Исследование судебной практики по административным правонарушениям, связанным с безопасностью персональных данных и защитой информации

Оглавление

Аннотация

Экспертно-аналитический центр группы компаний InfoWatch представляет исследование судебных дел о нарушениях, связанных с защитой информации по статьям Кодекса Российской Федерации об административных правонарушениях.

Для исследования мы выбрали статьи, которые относятся к обработке и обеспечению безопасности персональных данных, нарушению правил и незаконной деятельности в области защиты информации и разглашению информации ограниченного доступа.

Мы не рассматривали дела, связанные с отказом в доступе к информации, неразмещением данных в открытом доступе, со свободой слова, пропагандой, клеветой и т.п.

В этом отчете мы не повторяли данные отчетов официальных органов и судебной статистики, но анализировали судебные дела по статьям, относящимся к нарушениям в области связи и информации, исследуя не количество и распределение дел, но содержание дел: типы привлекаемых к ответственности лиц, географию судов, в которых были рассмотрены дела, правомерность доступа к раскрытой информации, типы решений и величину назначаемых наказаний, типы заявителей и т.д.

Основной акцент исследования был сделан на вопросы обеспечения защиты информации в автоматизированных системах, в том числе, при обработке персональных данных.

Только факты

- ✓ Для подготовки настоящего отчёта рассмотрено более 2 тысяч записей, содержащихся в ГАС «Правосудие» и относящихся к правоприменительной практике по статьям КоАП 13.11 – 13.14.
- ✓ Среди рассмотренных в «ГАС» Правосудие» актов сформирована выборка из 270 судебных дел.
- ✓ 72% судебных дел, выделенных в ходе исследования, относятся к безопасности персональных данных – статье 13.11 (части 1, 7 и 8); 25,8 % дел – к статье 13.14 «Разглашение информации с ограниченным доступом».

- ✓ Инициаторами возбуждения дел являются не только сами пострадавшие от распространения их персональных данных, но и государственные органы (Роскомнадзор или Прокуратура) при проведении проверок.
- ✓ 38% административных дел по статье 13.11 КоАП возбуждено Роскомнадзором или органами прокуратуры России (70 из 182 дел).

- ✓ В 36% случаях по статье 13.11 (ч.1, 7 и 8) Роскомнадзором или органами прокуратуры России было отказано заявителям в возбуждении дел, после чего заявители обращались в суд для обжалования постановлений об отказе.
- ✓ Решение об отказе в возбуждении дела в среднем обжалуют дважды, иногда - четыре-пять раз.

- ✓ 26% дел по ч.1 статьи 13.11 (за обработку ПДн в случаях, не предусмотренных законодательством РФ в области ПДн, либо обработку ПДн, несовместимую с целями сбора ПДн) относятся к нарушениям, связанным с применением средств автоматизации.

- ✓ Самый крупный штраф, назначенный по ч.1 статьи 13.11 юридическому лицу, составляет 30 тыс. рублей.

Сокращения

ГАС «Правосудие»	Государственная Автоматизированная система Российской Федерации «Правосудие»
КоАП РФ	Кодекс Российской Федерации об административных правонарушениях
ПДн	Персональные данные
ЭАЦ	Экспертно-аналитический центр ГК InfoWatch

Подход и предмет исследования

Для исследования мы выбрали статьи КоАП РФ, дела по которым, согласно нашему предположению, могут относиться к нарушениям в сфере информационной безопасности, и разделили их на три типа. Первый тип таких статей относится к утечкам персональных данных, второй – к нарушениям в сфере защиты информации, а третий – к нарушениям, связанным с отказом в доступе к информации, неразмещением информации в открытом доступе, со свободой слова, пропагандой, клеветой, нарушением авторских прав, размещением вакансий, содержащих информацию дискриминационного характера и т.п. Третий тип статей мы исключили из исследования, т.к. они не относятся к сфере защиты информации, в том числе к области деятельности компании InfoWatch.

Для исследования мы отобрали решения, вынесенные в период с 01.01.2019 г. по 31.12.2020 г. судебными инстанциями всех уровней (от районных судов до Верховного суда РФ) по делам об административных правонарушениях, связанным с утечками информации ограниченного доступа, а также в части утечек информации по причине нарушения требований по обработке персональных данных.

Таблица 1. Статьи, предварительно отобранные для исследования

Статья КоАП	Название
Утечки персональных данных и нарушения, приведшие к утечкам	
13.11	Нарушение законодательства Российской Федерации в области персональных данных
Нарушения в сфере защиты информации	
7.31.1	Нарушение порядка и (или) сроков возврата денежных средств, внесенных в качестве обеспечения заявок на участие в определении поставщика (подрядчика, исполнителя), порядка и (или) сроков блокирования операций по счету участника закупки, порядка ведения реестра участников электронного аукциона, получивших аккредитацию на электронной площадке, правил документооборота при проведении электронного аукциона, разглашение оператором электронной площадки, должностным лицом оператора электронной площадки информации об участнике закупки до подведения результатов электронного аукциона (действующая редакция)
13.12	Нарушение правил защиты информации
13.13	Незаконная деятельность в области защиты информации
13.14	Разглашение информации с ограниченным доступом
15.21	Неправомерное использование инсайдерской информации
17.13	Разглашение сведений о мерах безопасности
20.24	Незаконное использование специальных технических средств, предназначенных для негласного получения информации, в частной детективной или охранной деятельности

Для начала мы изучили статистику Судебного департамента РФ по количеству дел по всем приведенным выше статьям (см. раздел Официальная статистика). Отметили, что:

Таблица 2. Наличие официальной статистики по статьям КоАП за 2019-2020 гг.

Статья КоАП	Количество дел	Примечание
7.31.1	-	официальная статистика не приводится
13.11 13.12 13.13 13.14	-	в официальной статистике указано суммарное число дел по группе статей 13.11, 13.11.1, 13.12 ч.2, 4, 5, 13.13, 13.14, всего – 2 636 дел
15.21	-	приведена статистика суммарно по группе статей 15.21, 15.30 и 15.35 ч. 1, 4, всего – 35 дел
17.13	13	
20.24	-	приведена суммарная статистика по статьям 20.23 и 20.24, всего – 29 дел.

С полученными статистическими данными мы обратились к государственной автоматизированной системе «Правосудие», чтобы уточнить наличие актов судебных дел по указанным статьям для их исследования по сути нарушения и другим данным.

Результаты поиска в ГАС «Правосудие» судебных решений 2019-2020 гг. по отобранным статьям следующие:

- 67 записей о судебных делах по статье 7.31.1 на деле относились к статье 7.31 или, если все же они были связаны со статьей 7.31.1, то не касались сферы защиты информации, а были связаны с нарушением сроков возврата денежных средств для обеспечения заявки об участии в конкурсе;
- по статьям 13.11-13.14 за двухлетний период нами было обнаружено свыше двух тысяч записей;
- по статье 15.21 найдено 9 записей, но все они при открытии каждого из результатов поиска содержали дела по статье 5.21;
- по статье 17.13 в системе присутствуют 3 записи, но они фактически содержат дела по статьям 12.19 ч. 2, 7.13 и 19.13;
- по статье 20.24 система содержит 16 записей, но при проверке выяснилось, что 15 из них были ошибочно отнесены к этой статье, подтвердить отношений 16-й записи к статье 20.24 невозможно из-за отсутствия судебного акта (не прикреплён).

