ПРАВ

1. Каждая из Сторон должна принять такие меры законодательного и иного характера, которые могут понадобиться для того, чтобы установить в своем внутреннем законодательстве в качестве уголовно наказуемого деяния нарушение авторского права, как оно определяется законом данной Стороны в соответствии с обязательствами, которые она приняла на себя согласно Парижскому акту от 24 июля 1971 г. о внесении изменений в Бернскую конвенцию об охране литературных

и художественных произведений, Соглашению по торговым аспектам прав на интеллектуальную собственность, и Соглашению по авторским правам ВОИС (Всемирной организации интеллектуальной собственности), за исключением любых моральных прав, присвоенных в соответствии с такими конвенциями, когда такого рода действия совершаются преднамеренно, в коммерческом масштабе и посредством компьютерной системы.

2. Каждая из Сторон должна принять такие меры законодательного и иного характера, которые могут понадобиться для того, чтобы установить в своем внутреннем законодательстве в качестве уголовно наказуемого деяния нарушение смежных прав, как оно определяется законом данной Стороны в соответствии с обязательствами, которые она приняла на себя согласно Международной конвенции об охране прав исполнителей, изготовителей фонограмм и вещательных организаций (Римской конвенции), Соглашению по торговым аспектам прав на интеллектуальную собственность, а также Договору ВОИС по исполнениям и фонограммам, за исключением любых моральных прав, присвоенных в соответствии с такими конвенциями, когда такого рода действия совершаются преднамеренно, в коммерческом масштабе и посредством компьютерной системы.

3. Любая из Сторон может сохранить за собой право не налагать в определенных обстоятельствах уголовную ответственность по пунктам 1 и 2 данной статьи при условии, что доступны другие эффективные средства правовой защиты и что данное право не снижает международных обязательств Стороны, сформулированных в международных документах, упомянутых в пунктах 1 и 2 данной статьи.

### Часть 5. Дополнительная ответственность и санкции

#### **СТАТЬЯ 11.** ПОКУШЕНИЕ, ПОСОБНИЧЕСТВО И ПОДСТРЕКАТЕЛЬСТВО

1. Каждая из Сторон должна принять такие меры законодательного и иного характера, которые могут понадобиться для того, чтобы установить в своем внутрен-

нем законодательстве в качестве уголовно наказуемого деяния умышленное пособничество или подстрекательство к совершению любого из преступлений, предусмотренного статьями 2—10 данной Конвенции, и имеющее умыслом, чтобы подобное преступление было совершено.

2. Каждая из Сторон должна принять такие меры законодательного и иного характера, которые могут понадобиться для того, чтобы установить в своем внутреннем законодательстве в качестве уголовно наказуемого деяния умышленное покушение на совершение любого из преступлений, предусмотренного статьями 3—5, 7, 8, 9 (1)(a) и 9 (1)(c) данной Конвенции.

3. Каждая из Сторон может сохранить за собой право не применять, полностью или частично, пункт 2 данной статьи.

### **СТАТЬЯ 12.** КОЛЛЕКТИВНАЯ ОТВЕТСТВЕННОСТЬ

1. Каждая из Сторон должна принять такие меры законодательного и иного характера, которые могут понадобиться для того, чтобы гарантировать, что юридическое лицо будет нести ответственность за уголовное преступление, установленное в соответствии с данной Конвенцией, которое совершено для его выгоды любым физическим лицом, действующим либо индивидуально, либо как часть органа юридического лица, и которое занимает руководящее положение в рамках юридического лица, и такое положение основано на:

(a) полномочиях представлять это юридическое лицо;

(b) праве принимать решения от имени этого юридического лица;

(c) праве осуществлять контроль в рамках юридического лица.

2. Кроме случаев, уже предусмотренных в пункте 1, каждая из Сторон должна принять меры по обеспечению того, что юридическое лицо будет нести ответственность в тех случаях, когда отсутствие надлежащего надзора или контроля со стороны физического лица, упомянутого в пункте 1, сделало возможным совершение уголовного преступления, установленного в соот-

ветствии с данной Конвенцией, физическим лицом для выгоды данного юридического лица, действовавшим по его полномочиям.

3. В соответствии с юридическими принципами Стороны ответственность юридического лица может быть уголовной, гражданской или административной.

4. Такая ответственность наступает без какого-либо ущерба для уголовной ответственности физических лиц, которые совершили преступление.

#### **СТАТЬЯ 13.** САНКЦИИ И МЕРЫ

1. Каждая из Сторон должна принять такие меры законодательного и иного характера, которые могут понадобиться для того, чтобы гарантировать, что уголовные преступления, предусмотренные статьями 2—11, будут наказываться действенными, соразмерными и убедительными санкциями, включающими в себя лишение свободы.

2. Каждая из Сторон должна гарантировать, что на юридических лиц, несущих ответственность по статье 12, будут налагаться действенные, соразмерные и убедительные санкции или меры уголовного и неуголовного характера, в том числе денежные взыскания.

## Раздел 2. Процессуальные нормы

### Часть 1. Общие положения

#### **СТАТЬЯ 14.** СФЕРА ДЕЙСТВИЯ ПРОЦЕССУАЛЬНЫХ ПОЛОЖЕНИЙ

1. Каждая из Сторон должна принять такие меры законодательного и иного характера, которые могут понадобиться для установления полномочий и процедур, предусмотренных в данном разделе, в целях проведения определенных уголовных расследований или разбирательств.

2. Кроме случаев, особо оговоренных в статье 21, каждая из Сторон должна применять полномочия и процедуры, упомянутые в пункте 1:

(а) к уголовным преступлениям, предусмотренным статьями 2—11 данной Конвенции;

(b) к другим уголовным преступлениям, совершенным посредством компьютерной системы; а также

(c) к сбору доказательств по уголовному преступлению в электронной форме.

3.

(a) Каждая из Сторон может сохранить за собой право применять упомянутые в статье 20 меры только против преступлений или категорий преступлений, указанных в оговорках, при условии, что диапазон таких преступлений или категорий преступлений ограничен не более, чем диапазон нарушений, к которым применяются меры, упомянутые в статье 21. Каждая из Сторон должна рассмотреть вопрос об ограничении подобного рода права резервирования, чтобы содействовать самому широкому применению мер, упомянутых в статьях 20 и 21.

(b) В случае, если Сторона из-за ограничений в ее действующем законодательстве на время принятия данной Конвенции не в состоянии применить меры, упомянутые в статьях 20 и 21, к операциям по передаче данных в пределах компьютерной системы поставщика услуг и эта система

(i) функционирует для выгоды ограниченной группы пользователей,

(ii) не использует коммуникационные системы общего пользования и не связана с другой компьютерной системой, будь то государственная или частная,

то Сторона может сохранить за собой право не применять указанные меры к таким операциям по передаче данных. Каждая из Сторон должна рассмотреть вопрос об ограничении подобного рода права резервирования, чтобы содействовать самому широкому применению мер, упомянутых в статьях 20 и 21.

### **СТАТЬЯ 15.** УСЛОВИЯ И ГАРАНТИИ

1. Каждая из Сторон должна гарантировать, что учреждение, реализация и применение предусмотренных в настоящем Разделе полномочий и процедур будут ограничены условиями и гарантиями, предусмотренными в ее внутреннем законодательстве, которые должны обеспечить надлежащую защиту гражданских прав

и свобод, включая права, вытекающие из обязательств, принятых на себя данной стороной по Конвенции Совета Европы о защите прав человека и основных свобод 1950 г., Международному пакту ООН о гражданских и политических правах 1966 г. и по другим применимым в данном случае международным документам о правах человека, и которые должны основываться на принципе соразмерности.

2. В зависимости от характера полномочий или процедур, о которых идет речь, такие условия и гарантии должны включать в себя, среди прочего, надзор со стороны судебных или иных независимых органов; основания, оправдывающие их применение; а также ограничения на сферу и срок действия подобных полномочий или процедур.

3. В той мере, в какой это совместимо с общественными интересами, в особенности в отношении разумного отправления правосудия, каждая из Сторон должна рассмотреть воздействие изложенных в данном разделе полномочий и процедур на права, обязанности и законные интересы третьих лиц.

### Часть 2. Незамедлительное сохранение компьютерных данных

#### **СТАТЬЯ 16.** НЕЗАМЕДЛИТЕЛЬНОЕ СОХРАНЕНИЕ КОМПЬЮТЕРНЫХ ДАННЫХ

1. Каждая из Сторон должна принять такие меры законодательного и иного характера, которые могут понадобиться для того, чтобы предоставить ее компетентным органам возможность предписывать или сходным образом добиваться незамедлительного сохранения определенных компьютерных данных, включая данные трафика, которые хранятся посредством компьютерной системы, особенно в тех случаях, когда есть основания полагать, что существует опасность потери или изменения этих компьютерных данных.

2. В случаях, когда Сторона приводит в действие вышеприведенный пункт 1 посредством предписания лицу сохранить определенные компьютерные данные, находящиеся во владении или под контролем этого ли-

ца, Сторона должна принять такие меры законодательного и иного характера, которые могут понадобиться для того, чтобы обязать это лицо сохранять и поддерживать целостность подобных компьютерных данных в течение необходимого периода времени, который не может превышать 90 дней, чтобы позволить компетентным органам провести расследование по данному факту. Сторона может предусмотреть положение о возможности продления срока действия предписания.

3. Каждая из Сторон должна принять такие меры законодательного и иного характера, которые могут понадобиться для того, чтобы обязать хранителя данных или иное лицо, обязанное сохранять компьютерные данные, держать в тайне факт совершения таких процедур в течение промежутка времени, предусмотренного во внутреннем законодательстве.

