softline®
Мы всё сможем
30 лет в ИТ

Изменения в 152-ФЗ. Защита персональных данных сегодня

Состав Команды

Тихонов Илья
Руководитель направления по защите персональных данных.

Сазонов Анатолий
Руководитель направления безопасности промышленных предприятий.

Гострый Максим
Ведущий эксперт блока безопасности промышленных предприятий.

Федеральный закон "О персональных данных" от 27.07.2006 N 152-ФЗ

Персональные данные (сокр. ПДн)— сведения, относящиеся к прямо или косвенно определённому или определяемому физическому лицу (субъекту персональных данных)

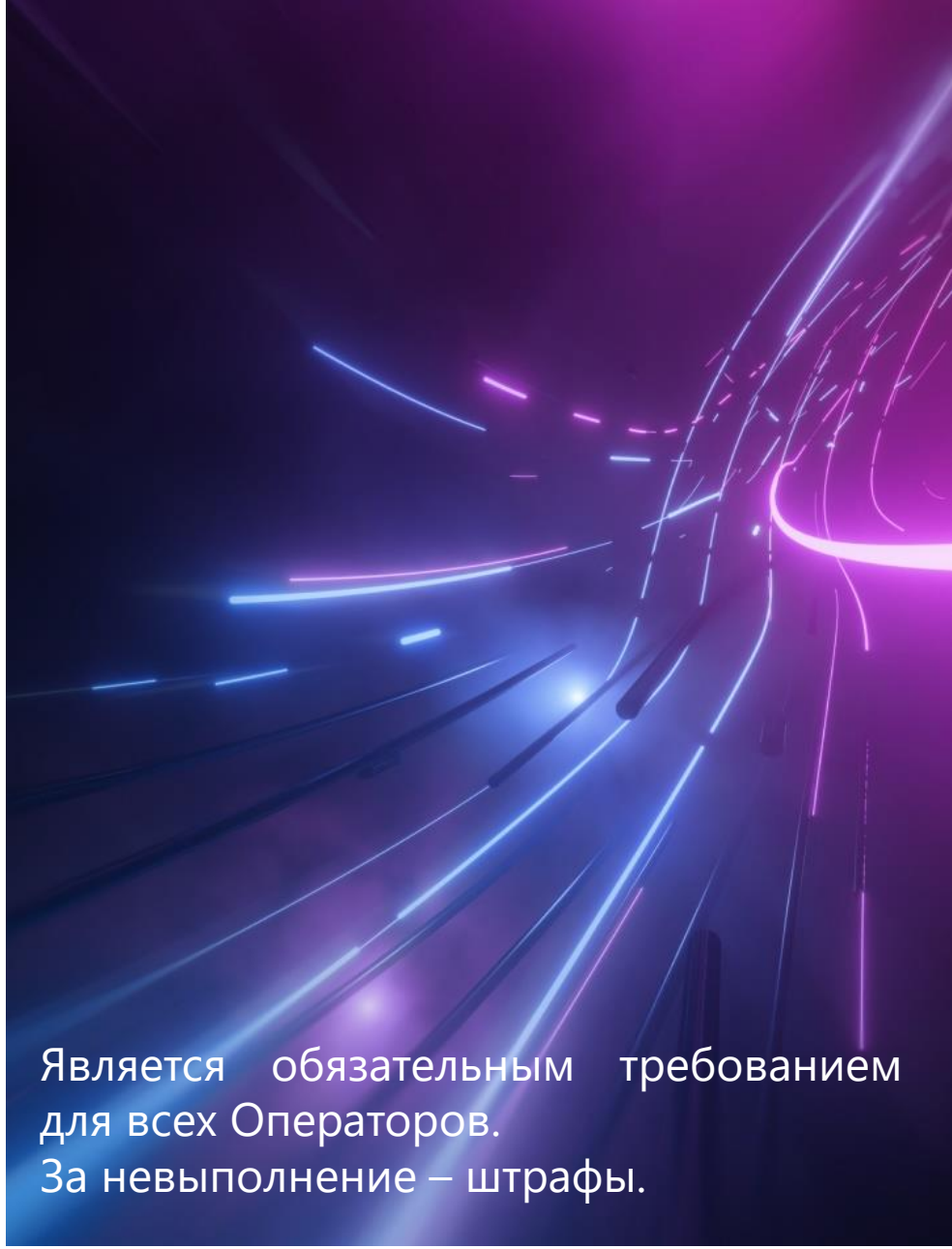
СУБЪЕКТ – доверяет свои персональные данные