Кроме того, часть записей не содержат акты с текстом самого решения.

Важно отметить, что срок давности для административного правонарушения составлял в 2019-2020 гг. 3 месяца. Таким образом, заявителям в 18% дел отказали в рассмотрении судебного дела в связи с истечением срока давности.

Как правило, дела рассматривают в течение месяца с момента подачи заявления в суд, процедура следующая:

1) заявитель подает жалобу в Роскомнадзор или органы прокуратуры;
2) если заявитель не удовлетворен постановлением Роскомнадзора или органа прокуратуры, то он подает жалобу на это постановление в суд;
3) если заявитель недоволен решением суда, то он может обжаловать это решение в следующей инстанции.

Как итог всего вышесказанного, **мы ограничили исследование статьями и теми их частями, по которым за исследуемый период имеется информации в ГАС «Правосудие» и релевантными тематике утечек информации ограниченного доступа, которые относятся к нарушениям в области защиты информации и, в том числе, персональных данных, а именно: 13.11 (ч.1, 7 и 8), 13.12 (ч.1), 13.13 и 13.14 Главы 13 КоАП РФ.** Ниже приведено описание каждой статьи и её части:

Таблица 3. Содержание выбранных для исследования статьей

Статья КоАП	Название
13.11 ч.1, 7 и 8	Нарушение законодательства Российской Федерации в области персональных данных ч.1 Обработка персональных данных в случаях, не предусмотренных законодательством Российской Федерации в области персональных данных, либо обработка персональных данных, несовместимая с целями сбора персональных данных ч.7 Невыполнение оператором, являющимся государственным или муниципальным органом, предусмотренной законодательством Российской Федерации в области персональных данных обязанности по обезличиванию персональных данных либо несоблюдение установленных требований или методов по обезличиванию персональных данных ч.8 Невыполнение оператором при сборе персональных данных, в том числе посредством информационно-телекоммуникационной сети "Интернет", предусмотренной законодательством Российской Федерации в области персональных данных обязанности по обеспечению записи, систематизации, накопления, хранения, уточнения (обновления, изменения) или извлечения персональных данных граждан Российской Федерации с использованием баз данных, находящихся на территории Российской Федерации
13.12 ч.1	Нарушение правил защиты информации ч.1. Нарушение условий, предусмотренных лицензией на осуществление деятельности в области защиты информации (за исключением информации, составляющей государственную тайну)
13.13	Незаконная деятельность в области защиты информации

13.14	Разглашение информации с ограниченным доступом

База судебных дел

Для исследования мы подготовили выборку судебных дел по выбранным для исследования статьям КоАП РФ на основе данных Государственной Автоматизированной системы Российской Федерации «Правосудие» (ГАС «Правосудие»). Для уточнения деталей судебных дел периодически обращались к ресурсам:

- Судебныерешения.рф;
- Сайты районных и городских региональных судов.

В базу судебных дел внесли данные о судебных делах за 2019-2020 гг. по выбранным статьям, включая:

- Номер дела
- Описание сути нарушения
- Дата поступления дела
- Дата судебного решения
- Регион
- Уровень и тип суда
- Надзорный орган (Роскомнадзор/прокуратура)
- Тип (юридическое/физическое лицо, российское/иностранное)
- ФИО/Название истца и ответчика
- Тип решения
- Тип и размер наказания

Ответчика по судебному делу относили к должностным лицам, если нарушитель внутри организации не был установлен и, как следствие, ответственность ложилась на сотрудника (зачастую руководителя организации), который наделен полномочиями локально-нормативным актами, например, должностными инструкциями.

Объем и качество данных

В системе ГАС «Правосудие» содержится следующее количество записей для каждой выбранной для исследования статьи:

Таблица 4. Количество записей в ГАС «Правосудие»

Статья КоАП	Название	Количество записей за 2019-2020 гг.
13.11	Нарушение законодательства Российской Федерации в области персональных данных	1911
13.12 ч.1	Нарушение правил защиты информации ч.1. Нарушение условий, предусмотренных лицензией на осуществление деятельности в области защиты информации (за исключением информации, составляющей государственную тайну)	8
13.13	Незаконная деятельность в области защиты информации	13

13.14	Разглашение информации с ограниченным доступом	184

Каждая запись ГАС «Правосудие» содержит информацию об одном судебном заседании по тому или иному делу.
Количество записей в Таблице 4 приведены суммарно за два года – 2019 и 2020. Если попробовать автоматически выделить выборки отдельно по 2019 г. и 2020 г., ГАС «Правосудие» выдает количество записей, сумма которых не совпадает с общим количеством за два года. Иногда разница составляет сотни записей, как в случае со статьей 13.11 КоАП РФ. Также для статьи 13.11 не представляется возможным автоматически определить число записей судебных решений отдельно по частям 1, 7 и 8: система ГАС «Правосудие» позволяет выделить только 526 записей решений по ч.1, по остальным частям информацию о количестве записей путём выборки установить невозможно, в связи с чем мы вручную просмотрели все найденные записи по статье.

Некоторые особенности полученных данных

1. Среди выложенных в ГАС «Правосудие» решений, которые должны относиться к статье 13.11, встречаются решения по статье 13.11.1 КоАП РФ за распространение информации о свободных рабочих местах или вакантных должностях, содержащей ограничения дискриминационного характера, которые мы не использовали, т.к. данная статья не относится к предмету исследования. И в целом зачастую при применении фильтра в ГАС «Правосудие» по определенной статье среди записей попадаются судебные дела по другим статьям, например, за нарушения правил дорожного движения.
2. При сравнении количества записей в ГАС «Правосудие» по делам статей главы 13 КоАП РФ (2116 судебных решений) с данными официальной статистики Судебного департамента РФ (2636 решений) за 2019 и 2020 годы становится очевидным, что в государственную систему вносят меньше судебных решений, чем их реально было вынесено (видимо, вносят с определённым запозданием).
3. В ходе исследования обнаружено, что в системе «Правосудие» записи судебных дел дублируются: в некоторых записях полностью совпадают номера дел, наименование судов и другие характеристики. Больше всего таких дублирующихся записей по статье 13.11 – их около 4% от общего числа записей по этой статье.
4. Еще одна особенность ГАС «Правосудие» - отсутствие в ней судебных актов по существенной части записей. Соответственно, установить суть нарушения, которое послужило причиной возбуждения дела, невозможно. Чтобы выделить судебные дела по интересующим нас тематикам, мы **сгруппировали ряд судебных решений**: относили к одному правонарушению (факту) несколько записей в ГАС «Правосудие» о состоявшихся судебных заседаниях, судебных делах, включая, например, обжалование решений и заседания с разными ответчиками **по одному инциденту**.
5. Записи в ГАС «Правосудие» за рассматриваемый период пополняются с небольшой периодичностью. Например, когда мы начинали исследование, ГАС «Правосудие» по статье 13.11 ч.1 выдавала 1908 записей, спустя 2 месяца – всего на три записи больше, то есть 1911 записей.

Наказания за нарушения

В данном разделе мы приводим штрафы за нарушение статей Кодекса РФ об административных правонарушениях в текущей редакции и не рассматриваем историю внесения поправок к статьям и изменения сумм штрафов.

