«Защита персональных данных

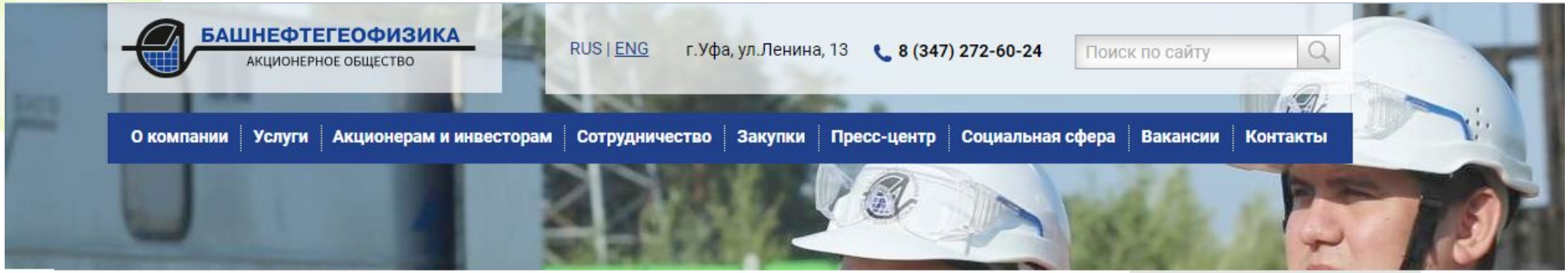
Дело № 4А-288

П О С Т А Н О В Л Е Н И Е

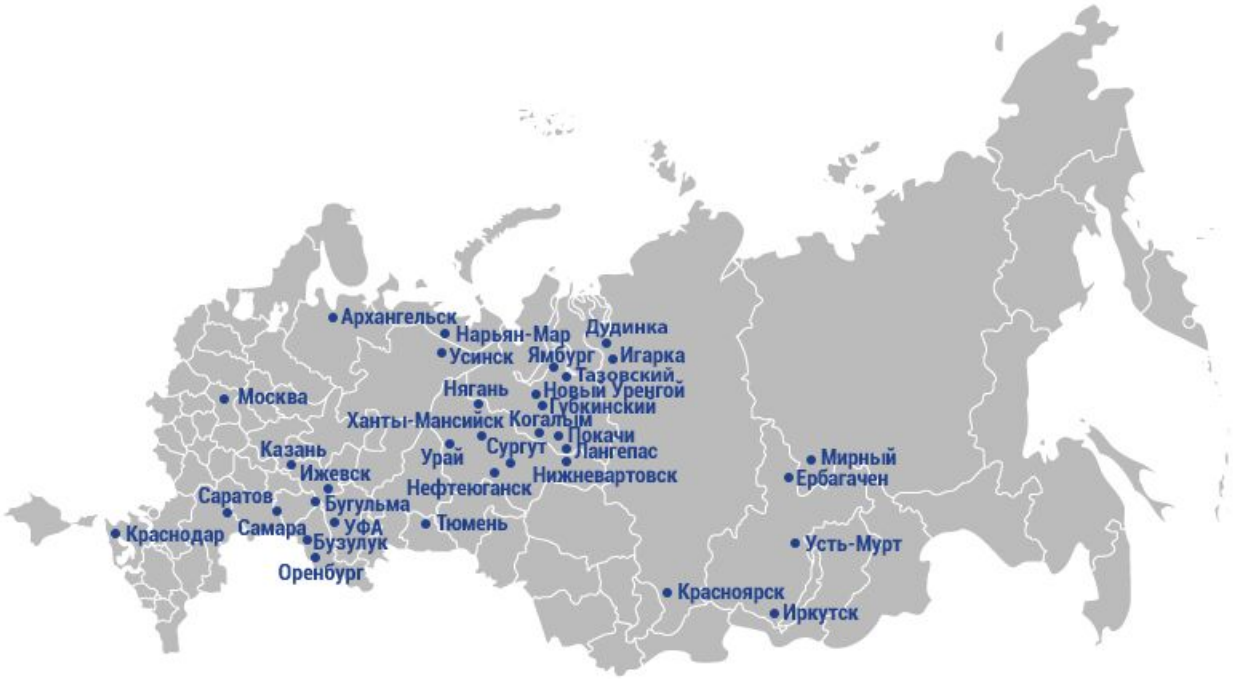
г. Тамбов 04 октября 2016 года

…

В силу ч. 2 ст. 18.1 Федерального закона «О персональных данных» №152-ФЗ от 27 июля 2006 года оператор обязан опубликовать или иным образом обеспечить неограниченный доступ к документу, определяющему его политику в отношении обработки персональных данных, к сведениям о реализуемых требованиях к защите персональных данных. *Оператор, осуществляющий сбор персональных данных с использованием информационно-телекоммуникационных сетей, обязан опубликовать в соответствующей информационно-телекоммуникационной сети документ, определяющий его политику в отношении обработки персональных данных, и сведения о реализуемых требованиях к защите персональных данных, а также обеспечить возможность доступа к указанном) документу с использованием средств соответствующей информационно - телекоммуникационной сети.*



ГЕОГРАФИЯ ДЕЯТЕЛЬНОСТИ АО «БАШНЕФТЕГЕОФИЗИКА»



Откликнуться

Инженер по бурению

Профильное образование и опыт проводки наклонно-направленных / горизонтальных скважин не менее 2-х лет

Откликнуться

Инженер по бурению DD

Профильное образование и опыт проводки наклонно-направленных / горизонтальных скважин не менее 1 года

Откликнуться

Все вакансии →

- История компании
- Организационная структура
- Руководство
- Управление персоналом
- Интегрированная система менеджмента

СОГЛАСИЕ

посетителя сайта на обработку персональных данных

Во исполнение требований законодательства о персональных данных (в том числе Федерального закона «О персональны данных» № 152-ФЗ от 27.07.2006 г.), настоящим свободно, своей волей и в своем интересе даю согласие АО «Башнефтегеофизика», которое находится по адресу: г.Уфа, ул.Ленина, 13, на автоматизированную и неавтоматизированну обработку моих персональных данных.