ОПЕРАТОР – обрабатывает и защищает персональные данные

РЕГУЛЯТОР – устанавливает правила и контролирует процесс обработки и защиты

ИНФОРМАЦИОННАЯ СИСТЕМА ПДн- Совокупность содержащихся в базах данных ПДн и обеспечивающих их обработку информационных технологий и технических средств.

ОБРАБОТКА ПДн - любое действие или совокупность действий, совершаемых с использованием средств автоматизации или без использования таких средств



Роскомнадзор: 230 млн записей с личными данными россиян утекли в сеть с начала 2022 года. произошло около 150 крупных утечек персональных данных

УТЕЧКИ 2022 – 2023 гг.

- «Яндекс.Еды»
- Delivery Club
- СДЭК
- Whoosh
- Гемотест
- Туту.ру
- DNS
- Спортмастер
- book24.ru
- askona.ru
- gloria-jeans.ru
- «Ашан»
- «Твой Дом»
- «Буквоед»
- «Леруа Мерлен»
- edimdoma.ru
- «ТВОЕ»

Роскомнадзор: порядка 200 млн записей о россиянах утекли в Сеть в 2023 году

В 2021 году Роскомнадзор провёл более 3,9 тысячи контрольных мероприятий в отношении операторов персональных данных (ПД), свыше 80% проверок выявили, что операторы работают с нарушениями, сообщило ведомство.

Почти 1,7 тыс. россиян получили бесплатную юридическую помощь в Центре правовой помощи гражданам в цифровой среде за 2022 год. Кроме того, суды удовлетворили 95% исков центра в интересах заявителей, свидетельствуют данные годового отчета деятельности центра

Оборотные штрафы

•Предлагается введение оборотных штрафов за утечку персональных данных до 3% от оборота компании (**от 5 до 500 млн. рублей**).

• Планируется изменить Уголовный кодекс и ввести наказание для лиц, которые украли, продали персональные данные либо создали порталы для сделок по незаконному обороту личной информации (ст.ст. 272, 273 и 274 УК РФ) - штраф **от 300 тыс. рублей до 3 млн. рублей**, лишение свободы на срок — до 10 лет, за намеренное распространение персональных данных граждан.

Этапы работ по проекту 1

1. Обследование	• Сбор данных об информационных системах Заказчика • Сбор данных о процессах обработки ПДн • Сбор данных о применяемых мерах и средствах защиты
2. Моделирование угроз безопасности	• Определение исходного уровня защищенности ИСПДн • Разработка модели угроз и модели нарушителя • Составление перечня актуальных угроз безопасности
3. Определение уровня защищенности ПДн	• Анализ исходных сведений об ИСПДн • Анализ актуальных угроз безопасности ПДн • Разработка актов определения уровней защищенности
4. Разработка концепции СЗПДн	• Выработка рекомендаций по оптимизации процессов обработки ПДн • Разработка различных вариантов реализации СЗПДн
5. Разработка технического задания	• Определение требований для установленного УЗ • Определение требований для нейтрализации актуальных угроз безопасности
6. Стендовые испытания СЗИ:	• Макетирование ИСПДн Заказчика • Проверка совместимости СЗИ с программными и техническими средствами ИСПДн