В текущей редакции КоАП, в отношении суммы штрафов действующей и в 2019-2020 гг., за нарушение положений федерального закона №152 ФЗ ("О персональных данных") согласно ч.1 статьи 13.11 КоАП за обработку персональных данных в случаях, не предусмотренных законодательством Российской Федерации в области персональных данных, либо обработку персональных данных, несовместимую с целями сбора персональных данных, нарушитель – частное лицо – может получить предупреждение или штраф в размере от 2 тыс. до 6 тыс. руб. При этом штраф для должностного лица составляет от 10 тыс. до 20 тыс. руб., а для юридического лица – от 60 тыс. до 100 тыс. руб. Что касается ч.7 статьи 13.11, административный штраф должностному лицу составит от 6 до 12 тысяч рублей.

В целях обеспечения информационной безопасности были внесены поправки к Федеральному Закону № 242, обязующие компании обрабатывать и хранить персональные данные россиян с использованием баз данных, размещенных на территории РФ. Обязанности по локализации обработки персональных данных распространяются и на иностранных операторов при условии использования доменного имени, связанного с РФ или его субъектами, а также при наличии русскоязычной версии сайта. Поправки вступили в силу 1 сентября 2015 года, однако ответственность за персональные данные была установлена только в 2019 году. За нарушение закона в части локализации предусмотрено наказание в виде штрафа для юридических лиц в размере до 6 млн рублей (ч. 8 ст. 13.11 КоАП РФ), в случае повторного нарушения – до 18 млн рублей (ч. 9 ст. 13.11 КоАП РФ).

Часть 1 статьи 13.12 КоАП РФ за нарушение условий, предусмотренных лицензией на осуществление деятельности в области защиты информации, подразумевает наложение административного штрафа на граждан в размере от 1000 до 1500 рублей, на должностных лиц – от 1500 до 2000 рублей, на юридических лиц – от 15 до 20 тысяч рублей.

Нарушение статьи 13.13 КоАП РФ, если применяется часть 1 статьи, влечет за собой наложение административного штрафа на граждан в размере от 500 до 1000 рублей, на должностных лиц – от 2 до 3 тысяч рублей с возможной конфискацией средств защиты информации, на юридических лиц – от 10 тысяч до 20 тысяч рублей с возможной конфискацией средств защиты информации. Часть 2 статьи 13.13 относится к нарушениям, связанным с использованием и защитой информации, составляющей государственную тайну, и штрафы здесь выше: штраф для должностных лиц составит от 4 до 5 тысяч рублей, а на юридических лиц – от 30 до 40 тысяч рублей, а также возможна конфискация созданных без лицензии средств защиты информации.

Статья 13.14 КоАП РФ за разглашение информации с ограниченным доступом предусматривает наложение наибольших административных штрафов: на граждан в размере от 5 до 10 тысяч рублей, на должностных лиц – от 40 до 50 тысяч рублей или дисквалификацию на срок до трех лет, а на юридических лиц – от 100 до 200 тысяч

рублей. Адвокаты, согласно этой статье, несут административную ответственность как должностные лица.

С 27 марта 2021 года вступили в силу положения федерального закона №19-ФЗ от 24.02.2021, согласно которым были увеличены штрафы за нарушение законодательства РФ в области персональных данных, предусмотрены штрафы за повторные нарушения и исключена мера административного наказания в виде предупреждения по некоторым пунктам. Вместе со штрафами увеличен срок давности привлечения к административной ответственности за нарушения в области персональных данных с 3 месяцев до 1 года (п. 1 ст. 4.5). В случае признания административного правонарушения длящимся, срок исчисляется со дня обнаружения данного правонарушения (п. 2 ст. 4.5), то есть со дня, когда должностное лицо, уполномоченное составлять протокол об административном правонарушении, выявило факт его совершения.

11 июня 2021 г. был опубликован подписанный президентом России Владимиром Путиным закон об увеличении штрафов за разглашение персональных данных до 50 тыс. рублей. Согласно документу, увеличиваются штрафы за разглашение «информации ограниченного доступа» для граждан (на данный момент они составляют от 500 рублей до 1 тыс. рублей) до 10 тыс. рублей, а также для должностных лиц (в настоящее время — от 4 тыс. до 5 тыс. рублей) – до 50 тыс. рублей. Уточняется, что под данное определение попадают различная конфиденциальная информация, включая коммерческую и банковскую тайны, тайну связи.

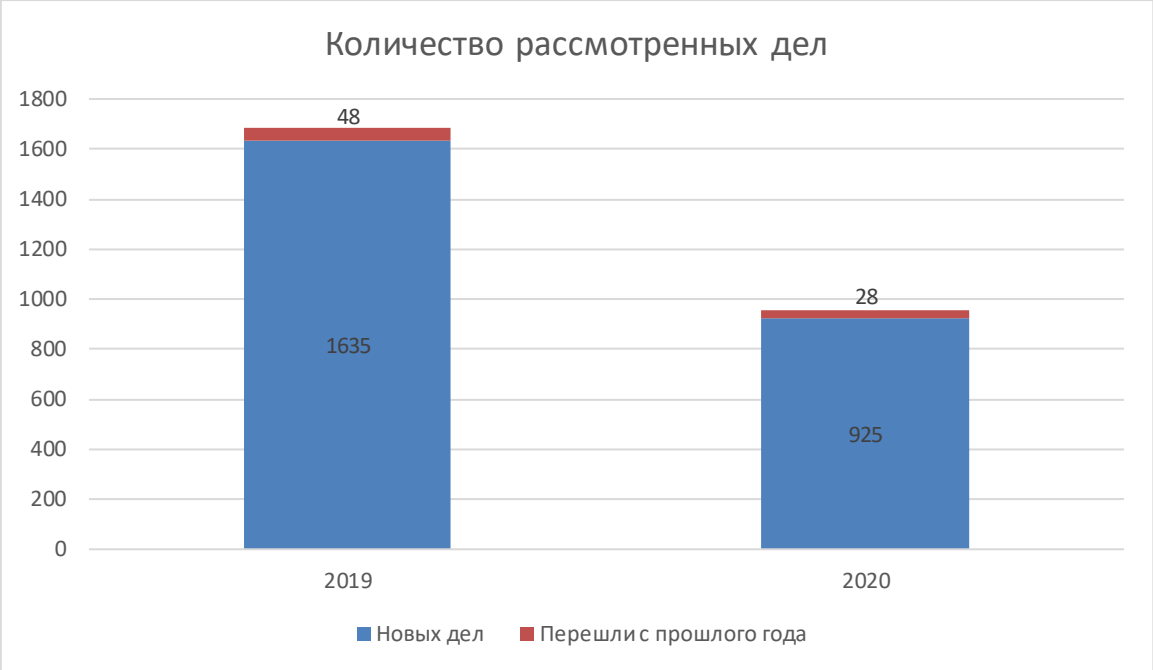
Официальная статистика

Официальная статистика Судебного департамента при Верховном суде Российской Федерации включает общее количество дел по статьям 13.11, 13.12, 13.13, 13.14 и 13.11.1 КоАП РФ без возможности определить количество дел по каждой отдельной статье. Статья 13.11.1, как ранее было сказано, исключена из исследования, т.к. она связана с распространением информации о свободных рабочих местах или вакантных должностях, содержащей ограничения дискриминационного характера, и не относится к предмету исследования.