4. Полномочия и процедуры, о которых идет речь в данной статье, подлежат действию положений, содержащихся в статьях 14 и 15.

### **СТАТЬЯ 17.** НЕЗАМЕДЛИТЕЛЬНОЕ СОХРАНЕНИЕ И ЧАСТИЧНОЕ ПРЕДОСТАВЛЕНИЕ ДАННЫХ ТРАФИКА

1. В отношении данных трафика, подлежащих сохранению согласно статье 16, каждая из Сторон должна принять такие меры законодательного и иного характера, которые могут понадобиться для того, чтобы:

(a) гарантировать, что подобное незамедлительное сохранение данных трафика будет возможно вне зависимости от того, сколько поставщиков услуг были вовлечены в операцию по передаче данной информации — один или несколько; а также

(b) гарантировать быстрое предоставление компетентным органам Стороны или лицу, назначенному таким компетентным органом, данных трафика в объеме, достаточном для того, чтобы Сторона могла идентифицировать поставщиков услуг и маршрут, по которому производилась передача информации.

3. Полномочия и процедуры, о которых идет речь в данной статье, подлежат действию положений, содержащихся в статьях 14 и 15.

## Часть 3. Предписание о предоставлении информации

### **СТАТЬЯ 18.** ПРЕДПИСАНИЕ О ПРЕДОСТАВЛЕНИИ ИНФОРМАЦИИ

1. Каждая из Сторон должна принять такие меры законодательного и иного характера, которые могут понадобиться для того, чтобы предоставить ее компетентным властям полномочия предписывать:

(a) лицу, находящемуся на ее территории, предоставить определенные компьютерные данные, находящиеся во владении или под контролем этого лица, которые хранятся в компьютерной системе или на носителе компьютерных данных; а также

(b) поставщику услуг, предлагающему свои услуги на территории Стороны, предоставить ту информацию о подписчиках, связанную с такими услугами, которая находится во владении или под контролем поставщика услуг.

2. Полномочия и процедуры, о которых идет речь в данной статье, подлежат действию положений, содержащихся в статьях 14 и 15.

3. В целях настоящей статьи «информация о подписчике» означает любую информацию в форме компьютерных данных или в любой иной форме, которой обладает поставщик услуг относительно подписчика его услуг, и отличную от данных трафика или данных содержания, с помощью которой можно установить:

(a) тип использованной коммуникационной услуги, примененные для этого технические средства и срок предоставления услуги;

(b) личность подписчика, его почтовый или географический адрес, номер телефона или иного средства доступа, информацию о выставлении счетов и их оплате, доступную на основании соглашения или договора об обслуживании;

(c) любую иную информацию о месте установки коммуникационного оборудования, доступную на основании соглашения или по договору об обслуживании.

### **СТАТЬЯ 19.** ПОИСК И ИЗЪЯТИЕ КОМПЬЮТЕРНЫХ ДАННЫХ

1. Каждая из Сторон должна принять такие меры законодательного и иного характера, которые могут понадобиться для того, чтобы позволить ее компетентным органам путем произведения обыска или сходным образом получать доступ на ее территории:

(a) к компьютерной системе в целом или отдельной ее части, а также к хранящимся там компьютерным данным; и

(b) к носителю компьютерных данных, на котором могут храниться компьютерные данные.

2. Каждая из Сторон должна принять такие меры законодательного и иного характера, которые могут понадобиться для того, чтобы гарантировать, что в случаях, когда ее органы производят обыск или сходным образом получают доступ к определенной компьютерной системе или отдельной ее части в соответствии с пунктом 1(a), а также имеют основания полагать, что искомые данные хранятся в другой компьютерной системе или какой-либо ее части на территории Стороны и такие данные законным образом доступны из изначальной системы или же доступны ей, то такие органы должны быть в состоянии быстро распространить сферу обыска на другую систему или сходным образом получить доступ к такой системе.

3. Каждая из Сторон должна принять такие меры законодательного и иного характера, которые могут понадобиться для того, чтобы позволить ее компетентным органам конфисковывать или равным образом изымать компьютерные данные, доступ к которым получен на основании пунктов 1, 2. Эти меры должны включать в себя полномочия:

(a) по конфискации или, равным образом, изъятию компьютерной системы, или ее части, или же носителя компьютерных данных;

(b) по изготовлению и сохранению копии таких компьютерных данных;

(c) по поддержанию целостности соответствующих сохраненных компьютерных данных; а также

(d) по прекращению доступа к этим компьютерным данным в компьютерной системе, к которой получен доступ, или удалению их из этой системы.

4. Каждая из Сторон должна принять такие меры законодательного и иного характера, которые могут понадобиться для того, чтобы позволить ее компетентным органам предписывать любому лицу, которое обладает сведениями о функционировании компьютерной системы или применяемых в ней мерах по защите компьютерных данных, предоставить, насколько это целесообразно, информацию, необходимую в целях обеспечения принятия мер, указанных в пунктах 1 и 2.

5. Полномочия и процедуры, о которых идет речь в данной статье, подлежат действию положений, содержащихся в статьях 14 и 15.

### Часть 5. Сбор компьютерных данных в режиме реального времени

#### **СТАТЬЯ 20.** СБОР ДАННЫХ ТРАФИКА В РЕЖИМЕ РЕАЛЬНОГО ВРЕМЕНИ

1. Каждая из Сторон должна принять такие меры законодательного и иного характера, которые могут понадобиться для того, чтобы позволить ее компетентным органам:

(a) собирать или записывать, путем применения технических средств на территории данной Стороны, а также

(b) принуждать поставщика услуг в пределах имеющихся у него технических возможностей:

(i) собирать или записывать путем применения технических средств на территории этой Стороны; или

(ii) сотрудничать с компетентными органами и помогать им собирать или записывать в режиме реального времени данные трафика, связанные с определенными операциями по передаче данных на ее территории, осуществляемыми посредством компьютерной системы.

2. В случае, если Сторона из-за установленных в ее национальном законодательстве принципов не в состоянии принять меры, указанные в пункте 1(a), она мо-

жет вместо этого принять такие меры законодательного и иного характера, которые могут понадобиться для того, чтобы обеспечить сбор или запись в режиме реального времени данных трафика, связанных с определенными операциями по передаче данных на ее территории, осуществляемыми посредством компьютерной системы.

3. Каждая из Сторон должна принять такие меры законодательного и иного характера, которые могут понадобиться для того, чтобы обязать поставщика услуг хранить в тайне факт исполнения любого из полномочий, предусмотренных в данной статье, а также любую связанную с этим информацию.

4. Полномочия и процедуры, о которых идет речь в данной статье, подлежат действию положений, содержащихся в статьях 14 и 15.

### **СТАТЬЯ 21.** ПЕРЕХВАТ ДАННЫХ СОДЕРЖАНИЯ

1. Каждая из Сторон должна принять такие необходимые меры законодательного и иного характера в отношении ряда серьезных преступлений, определенных в соответствии с ее национальным законодательством, которые позволили бы ее компетентным органам:

(a) собирать или записывать путем применения технических средств на территории этой Стороны, и

(b) принуждать поставщика услуг в пределах имеющихся у него технических возможностей:

(i) собирать или записывать путем применения технических средств на территории этой Стороны, или

(ii) сотрудничать с компетентными органами и помогать им собирать или записывать в режиме реального времени данные содержания определенных передач информации на ее территории, осуществляемых посредством компьютерной системы.

2. В случае, если Сторона из-за установленных в ее национальном законодательстве принципов не в состоянии принять меры, указанные в пункте 1(a), она может вместо этого принять такие меры законодательного и иного характера, которые могут понадобиться для того, чтобы обеспечить сбор или запись в режиме реального времени данных содержания определенных пе-

редач информации путем применения технических средств на данной территории.

3. Каждая из Сторон должна принять такие меры законодательного и иного характера, которые могут понадобиться для того, чтобы обязать поставщика услуг хранить в тайне факт исполнения любого из полномочий, предусмотренных в данной статье, а также любую связанную с этим информацию.

4. Полномочия и процедуры, о которых идет речь в данной статье, подлежат действию положений, содержащихся в статьях 14 и 15.

## Раздел 3. Юрисдикция

### СТАТЬЯ 22. ЮРИСДИКЦИЯ

1. Каждая из Сторон должна принять такие меры законодательного и иного характера, которые могут понадобиться для того, чтобы установить юрисдикцию по любому из преступлений, предусмотренных статьями 2—11 настоящей Конвенции, если оно совершено:

(a) на ее территории; или

(b) на борту судна под флагом данной Стороны; или

(c) на борту воздушного судна, зарегистрированного согласно законам данной Стороны; или

(d) одним из подданных данной Стороны, если правонарушение подпадает под действие уголовного законодательства на территории, где оно было совершено, или же если правонарушение совершено вне территориальной юрисдикции любого Государства.

2. Каждая из Сторон может сохранить за собой право не применять вовсе либо применять только в определенных случаях или при определенных обстоятельствах правила юрисдикции, установленные в пунктах (1)(b)—(1)(d) данной статьи или в любой их части.

3. Каждая из Сторон должна принять такие меры законодательного и иного характера, которые могут понадобиться для того, чтобы установить юрисдикцию в отношении правонарушений, указанных в пункте 1 статьи 24 настоящей Конвенции, в случаях, когда предполагаемый правонарушитель находится на ее террито-

рии, и после получения просьбы о его выдаче она не выдает его другой Стороне исключительно на основании его национальности.