Этапы работ по проекту 2

7. Техническое проектирование	Выбор необходимых средств защиты информации • Определение количественного состава СЗИ • Описание применения средств защиты информации • Разработка схем, планов и т. д.
8. Разработка комплекта ОРД	• Разработка необходимой организационно-распорядительной документации • Разработка необходимой эксплуатационной документации
9. Поставка и внедрение СЗИ	• Поставка СЗИ • Установка и настройка СЗИ • Проведение опытной эксплуатации СЗИ
10. Оценка соответствия (опционально)	• Оценка соответствия в форме проведения оценки соответствия или обязательной аттестации
11. Сопровождение системы (опционально)	• Консультационная и техническая поддержка проекта после его завершения

Новые требования 152-ФЗ (в силе)

С 1 сентября 2022 года вступают в силу изменения в закон «О персональных данных». Теперь операторы должны уведомлять Роскомнадзор о начале или осуществлении любой обработки персональных данных за исключением случаев, когда данные обрабатываются в целях защиты безопасности государства и общественного порядка, транспортной безопасности, или если Оператор обрабатывает данные исключительно без средств автоматизации

Борьба с утечками

1. Взаимодействие с ГосСОПКА

2. 24 часа на обнаружение утечки

3. 72 часа на расследование

Трансграничная передача ПДн

1. Отдельное уведомление в РКН

2. Формализация процесса трансграничной передачи в ОРД

Взаимодействие операторов ПДн

1. Изменение поручений на обработку ПДн

2. Наличие возможности запросить информацию о соблюдении 152-ФЗ

Взаимодействие с субъектами ПДн

1. 10 дней на ответ субъекту на его запрос

2. Субъект имеет право на запрос дополнительной информации у оператора

Взаимодействие с Роскомнадзором

1. Изменение подхода к уведомлению РКН

2. Подготовка новых уведомлений

Перечень документов по 152-ФЗ

1.Приказ о назначении лиц, ответственных за выполнение требований законодательства Российской Федерации в области обработки и защиты ПДн.
2.Положение об экспертной комиссии, включающее:
•форму акта определения уровня защищенности персональных данных, обрабатываемых в ИСПДн;
•форму акта оценки возможного вреда субъектам персональных данных при реализации угроз безопасности персональных данных.
3.Положение лице, ответственном за организацию обработки ПДн.
4.Положение о лице, ответственном за обеспечение безопасности ПДн.
5.Приказ об утверждении документов, регламентирующих обработку ПДн.
6.Политика в отношении обработки ПДн.
7.Положение об обработке персональных данных, включающее:
формы согласий субъектов на обработку ПДн;
форма обязательства о неразглашении ПДн;
форму поручения обработки ПДн.
8.Положение об обеспечении безопасности ПДн, включающее меры по:
идентификации и аутентификации субъектов доступа; • управлению доступом субъектов доступа к объектам доступа; ограничению программной среды; защите машинных носителей ПДн; регистрации событий безопасности; антивирусной защите; обнаружению вторжений; контролю защищенности ПДн; обеспечению целостности ИСПДн; обеспечение доступности ПДн; защите среды виртуализации; защите технических средств; реагированию на инциденты; управлению конфигурацией ИСПДн и СЗПДн.
9.Положение о порядке обработки ПДн без использования средств автоматизации.
10.Регламент контроля обеспечения безопасности ПДн, включающий:
•план внутренних проверок;
•журнал внутренних проверок обеспечения безопасности ПДн;
•форма отчета по контролю обеспечения безопасности ПДн.
11.Порядок рассмотрения запросов субъектов ПДн и контролирующих органов, включающий формы:
журнала регистрации обращений и запросов субъектов ПДн; журнала регистрации обращений и запросов надзорных органов; обращения субъекта ПДн на предоставление ПДн; предоставления сведений, запрашиваемых субъектом ПДн; уведомления субъекта ПДн об изменении ПДн; отзыва согласия субъекта на обработку ПДн; уведомления субъекта ПДн об уничтожении ПДн.
12. Инструкция пользователя ИСПДн.
13.Приказ об утверждении сведений, относящихся к обработке ПДн.
14.Перечень ИСПДн.
15.Перечень обрабатываемых ПДн.
16.Перечень материальных носителей ПДн и мест их хранения.
17.Паспорт ИСПДн (единый).
18.Перечень должностей работников, допущенных к автоматизированной и неавтоматизированной обработке ПДн.
19.Акт определения уровня защищенности ПДн.
20.Акт оценки возможного вреда субъектам ПДн.
21.Уведомление в Роскомнадзор: о намерении осуществлять обработку ПДн; о внесение изменений; о трансграничной передаче ПДн.
22.Приказ об утверждении экспертной комиссии.
23.Приказ о назначении ответственных лиц.
24.Приказ об утверждении журнала регистрации посетителей, включая форму журнала учета посетителей.
25.Приказ об утверждения перечня материальных носителей персональных данных, включая перечень материальных носителей персональных данных.
26.Приказ об организации защиты персональных данных, с использованием средств криптографической защиты информации в информационной системе персональных данных.
27.Порядок организации функционирования криптосредств.
28.Инструкция ответственного за эксплуатацию СКЗИ.
29.Инструкция пользователя СКЗИ.
30. Модель угроз