Согласно официальной статистике, по приведенным выше статьям:

- в 2019 году было рассмотрено **1683** дела: 48 дел, перешедших с 2018 года, и 1635 из 1686 поступивших в 2019;
- в 2020 году были рассмотрены **953** дела: 28 дел, перешедших с 2019 года, и 925 из 954 поступивших в 2020 году.

В 2020 году количество рассмотренных дел снизилось на 43%. Это может быть связано с тем, что, как показал анализ данных, большинство подобных дел связано с так называемыми «бумажными нарушениями», которых стало меньше выявляться при переходе большинства предприятий на дистанционную работу.



Всего за 2019-2020 гг. по статьям 13.11, 13.12, 13.13, 13.14 и 13.11.1 КоАП РФ судами Российской Федерации было рассмотрено 2636 дел.

Также некоторые статистические данные можно извлечь из отчетов о деятельности Роскомнадзора (РКН) на официальном сайте.

В 2019 году, согласно источнику, Роскомнадзором и его территориальными органами рассмотрено 43 045 жалоб на действия операторов, осуществляющих незаконную обработку персональных данных. По результатам рассмотрения жалоб граждан доводы заявителей подтвердились только в 7,2% случаев.

Территориальными органами Роскомнадзора за 2019 год составлено и направлено в суды 5437 протоколов об административных правонарушениях операторов ПДн. По итогам их рассмотрения наложено административных штрафов на сумму 4 751 130 рублей. **Надзорные органы, в основном, подавали судебные иски в отношении Интернет-ресурсов, которые незаконно распространяли базы данных с персональными данными граждан Российской Федерации.**

По статье 13.11 КоАП РФ Роскомнадзором и его территориальными органами было составлено 218 протоколов об административных правонарушениях, по результатам рассмотрения которых было наложено административных штрафов на общую сумму 1 214 000 рублей.

С начала функционирования в 2015 году реестра нарушителей прав субъектов персональных данных по результатам рассмотрения исковых заявлений, поданных Роскомнадзором и его территориальными органами, судами принято 507 положительных решений. Данных о распределении таких решений по статьям КоАП РФ и годам (в частности, 2019 и 2020 годам) и о судебной практике на сайте Роскомнадзора не приводится.

По данным РКН, в 2020 году к ним поступило 308 обращений в форме жалоб в рамках административного производства. Расшифровка по статьям этих обращений на сайте не представлена. Но отмечено, что более 65% обращений граждан поступает в

территориальные управления Роскомнадзора, расположенные в Центральном Федеральном округе, и порядка 30% относятся к сфере защиты персональных данных (42 255 обращений).

Результаты исследования

В ходе исследования были просмотрены свыше 2 тысяч записей (2 116) в ГАС «Правосудие» о судебных решениях по статьям 13.11-13.14. И только часть из них оказалась связана с защитой информации и, в частности, с безопасностью персональных данных. Напомним, что несколько записей о судебных решениях из ГАС «Правосудие» мы группировали в одно судебное дело, если: 1) решение суда было обжаловано; 2) несколько физических лиц или несколько сотрудников одного юридического лица допустили одно нарушение в отношении одного и того же лица/группы лиц. Таким образом, **была сформирована база из 270 судебных дел по выбранным для исследования статьям**: 13.11 ч.1, 7 и 8, 13.12 ч.1, 13.13 и 13.14.
Получилась следующая конверсия количества записей в ГАС «Правосудие» в список судебных дел (то есть выделены дела по факту нарушения вне зависимости от количества их рассмотрений, Таблица 5):

- 10% записей по статье 13.11 относятся к судебным делам по ч.1, 7 и 8;
- 12,5% для записей по ч.1 статьи 13.12;
- по 38% записей были собраны в судебные дела по статьям 13.13 и 13.14.

Таблица 5. Количество выделенных судебных дел

Номер статьи	**Количество записей в ГАС «Правосудие» от общего количества записей по статьям 13.11-13.14**		**Количество выделенных судебных дел и его отношение к количеству записей в ГАС «Правосудие»**	
13.11	1911 (все части)	90 %	195 (только ч. 1, 7 и 8)	10 %
13.12 ч.1	8	0,4 %	1	12,5 %
13.13	13	0,6%	5	38 %
13.14	184	9 %	69	38 %
Всего	**2116**		**270**	

Посмотрим на распределение выделенных и найденных нами судебных дел по статьям. Большая часть судебных дел, а именно 195 дел, или в процентном соотношении 72%, относится к статье 13.11 ч.1, 7 и 8 (Таблица 6). Вторая наиболее часто используемая в судебной практике по защите информации статья – это статья 13.14 (25,6 % от общего количества рассмотренных дел). Наименее часто используемая статья – 13.12 ч.1: по ней было обнаружено только одно дело, что составило 0,4% от общего количества.

Таблица 6. Соотношение по статьям судебных дел к общему числу

Статья	Количество судебных дел	Доля от общего количества, %
13.11	195	72
13.14	69	25,6
13.13	5	2
13.12 ч.1	1	0,4

Далее рассмотрим результаты исследования по каждой отдельной статье.

Статья 13.11 – Нарушение законодательства Российской Федерации в области персональных данных

Для исследования мы выбрали ч.1, 7 и 8 статьи 13.11, так как именно они, по нашим ожиданиям, должны были содержать дела, относящиеся к нарушениям требований к безопасной обработке персональных данных с применением средств автоматизации.
В итоге ожидания оправдались не полностью.
Часть записей в ГАС «Правосудие», относящихся к статье 13.11 КоАП РФ, не содержат судебные акты, поэтому установить суть рассматриваемых дел невозможно. Наличие судебных актов мы проверили на сайтах соответствующих региональных судов, но и в этих источниках текстов судебных актов не содержалось. Таких дел порядка 8% от общего числа представленных на сайте государственной системы.
Из остальных 92% записей нами было выделено:

- 182 судебных дела, рассмотренных по части 1;
- 8 дел – по части 7;
- 5 дел – по части 8 статьи 13.11 КоАП РФ.

Таблица 6. Соотношение компьютерных дел к общему числу дел

Номер статьи	Количество судебных дел	Количество дел, связанных с автоматизированной обработкой данных, и доля от количества дел по статье	Доля дел по статье от общего количества дел, связанных с автоматизированной обработкой данных
13.11 ч.1	182	48 26%	52%
13.11 ч.7	8	5* 63%	5%
13.11 ч.8	5	5 100%	5%
13.12 ч.1	1	0 -	-
13.13	5	5 100%	5%
13.14	69	30 44%	33%
Всего	270	93	100%

*Оставшаяся часть записей не содержит судебные акты и установить суть дела не представляется возможным

Только 34% судебных дел по вышеперечисленным статьям суммарно относятся к нарушениям с применением средств автоматизации (распространение информации в сети Интернет, через мессенджеры и т.д.). Перейдем к рассмотрению каждой выбранной части статьи 13.11.