4. Настоящая Конвенция не исключает какой-либо иной уголовной юрисдикции, осуществляемой в соответствии с национальным законодательством.

5. В случае, если сразу несколько Сторон предъявляют права на юрисдикцию по предполагаемому нарушению, установленному в соответствии с настоящей Конвенцией, вовлеченные Стороны должны, если это целесообразно, провести консультации с целью определения юрисдикции, наиболее подходящей для судебного преследования.

## Глава III. Международное сотрудничество

## Раздел 1. Общие принципы

### Часть 1. Общие принципы международного сотрудничества

#### **СТАТЬЯ 23.** ОБЩИЕ ПРИНЦИПЫ МЕЖДУНАРОДНОГО СОТРУДНИЧЕСТВА

В целях расследования или судебного преследования уголовных преступлений, связанных с компьютерными системами и данными, а также в целях сбора доказательств по уголовным преступлениям в электронной форме Стороны должны осуществлять самое широкое сотрудничество друг с другом в соответствии с положениями настоящей главы и через применение соответствующих международных документов о международном сотрудничестве в деле борьбы с преступностью, договоренностей, достигнутых на основе единообразного или взаимообязывающего законодательства, а также национальных законов.

### Часть 2. Принципы экстрадиции

#### **СТАТЬЯ 24.** ЭКСТРАДИЦИЯ

1.

(a) Данная статья применяется между Сторонами по вопросу об экстрадиции за уголовные преступления, предусмотренные статьями 2—11 настоящей Конвен-

ции, при условии, что такие преступления наказываются согласно законам обеих Сторон лишением свободы на максимальный срок не менее одного года или же наложением более серьезного взыскания.

(b) В случаях, если по соглашению, основывающемуся на единообразном или взаимообязывающем законодательстве или же на договоре об экстрадиции, применимом между двумя или более сторонами, включая Европейскую Конвенцию об экстрадиции (ETS № 24), предусматриваются различные нижние пределы наказания, должно применяться минимальное наказание, предусмотренное таким договором или соглашением.

2. Уголовные преступления, описанные в пункте 1 данной статьи, должны считаться преступлениями, влекущими за собой экстрадицию, во всех существующих между Сторонами соглашениях об экстрадиции. Стороны обязаны включать такие преступления в список преступлений, влекущих за собой экстрадицию, во все соглашения об экстрадиции, которые будут заключаться между Сторонами.

3. Если Сторона, обуславливающая экстрадицию наличием соответствующего соглашения, получает просьбу об экстрадиции от другой Стороны, с которой у нее нет соглашения об экстрадиции, то она может рассматривать настоящую Конвенцию в качестве юридического основания для экстрадиции в отношении любого уголовного преступления, указанного в пункте 1 данной статьи.

4. Стороны, которые не обуславливают экстрадицию наличием соответствующего соглашения, в отношениях между собой должны считать уголовные преступления, указанные в пункте 1 данной статьи, преступлениями, которые подлежат экстрадиции.

5. Экстрадиция подчиняется условиям, предусмотренным законами запрашиваемой Стороны или применимыми договорами об экстрадиции, в том числе основаниям, по которым запрашиваемая Сторона может отказаться от экстрадиции.

6. Если отказ в экстрадиции за уголовное преступление, указанное в пункте 1 данной статьи, производится исключительно на основании национальности

подозреваемого лица или же если запрашиваемая Сторона считает, что она обладает юрисдикцией по данному преступлению, то запрашиваемая Сторона по просьбе запрашивающей Стороны должна передать дело с целью судебного преследования своим компетентным органам и обязана уведомить в должной форме запрашивающую Сторону о результатах такого преследования. Указанные органы при принятии своих решений и проведении расследования и разбирательства должны действовать таким же образом, как и в случае любых других преступлений схожего типа согласно законодательству этой Стороны.

7.

(a) Во время подписания или при депонировании своей ратификационной грамоты или документа о принятии, утверждении или присоединении каждая из Сторон обязана предоставить Генеральному секретарю Совета Европы сведения о наименовании и адресе каждого органа, отвечающего за выдачу или принятие просьб об экстрадиции или предварительный арест при отсутствии соответствующего соглашения.

(b) Генеральный секретарь Совета Европы обязан создать и обновлять реестр назначенных Сторонами компетентных органов. Каждая из Сторон обеспечивает постоянное наличие в реестре корректной информации.

### Часть 3. Общие принципы взаимной помощи

#### **СТАТЬЯ 25.** ОБЩИЕ ПРИНЦИПЫ ВЗАИМНОЙ ПОМОЩИ

1. Стороны должны в самой широкой степени оказывать друг другу взаимную помощь в расследовании или судебном преследовании уголовных преступлений, связанных с компьютерными системами и данными, а также в сборе доказательств по уголовным преступлениям в электронной форме.

2. Каждая из Сторон должна также принять такие меры законодательного и иного характера, которые могут понадобиться для выполнения обязательств, изложенных в статьях 27—35.

3. Каждая из Сторон под влиянием экстренных обстоятельств может просить о содействии или предоставлении информации в рамках такого содействия средствами срочной связи, в том числе по факсу или электронной почте, в той мере, в какой такие средства обеспечивают соответствующий уровень безопасности и идентификации (включая использование шифрования, где это необходимо), с последующим формальным подтверждением по требованию запрашиваемой Стороны. Запрашиваемая Сторона должна принять запрос и ответить на него с помощью любых подобных средств срочной связи.

4. Если иное не предусмотрено особо в статьях настоящей главы, взаимная помощь подчиняется условиям, предусмотренным законами запрашиваемой Стороны или применимыми договорами о взаимной помощи, в том числе основаниям, по которым запрашиваемая Сторона может отказаться от сотрудничества. Запрашиваемая Сторона не должна осуществлять свое право на отказ от содействия в отношении преступлений, указанных в статьях 2—11, исключительно на том основании, что запрос касается преступления, которое она считает нарушением налогового законодательства.

5. В случае, если в соответствии с положениями настоящей главы запрашиваемая Сторона вправе обусловить оказание содействия наличием обоюдного признания соответствующего деяния преступлением, это условие считается выполненным вне зависимости от того, включает ли ее законодательство данное деяние в ту же самую категорию преступлений и использует ли оно ту же формулировку преступления, что и запрашивающая Сторона, если поведение, лежащее в основе деяния, в связи с которым испрашивается содействие, является по ее законодательству уголовным преступлением.

### **СТАТЬЯ 26.** ДОБРОВОЛЬНОЕ ПРЕДОСТАВЛЕНИЕ ИНФОРМАЦИИ

1. Любая из Сторон, действуя в рамках национального законодательства и без предварительного запроса, вправе направить другой Стороне информацию, полученную в ходе проводимого ей расследования, если

она считает, что предоставление данной информации будет способствовать возбуждению и проведению Стороной-получателем расследования или судебного преследования уголовных преступлений, установленных согласно настоящей Конвенции, или же приведет к направлению той Стороной запроса о содействии в соответствии с настоящей главой.

2. До предоставления такого рода информации направляющая Сторона вправе потребовать сохранения направляемой информации в тайне или использования ее согласно поставленным условиям. Если Сторона-получатель не в состоянии выполнить такие требования, она обязана уведомить об этом направляющую Сторону, которая вслед за этим принимает решение о необходимости предоставления информации. Принятие Стороной-получателем информации на поставленных условиях означает, что она обязана их выполнять.

### Часть 4. Принципы направления и выполнения запросов о содействии в случае отсутствия соответствующих международных соглашений

#### **СТАТЬЯ 27.** ПРИНЦИПЫ НАПРАВЛЕНИЯ И ВЫПОЛНЕНИЯ ЗАПРОСОВ О СОДЕЙСТВИИ В СЛУЧАЕ ОТСУТСТВИЯ СООТВЕТСТВУЮЩИХ МЕЖДУНАРОДНЫХ СОГЛАШЕНИЙ

1. В случае, если между запрашивающей и запрашиваемой Сторонами не заключено соглашений и договоров о взаимной помощи на основе единообразного или взаимообязывающего законодательства, применяются пункты 2—9 данной статьи. При наличии соответствующего соглашения, договора или законодательного акта настоящая статья не применяется, за исключением случаев, когда обе Стороны согласятся на то, чтобы вместо упомянутых правовых документов применялись отдельные или все последующие пункты данной статьи.

2.

(а) Каждая из Сторон обязана назначить центральный орган или органы, ответственные за отправку запросов о содействии и ответы на поступившие запросы,

выполнение подобных запросов или передачу их на выполнение в соответствующие органы.

(b) Центральные органы обязаны поддерживать между собой прямую связь.

(c) Во время подписания или депонирования своей ратификационной грамоты или документа о принятии, утверждении или присоединении каждая из Сторон обязана предоставить Генеральному секретарю Совета Европы сведения о наименованиях и адресах органов, назначенных в соответствии с данным пунктом.

(d) Генеральный секретарь Совета Европы обязан создать и обновлять реестр данных по центральным органам, назначенным Сторонами. Каждая из Сторон обеспечивает постоянное наличие в реестре корректной информации.

3. Запросы о содействии, направленные в соответствии с данной статьей, подлежат исполнению согласно указаниям запрашивающей Стороны, за исключением случаев, когда это противоречит законодательству запрашиваемой Стороны.

4. Помимо оснований для отказа, указанных в пункте 4 статьи 25, запрашиваемая Сторона имеет право отказать в содействии по следующим причинам:

(a) запрос сделан по поводу правонарушения, которое, по мнению запрашиваемой Стороны, является политическим или связано с такого рода правонарушением;

(b) запрашиваемая Сторона считает, что выполнение запроса может нанести ущерб ее суверенитету, безопасности, общественному порядку или другим существенным интересам.