Перечень документов по 152-ФЗ + изменения с 1.09

Изменения в комплекте ОРД по ПДн

◦ Логически объединены приказы, утверждающие ОРД, в соответствии с регулируемыми направлениями/областями

◦ Предусмотрены обновления ФЗ-152, в том числе вступившие в силу 01.03.23: в части трансграничной передачи ПДн, уведомлений об инцидентах ИБ

◦ Обновлена политика обработки ПДн: удобный табличный вид, для легкого обновления оператором ПДн, в случае изменения целей или состава ПДн

◦ Предусмотрена возможность подготовки двух Политик обработки ПДн для внешних и внутренних субъектов ПДн (для размещения на корпоративном сайте и внутреннем ресурсе организации)

◦ Обновлены положения по защите ПД - меры, предусмотренные 21 приказом, упорядочены и разделены на технические и организационные в связи с контролем этих мер разными ответственными лицами (ответственный за обеспечение безопасности ПДН и ответственный за организацию обработки ПДН)

Оценка вреда по персональным данным

С 1 марта 2023 г. применяются единые критерии оценки возможного ущерба субъектам ПД, утвержденные Приказом Роскомнадзора № 178 от 27.10.2022. Приказ распространяет действие на всех операторов и владельцев систем персданных

Высокая. Возникает при обработке информации, касающейся биометрических личных данных, касающейся принадлежности к расе, национальности, религии, убеждений и взглядов, привлечения к уголовной ответственности, сведений о состоянии здоровья, интимной жизни; ПД несовершеннолетних; поручении обрабатывать персданные российских граждан иностранцу; сборе ПД с применением баз данных, находящихся за границей.
Средняя. Распространение ПД на официальном интернет-сайте оператора, которые предоставлены неограниченному кругу лиц; обработка производится в дополнительных целях, которые не соответствуют первоначальной; потенциальным клиентам напрямую предлагаются товары и услуги, для чего используются базы другого оператора; согласие на обработку ПД взято на официальном интернет-сайте без дальнейшей проверки субъекта ПД.
Низкая. Низкий уровень вреда персональным данным предполагает, что ответственным за обработку назначен сотрудник, не состоящий в штате оператора; информация собрана из общедоступных источников персданных, сформированных на основании положений ст. 8 Федерального закона № 152-ФЗ от 27.07.2006.

Типовые ошибки операторов ПДн

- Не разработали и не опубликовали политику обработки персональных данных
- Не назначили ответственного за обработку персональных данных
- Не утвердили перечень лиц, которые имеют доступ к персональным данным
- Сбор и хранение лишних ПДн
- Не проводится работа по самоаудиту с персональными данными
- Не ознакомление работников под подпись о законе о персональных данных
- Не уведомили Роскомнадзор или неправильно заполнили уведомление об обработке персональных данных
- Не утвердили перечень мест хранения персональных данных
- Использование неверного бланка согласия на обработку персональных данных

softline®

Мы всё сможем

30 лет в ИТ

Трансформация.

Успешная. Цифровая. Защищённая.