Статья 13.11 ч.1 – Обработка персональных данных в случаях, не предусмотренных законодательством Российской Федерации в области персональных данных, либо обработка персональных данных, несовместимая с целями сбора персональных данных

Часть 1 статьи 13.11 подразумевает рассмотрение дел о нарушениях, касающихся обработки персональных данных в случаях, не предусмотренных законодательством РФ в области ПДн, либо обработки ПДн, несовместимой с целями их сбора. По нашим предположениям в начале этого исследования, судебные дела именно по этой статье могли относиться к нарушениям с использованием средств автоматизации и к утечкам информации (ПДн), но фактически из 182 дел только 48 дел (или 26% от общего количества) затрагивают такие нарушения (Таблица 6). Все остальные дела относятся к нарушениям при работе с бумажными носителями информации. Например, снятие и/или несоответствующее хранение ксерокопии паспорта.

Преобладающая часть судебных дел по ч.1 статьи 13.11 КоАП РФ была рассмотрена в регионах. Всего 6% (11 дел) рассматривали в судебных инстанциях Москвы, причем два дела направили из региональных инстанций для обжалования вынесенных решений.

В 65 случаях из 182, то есть в 36%, Роскомнадзор или органы прокуратуры отказали в возбуждении дела по обращениям, после чего заявители обращались в суд для обжалования постановлений об отказе. Практически все жалобы не были удовлетворены судом по причине отсутствия состава преступления или по истечению срока давности административного нарушения. Одно и то же решение об отказе в возбуждении дела, как правило, обжаловали дважды, иногда по четыре-пять раз.

Среди ответчиков доли физических и юридических лиц равны – 50% на 50%. В восьми случаях ответчиками были юридическое лицо и его сотрудник как физическое лицо. Среди физических лиц большинство (61%) несли ответственность за нарушение как должностные лица.

Заявителями чаще выступают физические лица, кроме случаев, когда инициаторами возбуждения дел являются не только сами пострадавшие от распространения их персональных данных, но и государственные органы (Роскомнадзор или Прокуратура) при проведении проверок (в 70 случаях из 182 дел – 38%). Истец-рекордсмен из Ивановской области направил иски к 24 различным лицам, включая юридические и относящиеся к ним должностные лица, а также физические лица. Среди них как коммерческие компании (например, Совкомбанк и М.Видео), так и государственные организации (такие как Управление Роспотребнадзора, Управление федерального казначейства, отделение МВД и т.п.). Доля дел, приходящихся на этого истца, составляет 13% и могла бы быть еще выше, если бы мы все решения, связанные с многочисленными обжалованиями по одному инциденту, не объединили в одно судебное дело.

Самые крупные штрафы, назначенные нескольким юридическим лицам (все из них коммерческие компании) по ч.1 статьи 13.11, составили 30 тыс. рублей. Эти нарушения

касались звонков коллекторов и сотрудников банка заявителям с требованиями погасить задолженность перед банками. Также это были звонки с рекламными целями. ПДн были получены официально или от заявителя в процессе получения кредита или из банка в процессе переуступки долга.

Явной корреляции между тяжестью нарушения и величиной наказания не прослеживается.

Так, злоумышленнику, который скопировал из ГАС «Выборы» на съемный носитель данные избирателей одного из участков в республике Татарстан, назначили штраф в размере 1500 рублей (кстати, даже такой штраф нарушитель пытался оспорить, причем четырежды, но безрезультатно). А за звонки в рекламных целях суды назначали административные штрафы от 5 до 30 тысяч рублей.

Статья 13.11 ч.7 – Невыполнение оператором, являющимся государственным или муниципальным органом, предусмотренной законодательством Российской Федерации в области персональных данных обязанности по обезличиванию персональных данных либо несоблюдение установленных требований или методов по обезличиванию персональных данных

Пять из восьми найденных в ГАС «Правосудие» записей о судебных заседаниях по ч.7 статьи 13.11 КоАП РФ относятся к административным правонарушениям с применением средств автоматизации. Среди таких нарушений, например, размещение на сайте администрации поселения сведений о доходах должностных лиц или на сайте детского сада приказа о зачислении учеников. Во всех пяти случаях в результате судебных заседаний было вынесено решение о назначении наказания в виде предупреждения.

Для оставшихся трех записей невозможно идентифицировать состав нарушения, так как судебные акты в общем доступе не выложены.

100% дел по ч.7 статьи 13.11 были рассмотрены в региональных судах и ни одного – в Москве.

Статья 13.11 ч.8 – Невыполнение оператором при сборе персональных данных, в том числе посредством информационно-телекоммуникационной сети "Интернет", предусмотренной законодательством Российской Федерации в области персональных данных обязанности по обеспечению записи, систематизации, накопления, хранения, уточнения (обновления, изменения) или извлечения персональных данных граждан Российской Федерации с использованием баз данных, находящихся на территории Российской Федерации

Согласно поправкам к Федеральному Закону № 242-ФЗ, компании обязаны обрабатывать и хранить персональные данные россиян с использованием баз данных, размещенных на территории РФ. Поправки вступили в силу 1 сентября 2015 года, однако ответственность была установлена только со 2 декабря 2019 года. За нарушение закона в части локализации (требования ч. 8 ст. 13.11 КоАП РФ) предусмотрено наказание в виде штрафа для юридических лиц в размере до 6 млн рублей.

На сегодня хранение персональных данных российских пользователей локализовали порядка 600 представительств зарубежных компаний в РФ, среди которых Apple, Microsoft, LG, Samsung, PayPal, Booking и другие. Тем не менее, ряд крупнейших

иностранных компаний проигнорировали требования закона по обеспечению информационной безопасности данных граждан РФ.

Еще в 2015 году Роскомнадзор начал проверки компаний на предмет нарушения информационной безопасности и направил компаниям официальные уведомления о необходимости соблюдения законодательства РФ в области персональных данных. В связи с отсутствием официального ответа на уведомление таких иностранных компаний, как Twitter и Facebook, Роскомнадзор в 2019 году был вынужден инициировать в отношении них административное производство.

13 февраля 2020 года мировым судьей Таганского районного суда города Москвы компании Твиттер Инк. и Фейсбук Инк. за отказ локализовать персональные данные россиян на территории России были признаны виновными в правонарушениях, предусмотренных ч. 8 ст. 13.11 КоАП. Каждой корпорации было назначено наказание в виде административного штрафа в размере 4 млн рублей. Компания Facebook штраф оплатила, в то время как Twitter отказался выполнять требование и подал апелляционную жалобу 28 февраля 2020 года. Суд жалобу отклонил.

В июле 2021 года тот же суд признал компанию Google виновной в совершении административного правонарушения по ч. 8 ст. 13.11 КоАП РФ. Штраф в 3 млн руб. стал первым для Google по этой статье.

Затем 26 августа 2021 года Таганский районный суд Москвы рассмотрел административные протоколы, составленные Роскомнадзором в отношении американских интернет-сервисов Facebook, WhatsApp и Twitter, согласно предписанию по обеспечению информационной безопасности не локализовавших на территории РФ базы данных российских пользователей к 1 июля 2021 года. **Решением суда WhatsApp был назначен штраф в размере 4 млн рублей по ч. 8 ст. 13.11 КоАП РФ. А компаниям Facebook и Twitter придется выплатить 15 млн рублей и 17 млн рублей, соответственно, за повторные нарушения требований о локализации персональных данных по ч. 9 ст. 13.11 КоАП РФ.**

Этим летом Госдума РФ одобрила законопроект, обязывающий крупные зарубежные ИТ-компании с ежедневной аудиторией в РФ от 500 тыс. человек открывать свои представительства в России. Такие организации должны будут с 1 января 2022 года создать филиалы, открыть представительства или учредить российские юридические лица, которые в полном объеме будут представлять интересы головных компаний во взаимодействии с Роскомнадзором.