5. Запрашиваемая Сторона вправе отложить выполнение запроса, если оно способно нанести ущерб уголовному расследованию или разбирательству, проводимому властями запрашиваемой Стороны.

6. До вынесения решения об отказе в содействии или откладывании выполнения запроса запрашиваемая Сторона должна после проведения консультаций с запрашивающей Стороной, если это целесообразно, рассмотреть возможность частичного удовлетворения запроса или удовлетворения его на условиях, которые она сочтет необходимыми.

7. Запрашиваемая Сторона обязана своевременно доводить до сведения запрашивающей Стороны результаты выполнения запроса о содействии. В случае вынесения отказа в содействии или откладывания выполнения запроса запрашиваемая Сторона должна уведомить запрашивающую Сторону о причинах вынесения подобного решения, а также указать причины, делающие невозможным выполнение запроса или значительно влияющие на сроки его выполнения.

8. Запрашивающая Сторона вправе потребовать от запрашиваемой Стороны сохранения в тайне как самого факта направления запроса, так и содержания запроса, направленного в соответствии с данной главой, в той степени, насколько при этом возможно выполнение запроса. Если запрашиваемая Сторона не может выполнить требование о неразглашении, она обязана незамедлительно уведомить об этом запрашивающую Сторону, после чего запрашивающая Сторона выносит решение о том, настаивает ли она на выполнении запроса на таких условиях.

9.

(a) В экстренных случаях запросы о содействии или предоставлении информации в рамках такого содействия могут направляться судебными органами запрашивающей Стороны непосредственно в адрес соответствующих органов запрашиваемой Стороны. В таком случае копия запроса должна быть одновременно направлена в центральные органы запрашиваемой Стороны через центральные органы запрашивающей Стороны.

(b) Любой запрос о содействии или предоставлении информации в рамках такого содействия, подаваемый в соответствии с данным пунктом, может быть направлен через Международную организацию уголовной полиции (Интерпол).

(c) В случае, если запрос направлен в соответствии с подпунктом (a) данной статьи и получен органом, не компетентным заниматься его рассмотрением, этот орган обязан передать запрос компетентному органу запрашиваемой Стороны и уведомить об этом запрашивающую Сторону.

(d) Запросы о содействии или предоставлении информации в рамках такого содействия, направленные в соответствии с данным пунктом и не предполагающие принудительных действий, могут быть направлены непосредственно компетентными органами запрашивающей Стороны в компетентные органы запрашиваемой Стороны.

(e) Во время подписания или депонирования своей ратификационной грамоты или документа о принятии, утверждении или присоединении каждая из Сторон может проинформировать Генерального секретаря Совета Европы о том, что в целях обеспечения эффективности запросы в соответствии с данным пунктом следует направлять в центральные органы данной Стороны.

### **СТАТЬЯ 28.** ПРИНЦИПЫ КОНФИДЕНЦИАЛЬНОСТИ И ОГРАНИЧЕННОГО ИСПОЛЬЗОВАНИЯ

1. В случае, если между запрашивающей и запрашиваемой Сторонами не заключено соглашений и договоров о взаимной помощи на основе единообразного или взаимообязывающего законодательства, применяются положения данной статьи. При наличии соответствующего соглашения, договора или законодательного акта настоящая статья не применяется, за исключением случаев, когда обе Стороны согласятся на то, чтобы вместо упомянутых правовых документов применялись отдельные или все последующие пункты данной статьи.

2. В ответ на направленный запрос запрашиваемая Сторона вправе обусловить предоставление информации и прочих материалов тем, что:

(a) информация будет сохраняться в тайне, если при отсутствии такого условия выполнение запроса не представляется возможным;

(b) информация будет использована исключительно для проведения расследования или разбирательства тех дел, которые указаны в запросе.

3. Если запрашивающая Сторона не может выполнить условие, указанное в пункте 2, она обязана незамедлительно уведомить об этом запрашиваемую Сторону, после чего запрашиваемая Сторона принимает решение о предоставлении информации. Принятие за-

прашивающей Стороной поставленных условий означает, что она обязана их выполнять.

4. Любая из Сторон, предоставляющих информацию и прочие материалы на условиях, указанных в пункте 2, вправе потребовать от другой Стороны объяснить, в связи с этими условиями, как будет использована предоставляемая информация и прочие материалы.

## Раздел 2. Особые положения

### Часть 1. Принципы содействия при принятии временных мер

#### **СТАТЬЯ 29.** НЕЗАМЕДЛИТЕЛЬНОЕ СОХРАНЕНИЕ КОМПЬЮТЕРНЫХ ДАННЫХ

1. Любая из Сторон вправе запросить другую Сторону предписать или иным способом добиться незамедлительного сохранения данных, хранящихся в компьютерной системе, расположенной на территории данной Стороны, и в отношении которых запрашивающая Сторона намеревается направить запрос о содействии с целью поиска данных или получения доступа к ним, их изъятия или обеспечения сохранности, а также предоставления этих данных.

2. В запросе на сохранение данных, направленном согласно пункту 1, должны быть указаны следующие сведения:

(a) наименование органа, обращающегося с запросом о сохранении данных;

(b) правонарушение, лежащее в основе уголовного расследования или разбирательства, с краткой характеристикой фактов по делу;

(c) компьютерные данные, которые подлежат сохранению, и их связь с правонарушением;

(d) любая информация, способствующая идентификации хранителя компьютерных данных и определению местонахождения компьютерной системы;

(e) необходимость в сохранении;

(f) намерение Стороны направить запрос о содействии с целью поиска данных или получения доступа

к ним, их изъятия или обеспечения сохранности либо предоставления этих данных.

3. По получении запроса от другой Стороны запрашиваемая Сторона обязана принять все надлежащие меры по незамедлительному сохранению указанных данных в соответствии со своим национальным законодательством. В целях обеспечения обработки запроса и выполнения процедуры сохранения данных обоюдное признание соответствующего деяния преступлением не является обязательным условием.

4. Относительно правонарушений, отличных от тех, которые перечислены в статьях 2—11 настоящей Конвенции, любая из Сторон, настаивающая на обоюдном признании соответствующего деяния преступлением в качестве обязательного условия для обработки запроса о содействии в поиске данных или получении доступа к ним, их изъятии или обеспечении сохранности либо предоставлении этих данных, вправе отказать в сохранении данных в соответствии с данной статьей в случае, если у нее имеются основания полагать, что на момент предоставления данных требование об обоюдном признании соответствующего деяния преступлением не может быть выполнено.

5. Кроме того, запрос о сохранении данных может быть отклонен, если:

(a) запрос сделан относительно правонарушения, которое, по мнению запрашиваемой Стороны, является политическим или связано с такого рода правонарушением;

(b) запрашиваемая Сторона считает, что выполнение запроса может нанести ущерб ее суверенитету, безопасности, общественному порядку или другим существенным интересам.

6. Если запрашиваемая Сторона считает, что процедура сохранения данных не обеспечит доступ к этим данным в будущем, поставит под угрозу или иным способом нанесет ущерб конфиденциальности расследования, проводимого запрашивающей Стороной, она обязана незамедлительно уведомить об этом запрашивающую Сторону, после чего запрашивающая Сторона принимает решение о необходимости исполнения запроса.

7. Срок сохранения данных, выполняемого на основании запроса, указанного в пункте 1, должен составлять не менее 60 дней, с тем чтобы дать запрашивающей Стороне возможность направить запрос о поиске данных или получении доступа к ним, их изъятии или обеспечении сохранности либо предоставлении этих данных. По получении запроса данные подлежат сохранению до вынесения решения по данному запросу.

### **СТАТЬЯ 30.** НЕЗАМЕДЛИТЕЛЬНОЕ ПРЕДОСТАВЛЕНИЕ СОХРАНЕННЫХ ДАННЫХ ТРАФИКА

1. В случае, если в ходе выполнения запроса о сохранении данных трафика в отношении определенной операции по передаче данных, направленного в соответствии со статьей 29, запрашиваемой Стороне станет известно, что в передаче данных был задействован поставщик услуг на территории другого государства, она обязана в срочном порядке предоставить запрашивающей Стороне данные трафика в объеме, достаточном для идентификации этого поставщика услуг и определения маршрута передачи данных.

2. В предоставлении данных трафика согласно пункту 1 может быть отказано только в том случае, если:

(a) запрос сделан по поводу правонарушения, которое, по мнению запрашиваемой Стороны, является политическим или связано с такого рода правонарушением;

(b) запрашиваемая Сторона считает, что выполнение запроса может нанести ущерб ее суверенитету, безопасности, общественному порядку или другим существенным интересам.

## Часть 2. Принципы содействия в отношении действий следственных служб

### **СТАТЬЯ 31.** ПРИНЦИПЫ СОДЕЙСТВИЯ В ОТНОШЕНИИ ДОСТУПА К КОМПЬЮТЕРНЫМ ДАННЫМ

1. Любая из Сторон имеет право направлять запросы другой Стороне с целью поиска или получения доступа к данным, хранящимся посредством компьютер-

ной системы на территории запрашиваемой Стороны, изъятия, обеспечения сохранности или предоставления таких данных, в том числе данных, сохраненных согласно статье 29.

2. Запрашиваемая Сторона обязана ответить на запрос путем применения международных правовых документов, соглашений и норм, указанных в статье 23, и в соответствии с другими соответствующими положениями данной главы.