В сентябре судебные приставы пришли в российский офис американской корпорации Google, чтобы взыскать неоплаченные штрафы, выписанные компании. Адвокат компании сообщил приставам, что они пришли в офис ООО Google, а претензии суда касаются компании Google LLC, которая находится в США. Российские власти рассчитывают, что новый законопроект позволит избежать таких ситуаций в дальнейшем[1].

[1] Информация о вышеприведенных судебных делах приведена исходя из публикаций в средствах массовой информации, а также в новостях на сайте Таганского районного суда г. Москвы. В ГАС «Правосудие» информации

В ГАС «Правосудие» была обнаружена запись об одном судебном деле, и оно возбуждено, в отличие от описанных выше, в отношении должностного лица, а не юридического. В ходе проверки Роскомнадзором Центра немецкого языка в Москве было обнаружено, что Центр передает персональные данные лиц, сдавших экзамен по немецкому языку, своим партнерам – Немецкому культурному центру имени Гете при Германском Посольстве в г. Москве, и Гете-Институту в г. Мюнхене (Германия). К ответственности привлекли директора Центра немецкого языка и назначили ей наказание в виде штрафа в размере 50 тысяч рублей. Мы писали об этом в своём отчёте об утечках за 2020 год.

Статья 13.12 ч.1 – Нарушение условий, предусмотренных лицензией на осуществление деятельности в области защиты информации (за исключением информации, составляющей государственную тайну)

По ч.1 статьи 13.12 в записях в ГАС «Правосудие» было найдено только одно судебное решение, касавшееся жалобы гражданина РФ на отказ МВД в возбуждении дела в отношении неустановленного лица, которое использовало его (заявителя) персональные данные для направления обращения в прокуратуру республики Марий Эл по вопросу водоснабжения. Заявитель не согласна с определением МВД, указывая на то, что в действиях неустановленного лица имеется состав нарушения, предусмотренного статьей 13.11 КоАП РФ, а не статьей 13.12 КоАП РФ как указал административный орган. Суд удовлетворил жалобу заявителя. Данных о дальнейшем рассмотрении нарушения в суде в системе ГАС «Правосудие» не обнаружено. Таким образом, по статье 13.12 ч.1 за 2019 и 2020 году, согласно ГАС «Правосудие», была только одна запись дела, которое по итогам исследования судебного акта не касается соблюдения лицензионных требований.

Фактически по статье 13.12 ч.1 (за нарушение условий, предусмотренных лицензией на осуществление деятельности в области защиты информации) в 2019-2020 годах в ГАС «Правосудие» судебных актов не обнаружено.

Статья 13.13 – Незаконная деятельность в области защиты информации

Записи в ГАС «Правосудие» за 2019-2020 гг. о делах по нарушениям, связанных с незаконной деятельностью в области защиты информации, содержат информацию о пяти судебных делах. Для трех из них представлены судебные акты, по которым можно судить, что нарушители осуществляли деятельность по оказанию услуг по передаче в налоговые и другие государственные органы отчетность без лицензии в области шифрования информации. Все они были инициированы ФСБ России и ответчиком выступало должностное лицо, ответственное за деятельность компании в сфере оказания услуг по составлению и предоставлению в налоговые и иные государственные органы отчетности по телекоммуникационным каналам связи с использованием

об этих судебных делах не представлено. Эти четыре дела возбуждены в отношении иностранных юридических лиц и рассмотрены в одном и том же районном суде в Москве.

шифровального (криптографического) средства без соответствующего разрешения (лицензии) в области шифрования информации.

Для еще двух дел судебные акты не выложены в открытый доступ ни в ГАС «Правосудие», ни на сайтах судов. Тем не менее, по косвенным признакам, таким как тип заявителя по делу (возбуждение дел во этих случаях также инициировала ФСБ России) и тип решения о виновности и назначении штрафа (состав нарушения относился к применяемой статье), мы можем предположить, что эти дела схожи с теми, для которых акты доступны для прочтения и относятся к делам по нарушениям с применением средств автоматизации.

Все пять дел, относящихся к статье 13.13, были рассмотрены в региональных судах и ни одного – в Москве.

Статья 13.14 – Разглашение информации с ограниченным доступом

По статье 13.14 из 184 записей в ГАС «Правосудие» нами было выделено 69 судебных дел, 30 из которых (43%) относятся к нарушениям с применением средств автоматизации. По виду нарушения дела по статье 13.14 достаточно разнообразны: это и передача персональных данных в группу мессенджера WhatsApp, и предоставление сведений без согласия заявителя в суды и Роскомнадзор для разбирательств, а также размещение на сайтах учебных заведений паспортов безопасности. Последние инициированы прокуратурой в ходе проверок ряда организаций в различных регионах. Суды по всем 11 делам назначили должностным лицам учреждений наказания в виде административного штрафа в размере 4000 рублей.

В качестве ответчика в судебных актах, обнаруженных в ГАС «Правосудие» за исследуемый период, в абсолютном большинстве случае выступали сотрудники организаций или должностные лица – в 61 случае из 69 (88%).

Только 3 дела из 69 (4%) были рассмотрено в судах Москвы и Московской области, соответственно, 66 дел (96%) – в региональных судах.

Заключение и выводы

Доли дел с нарушениями, в которых применялись средства автоматизации и без их применения

1. В 34% случаях по статьям 13.11-13.14 КоАП РФ в 2019-20 гг. были рассмотрены дела, связанные с правонарушениями с применением автоматизированных систем обработки персональных данных и другой конфиденциальной информации. Таким образом, **более трети правонарушений из нашей выборки были совершены с помощью сети «Интернет», компьютеров, телефонов и других систем**, что говорит о недостаточно высоком уровне информационной безопасности организаций. В остальных случаях утечки конфиденциальной информации произошли через неавтоматизированные каналы обработки данных.

1.1. В резюме нашего исследования хотели бы отметить, что по статьям КоАП РФ мы ожидали увидеть большое количество судебных дел, связанных с нарушениями с применением различных средств автоматизации, в том числе утечками информации. Однако, мы выяснили, что **суды чаще рассматривают дела, касающиеся неавтоматизированной обработки персональных данных и другой конфиденциальной информации**. К примеру, размещение персональных данных жителей-должников в подъездах по адресу их проживания на бумажных объявлениях или использование конфиденциальной информации противоположной стороны в судебных заседаниях, полученной по запросу в ведомствах.

Во всех изученных делах доступ к раскрытым персональным данным был правомерным.

1.2. Интересно, что распределение дел по каналам обработки ПДн неравномерно по статьям:

- по части 1 статьи 13.11 (за обработку ПДн в случаях, не предусмотренных законодательством РФ в области ПДн, либо обработку ПДн, несовместимую с целями сбора ПДн) – **26%** дел;
- по части 7 статьи 13.11 – **более 60%**.

А в случае применения части 8 статьи 13.11[2] и статьи 13.13[3] судебных дел по правонарушениям с использованием средств автоматизации – уже **100%**.

По статье 13.14 КоАП РФ[4] дел такого типа чуть меньше половины – **44%**.

[2] Невыполнение оператором при сборе персональных данных, в том числе посредством информационно-телекоммуникационной сети "Интернет", предусмотренной законодательством Российской Федерации в области разглашение информации с ограниченным доступом данных обязанности по обеспечению записи, систематизации, накопления, хранения, уточнения (обновления, изменения) или извлечения персональных данных граждан Российской Федерации с использованием баз данных, находящихся на территории Российской Федерации

[3] Незаконная деятельность в области защиты информации

[4] Разглашение информации с ограниченным доступом

Единственным исключением является часть 1 статьи 13.12, по которой, исходя из данных ГАС «Правосудие», дел по таким нарушениям найдено не было.

2. Типы судебных решений

Судебные решения по своему типу можно разделить на три категории:

1. Отказ в возбуждении дела – 32%;
2. Назначение наказания – 56%;
3. Другое (перевод дела в другую инстанцию, возвращение дела заявителю и т.п.) – 12%.

Решения как с отказом от возбуждения дела, так и по назначению наказания заявители многократно обжалуют в различных инстанциях. **Среднее число обжалований одного решения – 2 раза.**

3. Особенности

Интересной особенностью изученных нами судебных дел является то, что во всех них доступ к раскрытым персональным данным и другой конфиденциальной информации был правомерным, то есть персональные данные были раскрыты сотрудниками[5].

По всей выборке судебных дел в большинстве случаев (**в 65% дел**) **в качестве ответчиков** в 2019-2020 г. по статьям 13.11-13.14 КоАП РФ **выступали физические лица, включая должностных лиц**. В 24% дел ответчиками были коммерческие компании и в 11% – государственные организации. **Но есть случаи, когда по одному и тому же нарушению возбуждают несколько дел**: в отношении юридического лица (компании или госорганизации) и должностного лица, то есть человека, наделенного организационно-распорядительными или административно-хозяйственными функциями. Также рассматривают дела и в отношении нескольких физических лиц, допустивших нарушения в сфере использования конфиденциальной информации.

4. Наказания

Наказания за административные правонарушения по статьям 13.11-13.14 в 2019-2020 годах: **самый крупный штраф физическому лицу** был по части 8 статьи 13.11, он был назначен должностному лицу за передачу персональных данных россиян иностранной организации и составил 50 тысяч рублей. **В случае юридического лица как ответчика**

[5] Ответчиками в судебных делах выступали сотрудники и должностные лица, а не злоумышленники, получившие доступ к данным нелегально извне. Очевидно, что дела, касающиеся несанкционированного доступа к конфиденциальной информации со стороны хакеров или других нарушителей, суды рассматривают по статьям Уголовного кодекса РФ (тема следующего исследования).

самый крупный штраф – 17 млн рублей – назначен за повторное нарушение статьи о локализации персональных данных россиян в Российской Федерации.
Самый крупный оплаченный штраф – 4 млн рублей – компания Facebook внесла за отказ от хранения персональных данных российских пользователей на серверах в РФ.
Но необходимо понимать, что выплата штрафа не освобождает от обязанности устранить нарушение и выполнить требования, изложенные в предписании, составленном по результатам проверки. Повторное наказание будет гораздо серьёзнее и все равно сохранится требование устранить нарушение.

5. География

Географическое распределение судов, в которых в 2019-2020 гг. рассматривали дела по статьям 13.11-13.13 КоАП РФ: 93% дел были рассмотрены в регионах и только 7% – в Москве и Московской области.
100% дел по части 7 статьи 13.11 были рассмотрены в региональных судах, не в Москве.

Общие выводы

1. Несмотря на наличие федеральных законов и статей Кодекса об административных правонарушениях, относящихся к защите информации, в т.ч. персональных данных, на текущий момент судебная практика в этой сфере неразвита. Причиной этому может служить отсутствие государственных требований и практики информирования пострадавших и государственных органов об утечках конфиденциальной информации, **в связи с чем необходимо установление административной и уголовной ответственности в отношении должностных лиц за неинформирование о подобных инцидентах.**

2. Ввиду редкости обращений в суд лицами, пострадавшими от утечек персональных данных, и низкими штрафами за большинство нарушений правил безопасной обработки ПДн, ситуация в этой сфере пока плохо контролируема.

По окончании 2021 и поступлении новых данных мы планируем изучить, как изменилась ситуация и повлияло ли на неё повышение штрафов за нарушения, связанные с обработкой персональных данных.

Мониторинг утечек на сайте InfoWatch

На сайте Экспертно-аналитического центра InfoWatch регулярно публикуются отчеты по утечкам информации и самые громкие инциденты с комментариями экспертов InfoWatch.
Следите за новостями утечек, новыми отчетами, аналитическими и популярными статьями на наших каналах:

- Почтовая рассылка
- Facebook
- Telegram

Экспертно-аналитический центр InfoWatch
www.infowatch.ru/analytics

Глоссарий

ГАС «Правосудие» - Государственная автоматизированная система Российской Федерации.
Запись в ГАС «Правосудие» - запись на сайте https://bsr.sudrf.ru/, включающая информацию об одном судебном решении.
Судебное дело – совокупность судебных решений всех инстанций, которые относятся к одному факту нарушения кодекса об административных нарушениях.
Нарушение с применением средств автоматизации – нарушение Кодекса об административных нарушениях РФ с использованием компьютера, средств связи и сети Интернет.

Канал утечки информации – способ утечки информации; предполагает сценарий, в результате выполнения которого потерян контроль над информацией, нарушена ее конфиденциальность.
На данный момент аналитики InfoWatch выделяют 8 самостоятельных каналов утечки (далее - классификаторы):

- «Оборудование (сервер, СХД, ноутбук, ПК)», – компрометация информации в ходе обслуживания, в результате кражи или потери оборудования.
- «Мобильные устройства» – утечка информации вследствие нелегитимного использования мобильного устройства/кражи мобильного устройства (смартфоны, планшеты). Использование данных устройств рассматривается в рамках парадигмы BYOD.
- «Съемные носители» – потеря/кража съемных носителей (CD, USB, карты памяти и др.).
- «Сеть (сетевой канал)» – утечка через браузер (отправка данных через веб-интерфейс в личную почту, формы ввода в браузере), нелегитимное использование внутренних ресурсов сети, FTP, облачных сервисов, нелегитимная публикация информации на веб-сервисе.
- «Электронная почта» – утечка данных через корпоративную электронную почту.
- «Бумажные документы» – утечка информации вследствие неправильного хранения/утилизации бумажной документации, через печатающие устройства (отправка на печать и кража/вынос конфиденциальной информации на бумаге).
- «IM –сервисы мгновенных сообщений» - утечка информации при передаче ее голосом, в текстовом виде, а также через видео - при использовании мессенджеров.
- «Не определено» - категория, используемая в случае, когда сообщение об инциденте в СМИ не позволяет точно определить канал утечки.