3. Запрос подлежит незамедлительному ответу, если:

(a) имеются основания полагать, что существует серьезная опасность потери или изменения компьютерных данных, о которых идет речь;

(b) правовые документы, соглашения и нормы, указанные в пункте 2, так или иначе предполагают оказание незамедлительного содействия.

### **СТАТЬЯ 32.** ТРАНСГРАНИЧНЫЙ ДОСТУП К КОМПЬЮТЕРНЫМ ДАННЫМ, НАХОДЯЩИМСЯ В СИСТЕМАХ ОБЩЕГО ДОСТУПА, ЛИБО ПРИ ПОЛУЧЕНИИ СООТВЕТСТВУЮЩЕГО РАЗРЕШЕНИЯ

Любая из Сторон имеет право без согласия другой Стороны:

(a) получать доступ к компьютерным данным из открытых источников, находящихся в системах общего доступа, независимо от территориального местонахождения этих данных;

(b) посредством компьютерной системы на своей территории получать доступ к компьютерным данным, расположенным на территории другой Стороны, при получении правомерного и добровольного согласия со стороны лица, обладающего законным правом на предоставление данных этой Стороне посредством вышеупомянутой компьютерной системы.

### **СТАТЬЯ 33.** СОДЕЙСТВИЕ В СБОРЕ ДАННЫХ ТРАФИКА В РЕЖИМЕ РЕАЛЬНОГО ВРЕМЕНИ

1. Стороны обязаны содействовать друг другу в сборе в режиме реального времени данных трафика, связанных с определенными операциями по передаче дан-

ных, осуществляемыми на территории Сторон посредством компьютерной системы. С учетом положений пункта 2, такое содействие оказывается в порядке и на принципах, предусмотренных в национальном законодательстве.

2. Каждая из Сторон обязана оказывать такого рода содействие, по меньшей мере, применительно к тем уголовным преступлениям, когда сбор данных трафика в режиме реального времени был бы возможен в случае аналогичного внутригосударственного расследования.

### **СТАТЬЯ 34.** СОДЕЙСТВИЕ В ПЕРЕХВАТЕ ДАННЫХ СОДЕРЖАНИЯ

Стороны обязаны оказывать друг другу содействие в сборе или записи в режиме реального времени данных содержания, связанных с определенными операциями по передаче данных посредством компьютерной системы, в той мере, в какой это допускается применимыми в данном случае международными соглашениями и национальными законами.

## Часть 3. Организация и функционирование круглосуточной сети

### **СТАТЬЯ 35.** ОРГАНИЗАЦИЯ И ФУНКЦИОНИРОВАНИЕ КРУГЛОСУТОЧНОЙ СЕТИ

1. Каждая из Сторон обязуется назначить коммуникационный пункт, доступный 24 часа в сутки, 7 дней в неделю, с целью обеспечения оказания незамедлительного содействия в проведении расследования или разбирательства в отношении уголовных преступлений, связанных с использованием компьютерных систем или данных, и в сборе доказательств по уголовным преступлениям в электронном виде. Под содействием подразумевается помощь в осуществлении или, с разрешения национального законодательства либо согласно установившейся практике, непосредственное осуществление следующих мер:

(a) предоставление технической поддержки;

(b) сохранение данных, в соответствии со статьями 29—30;

(c) сбор доказательств, предоставление правовой информации и обнаружение подозреваемых.

2.

(a) Коммуникационный пункт каждой из Сторон должен обладать возможностями для обмена данными и сообщениями с коммуникационным пунктом другой Стороны посредством срочной связи.

(b) В случае, если назначенный Стороной коммуникационный пункт не является частью органа или органов, ответственных за оказание международного содействия и проведение экстрадиции, данный коммуникационный пункт должен иметь гарантированную возможность сообщения с таким органом или органами посредством срочной связи.

3. Каждая из Сторон обязана гарантировать наличие оборудования и обученного персонала для обеспечения бесперебойной работы сети.

## Глава IV. Заключительные положения

### **СТАТЬЯ 36.** ПОДПИСАНИЕ И ВСТУПЛЕНИЕ В СИЛУ

1. Настоящая Конвенция открыта для подписания Государствами — членами Совета Европы и теми не входящими в состав Совета Европы Государствами, которые принимали участие в ее разработке.

2. Настоящая Конвенция подлежит ратификации, принятию или утверждению. Грамоты о ратификации, принятии или утверждении подлежат депонированию у Генерального секретаря Совета Европы.

3. Настоящая Конвенция вступает в силу в первый день следующего месяца по истечении трехмесячного срока с момента, когда пять стран, в том числе, как минимум, три Государства — члена Совета Европы, выразят свое согласие на обязательность для них Конвенции в соответствии с положениями пунктов 1—2.

4. В отношении любого из Государств, подписавших Конвенцию, а впоследствии выразивших согласие на обязательность для них ее положений, Конвенция вступает в силу в первый день следующего месяца по исте-

чении трехмесячного срока с момента выражения Государством согласия на обязательность для него Конвенции, в соответствии с положениями пунктов 1—2.

### **СТАТЬЯ 37.** ПРИСОЕДИНЕНИЕ К КОНВЕНЦИИ

1. После вступления в силу настоящей Конвенции Комитет министров Совета Европы, после проведения консультаций с Договаривающимися Государствами и получения единодушного согласия со стороны этих Государств, может предложить присоединиться к Конвенции любому Государству, не входящему в Совет Европы и не принимавшему участия в разработке Конвенции. Решение принимается большинством голосов, предусмотренным в пункте (d) статьи 20 Устава Совета Европы, и всеми голосами представителей Договаривающихся Государств, правомочных заседать в Комитете.

2. В отношении любого из Государств, присоединяющихся к настоящей Конвенции в соответствии с вышеизложенным пунктом 1, Конвенция вступает в силу в первый день следующего месяца по истечении трехмесячного срока с момента депонирования документа о присоединении у Генерального секретаря Совета Европы.

### **СТАТЬЯ 38.** ТЕРРИТОРИАЛЬНОЕ ПРИМЕНЕНИЕ

1. Во время подписания или депонирования своей ратификационной грамоты или документа о принятии, утверждении или присоединении любое Государство может определить территорию или территории, на которые будет распространяться действие настоящей Конвенции.

2. Любое Государство может в более позднюю дату посредством декларации, адресованной Генеральному секретарю Совета Европы, распространить действие настоящей Конвенции на любую другую указанную в декларации территорию. В отношении такой территории Конвенция вступает в силу в первый день следующего месяца по истечении трехмесячного срока с момента получения такой декларации Генеральным секретарем.

3. Любая поданная на основании двух предыдущих пунктов декларация может быть отозвана в отношении любой указанной в ней территории путем уведомления в адрес Генерального секретаря Совета Европы. Отзыв вступает в силу в первый день следующего месяца по истечении трехмесячного срока с момента получения Генеральным секретарем такого уведомления.

### **СТАТЬЯ 39.** ДЕЙСТВИЕ КОНВЕНЦИИ

Цель настоящей Конвенции заключается в дополнении применимых между Сторонами многосторонних или двусторонних соглашений и договоров, в том числе положений:

— Европейской конвенции об экстрадиции, открытой для подписания 13 декабря 1957 г. в Париже (ETS № 24);

— Европейской конвенции об оказании содействия в расследовании уголовных дел, открытой для подписания 20 апреля 1959 г. в Страсбурге (ETS № 30);

— Дополнительного Протокола к Европейской Конвенции об оказании содействия в расследовании уголовных дел, открытого для подписания 17 марта 1978 г. в Страсбурге (ETS № 99).

2. Если между двумя или более Сторонами уже заключено соглашение или договор, предмет которого совпадает с предметом настоящей Конвенции, либо отношения по данному вопросу оговорены каким-либо иным способом, либо будут оговорены в будущем, эти Стороны вправе также применять такое соглашение или договор и регламентировать свои отношения в данной области соответствующим образом. Однако в случае, если Стороны регламентируют свои отношения по вопросам, рассматриваемым настоящей Конвенцией, иным образом, чем установлено в Конвенции, они не должны при этом совершать действий, противоречащих целям и принципам настоящей Конвенции.

3. Настоящая Конвенция никоим образом не задевает других прав, ограничений, обязательств и обязанностей любой из Сторон.

**СТАТЬЯ 40.** ВВЕДЕНИЕ ДОПОЛНИТЕЛЬНЫХ ЭЛЕМЕНТОВ

Во время подписания или депонирования своей ратификационной грамоты или документа о принятии, утверждении или присоединении любое из Государств путем подачи письменного заявления на имя Генерального секретаря Совета Европы может объявить, что оно пользуется правом требовать введения дополнительных элементов состава преступления, как это предусмотрено статьей 2, статьей 3, статьей 6, пунктом 1(b) статьи 7, пунктом 3 статьи 9 и пунктом 9(e) статьи 27.

**СТАТЬЯ 41.** ФЕДЕРАТИВНОЕ УСЛОВИЕ

1. Федеративное государство может сохранить за собой право принять обязательства по главе II данной Конвенции, совместимые с его фундаментальными принципами, регламентирующими отношения между его центральным правительством и государствами, входящими в его состав, или другими подобными территориальными субъектами, при условии, что оно будет в состоянии осуществлять сотрудничество согласно главе III.

2. При использовании права резервирования по пункту 1 федеративное государство не может применять данное право в целях уклонения или существенного уменьшения своих обязательств по обеспечению мер, установленных в главе II. В целом оно должно обеспечить широкое и эффективное применение указанных мер.