Компьютерная атака – целенаправленное воздействие программных и (или) программно-аппаратных средств на объекты критической информационной инфраструктуры, сети электросвязи, используемые для организации взаимодействия таких объектов, в целях нарушения и (или) прекращения их функционирования и (или) создания угрозы безопасности обрабатываемой такими объектами информации [Федеральный закон от 26.07.2017 N 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации»].
Компьютерный инцидент – факт нарушения и (или) прекращения функционирования объекта критической информационной инфраструктуры, сети электросвязи, используемой для организации взаимодействия таких объектов, и (или) нарушения безопасности обрабатываемой таким объектом информации, в том числе произошедший в результате компьютерной атаки [Федеральный закон от 26.07.2017 N 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации»].
Конфиденциальность информации – обязательное для выполнения лицом, получившим доступ к определенной информации, требование не передавать такую информацию третьим лицам без согласия ее обладателя [Федеральный закон «Об информации, информационных технологиях и о защите информации» № 149-ФЗ, п.7 ст.2].
Конфиденциальная информация – сведения конфиденциального характера, в соответствии с Указом Президента РФ от 6 марта 1997 г. №188.

В данном отчете (исследовании) авторы относят к таким сведениям информацию, доступ к которой осуществляется строго ограниченным и известным кругом лиц с условием, что информация не будет передана третьим лицам без согласия владельца информации. Помимо персональных данных, это платежная информация, коммерческие секреты и ноу-хау, а также государственные и военные секреты. В некоторых случаях при анализе полученных сведений определить тип конфиденциальной информации не представляется возможным, поэтому она относится в категории «не определено».

Нарушитель информационной безопасности организации (нарушитель) – физическое лицо или логический объект, случайно или преднамеренно совершивший действие, следствием которого является нарушение информационной безопасности организации [ГОСТ Р 53114-2008, статья 3.3.5].

В БДУ ФСТЭК России bdu.fstec.ru приведены следующие виды нарушителей/ источников угроз:

- внутренний нарушитель (потенциал низкий, средний, высокий);
- внешний нарушитель (потенциал низкий, средний, высокий).

В данном отчете (исследовании) к категории «нарушитель» авторы относят лицо, которое по ошибке или осознанно (с умыслом – злоумышленник) совершило определенные запрещенные действия, повлекшие утечку информации.

InfoWatch различает два вида нарушителей – «внешний нарушитель» и «внутренний нарушитель», а также шесть категорий нарушителей:

- Внешний нарушитель – Хакер/неизвестное лицо: взломщики компьютерных сетей, в том числе представляющие организованную киберпреступность; владельцы хакерского инструментария (библиотек); взломщики, действующие в политических и социальных целях, - хактивисты; сотрудники иностранных разведок и армий; похитители оборудования с конфиденциальной информацией.
- Рядовой сотрудник.
- Топ-менеджер (руководитель).
- Системный администратор.
- Подрядчик: сторонние исполнители работ по заказу компании, партнеры и внештатные сотрудники.
- Бывший сотрудник.

В рамках исследования топ-менеджеров, системных администраторов, а в отдельных случаях и подрядчиков авторы включают в категорию привилегированных пользователей, то есть пользователей, наделенных повышенными правами доступа к информации. Как правило, действия таких пользователей в информационной системе службами информационной безопасности контролируются слабо либо не контролируются.

Иных пользователей корпоративной информационной системы (рядовых сотрудников) авторы относят к непривилегированным, обычным пользователям.

Неправомерный доступ – см. несанкционированный доступ.

Несанкционированный доступ – доступ к информации или к ресурсам автоматизированной информационной системы, осуществляемый с нарушением установленных прав и (или) правил доступа [ГОСТ Р 53114-2008, статья 3.3.6].

Примечания:

1. Несанкционированный доступ может быть осуществлен преднамеренно или непреднамеренно.
2. Права и правила доступа к информации и ресурсам информационной системы устанавливаются для процессов обработки информации, обслуживания автоматизированной информационной системы, изменения программных, технических и информационных ресурсов, а также получения информации о них.

В данном отчете (исследовании) авторы используют также словосочетание «нелегитимный доступ».

Несанкционированное воздействие на информацию – воздействие на защищаемую информацию с нарушением установленных прав и (или) правил доступа, приводящее к утечке, искажению, подделке, уничтожению, блокированию доступа к информации, а также к утрате, уничтожению или сбою функционирования носителя информации [ГОСТ Р 50922-2006, статья 2.6.6]

Правонарушение – неправомерное поведение, запрещенное законом под угрозой наступления ответственности общественно вредное или опасное деяние.

Выделяют: преступление (в рамках УК РФ и УПК РФ), административное правонарушение (в рамках КОАП РФ), налоговое правонарушение (в рамках НК РФ).

В отчетах (исследованиях) авторы используют понятие «правонарушение» как родовое (общее) по отношению к преступлению и административному правонарушению.

Привилегированный пользователь – к таким пользователям InfoWatch относит категории лиц, имеющие расширенные права доступа в информационные системы, полномочия по изменению конфигураций и назначения прав администраторов другим пользователям. К привилегированным пользователям относятся руководители различного уровня, системные администраторы, в некоторых случаях подрядчики и другие категории.

Разглашение информации – несанкционированное доведение защищаемой информации до лиц, не имеющих права доступа к этой информации [ГОСТ Р 53114-2008, статья 3.3.11].

Разглашение информации, составляющей коммерческую тайну, – действие или бездействие, в результате которых информация, составляющая коммерческую тайну, в любой возможной форме (устной, письменной, иной форме, в том числе с использованием технических средств) становится известной третьим лицам без согласия обладателя такой информации либо вопреки трудовому или гражданско-правовому договору [98-ФЗ «О коммерческой тайне» п.9 ст.3]

Событие: Возникновение или наличие определенной совокупности обстоятельств [ГОСТ Р 53114-2008, статья 3.2.8].

Примечания:

1. Характер, вероятность и последствия события могут быть не полностью известны.
2. Событие может возникать один или несколько раз.
3. Вероятность, связанная с событием, может быть оценена.
4. Событие может состоять из невозникновения одного или нескольких обстоятельств.
5. Непредсказуемое событие иногда называют «инцидентом».
6. Событие, при котором не происходит никаких потерь, иногда называют предпосылкой к происшествию [инциденту], опасным состоянием, опасным стечением обстоятельств и т.д.

Утечка информации – неконтролируемое распространение защищаемой информации в результате ее разглашения, несанкционированного доступа к информации и получения защищаемой информации иностранными разведками [ГОСТ Р 53114-2008, статья 3.3.10].

В данном отчете (исследовании) InfoWatch к категории «утечка информации» относится событие, когда в результате умышленных или неумышленных действий внутреннего или внешнего нарушителя обладатель информации ограниченного доступа (компания) утрачивает контроль над этой информацией.

Умышленная (злонамеренная) утечка информации – InfoWatch понимает под ней такую утечку, когда пользователь, работающий с информацией ограниченного доступа, предполагал возможные негативные последствия своих действий, осознавал их противоправный характер, был предупрежден об ответственности и действовал из корыстных побуждений, преследуя личную выгоду, или руководствовался иными мотивами (месть, зависть, личная неприязнь и т.д.). При этом в результате таких действий контроль над информацией со стороны ее обладателя был утрачен. При этом неважно, повлекли ли действия пользователя негативные последствия в действительности, равно как и то, понесла ли компания убытки, связанные с действиями пользователя. Также к умышленным утечкам относятся все утечки, спровоцированные хакерскими атаками или физическим доступом извне к носителям информации ограниченного доступа, принадлежащей компании.