3. В отношении положений настоящей Конвенции, применение которых подпадает под юрисдикцию входящих в федерацию государств или других подобных территориальных субъектов, которые по конституционной системе федерации не обязаны принимать законодательных мер, федеральное правительство должно сообщать компетентным органам таких государств об упомянутых положениях со своим положительным мнением, побуждая их предпринимать надлежащие действия по их реализации.

### **СТАТЬЯ 42.** ОГОВОРКИ

Во время подписания или депонирования своей ратификационной грамоты или документа о принятии, утверждении или присоединении любое из Государств путем подачи письменного заявления на имя Генерального секретаря Совета Европы может объявить, что оно пользуется оговоркой или оговорками, предусмотренными в пункте 2 статьи 4, пункте 3 статьи 6, пункте 4 статьи 9, пункте 3 статьи 10, пункте 3 статьи 11, пункте 3 статьи 14, пункте 2 статьи 22, пункте 4 статьи 29 и пункте 1 статьи 41. Иные оговорки не допускаются.

### **СТАТЬЯ 43.** СТАТУС И СНЯТИЕ ОГОВОРОК

1. Любая из Сторон, сделавшая оговорку на основании статьи 42, может полностью или частично снять ее посредством уведомления в адрес Генерального секретаря Совета Европы. Снятие оговорки вступает в силу с момента получения такого уведомления Генеральным секретарем. Если в уведомлении указана дата, когда снятие оговорки вступает в силу, и эта дата наступает позднее дня получения уведомления Генеральным секретарем, снятие должно вступить в силу в указанную более позднюю дату.

2. Сторона, сделавшая оговорку в соответствии со статьей 42, должна снять такую оговорку, полностью или частично, как только позволят обстоятельства.

3. Генеральный секретарь Совета Европы может периодически запрашивать Стороны, сделавшие одну или более оговорок, упомянутых в статье 42, относительно перспектив снятия ими таких оговорок.

### **СТАТЬЯ 44.** ПОПРАВКИ

1. Любая Сторона может предлагать внесение поправок в настоящую Конвенцию. Генеральный секретарь Совета Европы сообщает о таких предложениях Государствам — членам Совета Европы; государствам, не являющимся членами Совета Европы, но участвовавшим в разработке настоящей Конвенции; а также всем Государствам, которые присоединились к Конвен-

ции либо получили приглашение присоединиться к ней в соответствии с положениями статьи 37.

2. О любой поправке, предложенной любой из Сторон, сообщается Европейскому комитету по проблемам преступности (CDPC), который должен представить на рассмотрение Комитета министров свое мнение относительно предложенной поправки.

3. Комитет министров рассматривает предложенную поправку и представленное Европейским комитетом по проблемам преступности (CDPC) мнение и, после консультаций со Сторонами настоящей Конвенции, не являющимися членами Совета Европы, может принять эту поправку.

4. Текст поправки, принятой Комитетом министров в соответствии с пунктом 3 данной статьи, пересылается Сторонам для принятия.

5. Любая поправка, принятая в соответствии с пунктом 3 данной статьи, вступает в силу на тридцатый день после того, как все Участники сообщат Генеральному секретарю о своем принятии поправки.

### **СТАТЬЯ 45.** РАЗРЕШЕНИЕ СПОРОВ

1. Европейский комитет по проблемам преступности (CDPC) должен информироваться о толковании и применении настоящей Конвенции.

2. В случае разногласий в отношении толкования или применения настоящей Конвенции заинтересованные Стороны должны стремиться к их дружественному разрешению путем переговоров или с помощью любых других средств мирного урегулирования по своему выбору, включая передачу рассмотрения спорного вопроса в Европейский комитет по проблемам преступности (CDPC), в арбитраж, чьи решения должны иметь обязательную силу для Сторон, или же в Международный суд, по согласованию заинтересованных Сторон.

### **СТАТЬЯ 46.** КОНСУЛЬТАЦИИ МЕЖДУ СТОРОНАМИ

1. Стороны должны периодически проводить консультации с целью содействия:

(a) эффективному использованию и осуществлению настоящей Конвенции, включая определение любых

возникающих в связи с этим проблем, а также последствий любых деклараций или оговорок, сделанных согласно настоящей Конвенции;

(b) обмену информацией относительно важных событий и разработок в юридической, политической и технологической областях, имеющих отношение к киберпреступлениям, а также к сбору доказательств в электронной форме;

(c) рассмотрению возможных дополнений или поправок к Конвенции.

2. Европейский комитет по проблемам преступности (CDPC) должен периодически информироваться о результатах, достигнутых в ходе упомянутых в пункте 1 консультаций.

3. Европейский комитет по проблемам преступности (CDPC) должен надлежащим образом содействовать упомянутым в пункте 1 консультациям и принимать меры, необходимые для того, чтобы содействовать Сторонам в их усилиях по дополнению и совершенствованию Конвенции. По меньшей мере в течение трех лет после вступления данной Конвенции в силу Европейский комитет по проблемам преступности (CDPC) в сотрудничестве со Сторонами должен проводить обзор всех положений Конвенции и в случае необходимости рекомендовать внесение любых уместных поправок.

4. Кроме случаев, когда Совет Европы принимает на себя соответствующие обязательства, расходы по выполнению положений пункта 1 несут Стороны в соответствии с определенным ими способом.

5. Секретариат Совета Европы оказывает Сторонам помощь в выполнении ими своих функций в соответствии с настоящей статьей.

### **СТАТЬЯ 47.** ДЕНОНСАЦИЯ

1. Любая из Сторон может в любое время денонсировать настоящую Конвенцию посредством уведомления в адрес Генерального секретаря Совета Европы.

2. Такая денонсация вступает в силу в первый день следующего месяца по истечении трехмесячного срока после даты получения уведомления Генеральным секретарем.

**СТАТЬЯ 48.** УВЕДОМЛЕНИЕ

Генеральный секретарь Совета Европы уведомляет Государства — члены Совета Европы; Государства, не являющиеся членами Совета Европы, но участвовавшие в разработке настоящей Конвенции; а также все Государства, которые присоединились к Конвенции либо получили приглашение присоединиться к ней, о:

(a) любом подписании Конвенции;

(b) депонировании любой ратификационной грамоты или документа о принятии, утверждении или присоединении;

(c) любой дате вступления настоящей Конвенции в силу в соответствии с положениями статей 36 и 37;

(d) любой декларации, сделанной в соответствии со статьей 40, или любой оговорке, сделанной в соответствии со статьей 42;

(e) любом другом акте, уведомлении или сообщении, касающемся настоящей Конвенции.

В удостоверение чего нижеподписавшиеся, в должной форме уполномоченные на это, подписали настоящую Конвенцию.

Совершено в городе Будапеште, ноября 23-го дня 2001 года, на английском и французском языках, при этом оба текста являются равно аутентичными, в одном экземпляре, который должен будет храниться в архиве Совета Европы. Генеральный секретарь Совета Европы пересылает заверенные копии каждому Государству — члену Совета Европы; Государствам, не являющимся членами Совета Европы, но участвовавшим в разработке настоящей Конвенции; а также всем Государствам, которым было предложено присоединиться к настоящей Конвенции.

**Международный стандарт 27032:2012**

## ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ. МЕТОДЫ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ. РУКОВОДЯЩИЕ УКАЗАНИЯ ПО ОБЕСПЕЧЕНИЮ КИБЕРБЕЗОПАСНОСТИ

Стандарт 27032:2012 позволяет обеспечить безопасность онлайн-операций, обмена персональной информацией через Интернет и защитить компьютер при просмотре веб-сайтов.

Поскольку Интернет необходим при осуществлении разных видов деятельности, от обмена важными рабочими документами до оплаты счетов, кибербезопасность стала важнейшей темой повестки дня. Стандарт позволяет сделать киберпространство безопаснее.

Киберпространство — комплексная среда, позволяющая осуществлять взаимодействие между людьми, программным обеспечением и службами, используя глобально распределенные устройства и сети информационных и коммуникационных технологий. Взаимодействие играет важнейшую роль для обеспечения безопасности онлайновой среды. В стандарте рассматриваются ранее не решенные вопросы безопасности, возникшие вследствие недостаточной коммуникации между различными пользователями и провайдерами (поставщиками услуг) киберпространства. В нем рассматриваются риски, не охватываемые современными технологиями безопасности в Интернете, сетях, при передаче информации и осуществлении коммуникаций.

Йохан Амсенга, председатель рабочей группы, разработавшей стандарт, разъясняет: «Устройства и связанные сети, поддерживающие киберпространство, имеют множество владельцев, каждый из которых ведет собственный бизнес и решает вопросы эксплуатации и регулирования. Множество пользователей и провайдеров не только не имеют общих исходных данных,

но и рассматривают проблемы обеспечения безопасности под разными углами зрения. Такой фрагментированный подход порождает уязвимости в безопасности киберпространства. Стандарт предлагает всеобъемлющее совместное решение по сокращению таких рисков, основанное на участии многих заинтересованных лиц».

Стандарт устанавливает принципы:

- обмена информацией;
- координации;
- разрешения инцидентов.

Стандарт обеспечивает надежное и безопасное взаимодействие и защиту персональных данных пользователей во всем мире. Он помогает подготовиться, идентифицировать, осуществить мониторинг и реагировать на:

- атаки с применением социальной инженерии;
- хакерство;
- вредоносные приложения (malware);
- шпионские приложения (spyware);
- другое нежелательное программное обеспечение.

## Резолюция Генеральной Ассамблеи Организации Объединенных Наций A/RES/57/239

В 2002 году ООН приняла резолюцию по созданию глобальной культуры кибербезопасности, определив основные элементы:

- **осведомленность:** участники должны быть осведомлены о необходимости безопасности информационных систем и сетей и о том, что они могут сделать для повышения безопасности;

- **ответственность:** участники отвечают за безопасность информационных систем и сетей сообразно с ролью каждого из них. Участники должны подвергать свои политику, практику, меры и процедуры регулярному обзору и оценивать, соответствуют ли они среде их применения;

- **реагирование:** участники должны принимать своевременные и совместные меры по предупреждению инцидентов, затрагивающих безопасность, их обнаружению и реагированию на них. Они должны обмениваться в надлежащих случаях информацией об угрозах и факторах уязвимости и вводить процедуры, предусматривающие оперативное и эффективное сотрудничество в деле предупреждения таких инцидентов, их обнаружения и реагирования на них. Это может предполагать трансграничный информационный обмен и сотрудничество;

- **этика:** поскольку информационные системы и сети проникли во все уголки современного общества, участникам необходимо учитывать законные интересы других и признавать, что их действия или бездействие могут повредить другим;

- **демократия:** безопасность должна обеспечиваться так, чтобы это соответствовало ценностям, которые признаются демократическим обществом, включая свободу обмена мыслями и идеями, свободный поток

информации, конфиденциальность информации и коммуникации, надлежащую защиту информации личного характера, открытость и гласность;

- **оценка риска:** все участники должны выполнять периодическую оценку риска, которая: позволяет выявлять угрозы и факторы уязвимости; имеет достаточно широкую базу, чтобы охватить такие ключевые внутренние и внешние факторы, как технология, физические и человеческие факторы, применяемая методика и услуги третьих лиц, сказывающиеся на безопасности; дает возможность определить допустимую степень риска; помогает выбрать надлежащие инструменты контроля, позволяющие регулировать риск потенциального ущерба информационным системам и сетям с учетом характера и значимости защищаемой информации;

- **проектирование и внедрение средств обеспечения безопасности:** участники должны рассматривать соображения безопасности в качестве важнейшего элемента планирования и проектирования, эксплуатации и использования информационных систем и сетей;

- **управление обеспечением безопасности:** участники должны принять комплексный подход к управлению обеспечением безопасности, опираясь на динамичную оценку риска, охватывающую все уровни деятельности участников и все аспекты их операций;

- **переоценка:** участники должны подвергать вопросы безопасности информационных систем и сетей обзору и повторной оценке и вносить надлежащие изменения в политику, практику, меры и процедуры обеспечения безопасности, учитывая при этом появление новых и изменение прежних угроз и факторов уязвимости.

# СЛОВАРЬ ТЕРМИНОВ И ОПРЕДЕЛЕНИЙ

**Аватар** — графическое представление интернет-пользователя. Может быть двухмерным изображением (иконкой), трехмерной моделью или представлен в виде текста.

**Авторское право** — право, которым обладает автор на созданные им произведения науки, литературы и искусства. Выступает в качестве гарантии того, что интеллектуальный или творческий труд автора даст ему возможность заработать на результатах своего труда. Никто без разрешения автора не может воспроизводить, распространять, публично демонстрировать, продавать, импортировать, пускать в прокат, публично исполнять, показывать, исполнять в эфире или размещать в Интернете его произведение.

**Аккаунт** — учетная запись, представляющая собой совокупность данных о пользователе, которые тот вводит и хранит на каком-либо сайте или интернет-сервисе.

**Аниме** — японская анимация, мультфильмы, рассчитанные в основном на подростковую и взрослую аудитории. Издается в форме телевизионных сериалов и фильмов. Сюжеты могут описывать множество персонажей, отличаться разнообразием мест и эпох, жанров и стилей.

**Брандма́уэр Windows** — встроенный в Microsoft Windows межсетевой экран; является частью Центра обеспечения безопасности Windows.

**Браузер** — прикладное программное обеспечение для просмотра веб-страниц, содержания веб-документов, компьютерных файлов и их каталогов, управления веб-приложениями, а также для решения других задач. В глобальной сети браузеры используют для запроса, обработки, манипулирования и отображения содержания веб-сайтов.

**Виртуальная реальность** — созданный техническими средствами мир, передаваемый человеку через его ощущения: зрение, слух, осязание и др. Имитирует как воздействие, так и реакции на воздействие.

**Вмешательство в данные** — противоправное повреждение, удаление, нарушение, изменение либо пресечение компьютерных данных.

**Вмешательство в систему** — серьезное противоправное препятствование функционированию компьютерной системы путем ввода, передачи, повреждения, удаления, нарушения, изменения либо пресечения компьютерных данных.

**Деструктивное восприятие мира и окружения** — разрушительное поведение человека, отклоняющееся от медицинских и психологических норм, приводящее к нарушению качества его жизни, снижению критичности к своему поведению, искаженному восприятию и пониманию происходящего, снижению самооценки и эмоциональным нарушениям, что в итоге приводит к состоянию социальной дезадаптации личности, вплоть до ее полной изоляции. Деструктивность неизбежно присутствует у каждого индивида, однако обнаруживается, как правило, в переломные периоды его жизни. Прежде всего это относится к подросткам, возрастные особенности психики которых в совокупности с проблемой социализации и недостатком внимания со стороны взрослых приводят к деструктивным изменениям личности.

**Детский суицид** — непосредственное совершение ребенком действий, направленных на лишение себя жизни.

**Защита информации** — деятельность, направленная на предотвращение утечки информации, несанкционированных и непреднамеренных воздействий на информацию.

**Зомбирование** — форсированная обработка подсознания человека, превращение его в бездушного, беспрекословного, послушного чужой (обычно злой) воле.

**Инсайдерская угроза** — вредоносная для организации угроза, которая может исходить от людей внутри организации (работников, бывших работников, подрядчиков, деловых партнеров), у которых есть информация о методах безопасности внутри организации, данных и компьютерных системах.

**Интеллектуальная собственность** — совокупность исключительных прав на конкретные результаты интеллектуальной деятельности человека, начиная с новых изобретений и знаков, обозначающих собственность на продукты и услуги, и заканчивая книгами, фотографиями, кинофильмами и музыкальными произведениями.

**Интернет** — всемирная система объединенных компьютерных сетей для хранения и передачи информации.

**Интернет-ресурс (сайт)** — элемент сети Интернет; массив связанных данных, имеющий уникальный адрес и воспринимаемый пользователем как единое целое.

**Интернет-сервис** — сайт, представляющий в основном бесплатные услуги для пользователей (например, поисковая система, почтовая служба, бесплатный хостинг и т. д.).

**Информационная безопасность** — практика предотвращения несанкционированного доступа, использования, раскрытия, искажения, изменения, исследования, записи или уничтожения информации, вне зависимости от формы ее представления (электронной или физической).

**Канал связи** — система технических устройств и среда распространения сигналов, обеспечивающая передачу информации между абонентами.

**Кибератака (хакерская атака)** — покушение на информационную безопасность компьютерной системы.

**Кибербезопасность** — набор средств, стратегий, принципов обеспечения безопасности, гарантий безопасности, подходов к управлению рисками, действий, профессиональной подготовки, страхования и технологий, которые используются для защиты киберсреды, ресурсов организаций и пользователей.

**Кибербезопасность объекта** — свойство объекта, характеризующее его возможность не быть причиной образования ущерба для киберпространства.

**Кибербуллинг** — преследование сообщениями, содержащими оскорбления, агрессию, запугивание, с помощью различных интернет-сервисов.

**Кибервымогатель** — хакер, проводящий кибератаки с помощью вымогательского программного обеспечения.

**Киберзащищенность объекта** — свойство объекта, характеризующее его возможность предотвращать образование ущерба от хакерских кибератак или уменьшать величину такого поражения.

**Кибернетика** — наука об общих закономерностях получения, хранения, преобразования и передачи информации в сложных управляющих системах, будь то машины, живые организмы или общество.

**Киберпреступление** — преступление, совершаемое с использованием компьютера и (или) Интернета. Может совершаться с помощью различных методов и инструментов (например, фишинг, вирусы, шпионское программное обеспечение, программы-вымогатели и социальная инженерия) чаще всего с целью кражи личных данных или финансовых средств.

**Киберпреступность** — любая преступная активность, где компьютер является предметом, а информационная безопасность — объектом преступления, а также любые действия, где компьютеры использу-

ются как орудия или средства совершения преступлений против собственности, авторских прав, общественной безопасности или нравственности (например, компьютерное мошенничество и т. п.). Примыкают к киберпреступности действия, направленные на поддержание условий для ее существования и развития (использование электронной почты для коммуникации, создание собственных сайтов, направленных на распространение криминальной идеологии, а также обмен криминальным опытом и специальными познаниями).

**Киберпространство** — виртуальное пространство, в котором функционируют и взаимодействуют кибер-объекты.

**Киберриск** — потеря информации на одном компьютере до кибератак, связанных с функционированием систем вычислений.

**Киберсреда** — условная среда, в которой происходит обмен информацией посредством компьютерных сетей.

**Киберугроза (киберопасность)** — незаконное проникновение или угроза вредоносного проникновения в виртуальное пространство для достижения политических, социальных или иных целей.

**Компьютер** — устройство или система, способная выполнять заданную, четко определенную, изменяемую последовательность операций.

**Компьютерная сеть** — совокупность компьютеров, соединенных с помощью каналов связи в единую систему и работающих под управлением специального программного обеспечения.

**Компьютерный вирус** — вид вредоносного программного обеспечения, способного создавать копии самого себя и внедряться в код других программ, системные области памяти, загрузочные секторы, а также распространять свои копии по разнообразным каналам связи. Часто его сопутствующей функцией является нарушение работы программно-аппаратных

комплексов — удаление файлов и даже операционной системы, приведение в негодность структур размещения данных, блокирование работы пользователей.

**Концепция стратегии кибербезопасности в Российской Федерации** — условия, при которых все объекты киберпространства защищены от максимально возможного количества угроз, а также воздействий с нежелательными последствиями.

**Крэкерская атака** — действие, целью которого является захват контроля (повышение прав) над удаленной (локальной) вычислительной системой, ее дестабилизация либо отказ в обслуживании.

**Линия связи** — совокупность технических устройств и физической среды, обеспечивающих передачу сигналов от передатчика к приемнику. На основе линий связи строятся каналы связи.

**Локальная компьютерная сеть** — система взаимосвязанных компьютеров, находящихся на небольшой территории, например в учреждении или на территории учебного заведения. Компьютеры в этой сети могут связываться как с центральным компьютером, так и друг с другом. Такая сеть используется как система связи, а также для обеспечения широкого доступа к возможностям центрального компьютера.

**Маркетплейс** — онлайн-площадка, систематизирующая информацию о товарах и услугах разных компаний, зарегистрированных в системе. Предоставляет эту информацию по запросу покупателя в структурированном виде, пригодном для сравнения, выбора и осуществления покупки выбранного товара.

**Медиаграмотность** — умение пользоваться поисковыми системами, обеспечивающими доступ к информации, критически анализировать содержание информации и создавать сообщения в разных видах, жанрах и формах.

**Мессенджер** — программа по обмену мгновенными сообщениями.

**Незаконный доступ** — противоправный умышленный доступ к компьютерной системе либо ее части.

**Незаконный перехват** — противоправный умышленный перехват не предназначенных для общественности передач компьютерных данных на компьютерную систему, с нее либо в ее пределах.

**Нейролингвистическое программирование** — направление в психотерапии и практической психологии, основанное на технике моделирования (копирования) вербального и невербального поведения людей, добившихся успеха в какой-либо области, и наборе связей между формами речи, движением глаз, тела и памятью.

**Онлайн-урок** — одна из форм проведения современного урока, при которой обучение проводится в режиме реального времени через Интернет.

**Операционная система** — комплекс взаимосвязанных программ, предназначенных для управления ресурсами компьютера и организации взаимодействия с пользователем.

**Оффшорный счет** — счет в банке, который расположен вне страны проживания клиента. Банки, предоставляющие открытие оффшорных счетов, как правило, находятся в юрисдикциях с очень низкими налоговыми ставками и предоставляют ряд юридических и финансовых преимуществ.

**Патч** — автоматизированное, отдельно поставляемое программное средство, используемое для устранения проблем в программном обеспечении или изменения его функционала.

**Пиратское программное обеспечение** — нелегально скопированное и распространенное программное обеспечение на дисках и в компьютерных сетях, как правило, со снятой программной защитой.

**Преступление в киберпространстве** — противоправное вмешательство в работу компьютеров, компьютерных программ, компьютерных сетей, несанкцио-

нированная модификация компьютерных данных, а также иные противоправные общественно опасные действия, совершенные с помощью или посредством компьютеров, компьютерных сетей и программ.

**Программное обеспечение** — совокупность программ, позволяющих осуществить на компьютере автоматизированную обработку информации.

**Профайл** — страница пользователя, на которой отображается вся актуальная информация: имя и фамилия, дата регистрации, место нахождения, контакты и краткое самоописание.

**Сервер** — специализированный компьютер или специализированное оборудование для выполнения на нем сервисного программного обеспечения.

**Системный администратор (сисадмин)** — сотрудник, должностные обязанности которого подразумевают обеспечение штатной работы парка компьютерной техники, сети и программного обеспечения. Зачастую сисадмину вменяется обеспечение информационной безопасности в организации.

**Скриншот (скрин)** — изображение, полученное устройством и показывающее в точности то, что видит пользователь на экране монитора или другого визуального устройства вывода.

**Сленг** — набор особых слов или новых значений уже существующих слов, употребляемых в различных группах людей (профессиональных, общественных, возрастных).

**Смежное право** — совокупность норм, предоставляемых для правовой охраны интересов правообладателей в отношении объектов интеллектуальной деятельности (фонограмм, произведений науки, литературы и искусства, базы данных).

**Социальное бойкотирование** — форма политической и экономической борьбы, которая предполагает полное или частичное прекращение отношений с отдельным лицом, организацией, предприятием.

**Спам** — массовая рассылка корреспонденции рекламного или иного характера лицам, не выражавшим желания ее получать.

**Субкультурная мода** — яркие визуальные образы, на которые активно работает индустрия моды.

**Транзакция** — серия операций по обмену информацией, в результате которых в систему вносятся изменения.

**Троянская программа** — это вредоносная компьютерная программа, которая используется для заражения системы компьютера и приводит к вредоносной активности на нем. Как правило, такие программы используются для кражи личной информации, распространения других вирусов или просто нарушения производительности компьютера. Кроме того, хакеры могут использовать их для получения несанкционированного удаленного доступа к зараженным компьютерам, заражения файлов и повреждения системы.

**Файл** — последовательный набор данных, распознаваемый компьютером как единое целое, имеющий собственное имя и расширение.

**Фиат** — в переводе с латинского означает «указание» или «декрет».

**Фашизм** — идеология, политическое движение и социальная практика, которые характеризуются следующими признаками и чертами: обоснованием по расовому признаку превосходства и исключительности одной нации, провозглашаемой в силу этого господствующей; нетерпимостью и дискриминацией по отношению к другим «чужеродным», «враждебным» нациям и национальным меньшинствам; отрицанием демократии и прав человека; насаждением режима, основанного на принципах тоталитарно-корпоративной государственности, однопартийности и вождизма; утверждение насилия и террора в целях подавления политического противника и любых форм инакомыслия; милитаризацией об-

щества, созданием военизированных формирований и оправданием войны как средства решения межгосударственных проблем.

**Фишинг** — вид интернет-мошенничества, целью которого является получение доступа к конфиденциальным данным пользователей — логинам и паролям.

**Хакер** — компьютерный взломщик, проникающий в закрытые информационные сети, банки данных с целью получения доступа к секретной информации, а также заражения их вирусом.

**Хакерская атака** — мозговой штурм, направленный на нахождение пути решения сложных задач. В хакерской атаке могут принимать участие один или несколько высококлассных специалистов (хакеров). В результате мозгового штурма могут быть придуманы нетрадиционные методы решения проблемы или внесены оптимизирующие корректировки в уже существующие методы.

**Хостинг** — услуга по предоставлению ресурсов для размещения информации на сервере, постоянно находящемся в сети (обычно Интернет).

**Цифровая репутация** — негативная или позитивная информация о пользователе в сети.

**Цифровизация** — переход на цифровой способ связи, записи и передачи данных с помощью цифровых устройств.

**Чат** — общение в Интернете, когда разговор ведется в реальном времени.

**Электронная почта** — технология и предоставляемые ею услуги по пересылке и получению электронных сообщений, которые распределяются в компьютерной сети.

**Электронные деньги** — платежные средства, представленные и обращаемые в электронном виде, оборот которых гарантирует анонимность сторон, участву-

ющих в расчетах: безналичных расчетах между продавцами и покупателями, банками и их клиентами, осуществляемых посредством компьютерной сети, систем связи с применением средств кодирования информации и ее автоматической обработки.

**Электронные нефиатные деньги** — электронные единицы стоимости, которые установлены негосударственными платежными системами; не равны государственным валютам.

**Электронные фиатные деньги** — электронные единицы стоимости, которые установлены и гарантируются государством; равны государственным валютам.

**Android** — операционная система для смартфонов, планшетов, электронных книг, цифровых проигрывателей, наручных часов, фитнес-браслетов, игровых приставок, ноутбуков, нетбуков, смартбуков, телевизоров и других устройств.

**Fancy Bear** — хаккерская группа, действующая с 2004 г. Известна кибератаками на государственные, информационные, военные структуры зарубежных стран.

**IBM X-Force Research and Development** — одна из наиболее признанных в мире научно-исследовательских групп в области коммерческой безопасности.

**IT-специалист** — представитель одной из множества профессий в области информационных технологий (программист, разработчик, администратор сетей и баз, модератор, специалист по робототехнике, по информационной безопасности, web-дизайнер, 3D-аниматор).

**LinkedIn** — социальная сеть для поиска и установления деловых контактов.

**Mossack Fonseca** — юридическая фирма со штаб-квартирой в Панаме и более чем 40 офисами по всему миру. Специализируется на торговом праве, торговых услугах и финансовом консультировании частных лиц и организаций.

**PDF-атака** — атака с помощью зараженного файла.

**SEO (Search Engine Optimization)** — совокупность работ, направленных на улучшение позиций сайта в результатах выдачи поисковых систем для увеличения посещаемости сайта.

**Western Union** — американская компания, специализирующаяся на предоставлении услуг денежного посредничества. Является одним из лидеров на рынке международных денежных переводов.

**Wi-Fi** — зарегистрированный в 1991 г. нидерландской компанией бренд «WECA», что обозначало словосочетание «Wireless Fidelity» (переводится как «беспроводная точность»). До нашего времени дошла аббревиатура Wi-Fi.

**Yahoo** — одна из популярнейших в мире поисковых систем.

# СПИСОК РЕКОМЕНДУЕМОЙ ЛИТЕРАТУРЫ

ГОСТ Р 50922-2006. Защита информации. Основные термины и определения.

ГОСТ Р 52653-2006. Информационно-коммуникационные технологии в образовании. Термины и определения.

# СОДЕРЖАНИЕ