АО «Башнефтегеофизика» вправе осуществлять обработку моих персональных данных следующими способами: сбор, зап систематизация, накопление, хранение, обновление, изменение, использование в соответствии с действующим законодательством.

Согласие на обработку персональных данных дается мною для целей содействия проведения АО «Башнефтегеофизика» подбора персонала, повышения осведомленности посетителей сайта bngf.ru.

Данное согласие на обработку моих персональных данных выдано АО «Башнефтегеофизика» и может быть отозвано мно любой момент в период его действия путем направления в АО «Башнефтегеофизика» соответствующего заявления.

В случае направления отзыва согласия на обработку моих персональных данных, АО «Башнефтегеофизика» прекращает обработку моих персональных данных и уничтожает мои персональные данные в срок, не превышающий пять рабочих дн момента поступления указанного отзыва.

Производя отправку сообщения через форму обратной связи на страницах веб сайта – я тем самым принимаю соглашени добровольной форме на обработку моих персональных данных.

УФИМСКИЙ ГОСУДАРСТВЕННЫЙ АВИАЦИОННЫЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ

- Руководство университета
- Студенческий городок
- Наши партнеры
- СМИ о нас
- Структура университета
- Ученый совет
  - Объявления
  - Список членов ученого совета
  - Документы о работе Учёного совета
  - Комиссии ученого совета
  - План работы на учебный год
- Документы
- Пресс-центр
- Социальная работа
  - Психологическое сопровождение образовательного процесса
  - Информация для лиц обучающихся с ограниченными возможностями здоровья
  - Остановим СПИД вместе!
- Обеспечение безопасности
  - Противодействие коррупции
  - Противодействие идеологии терроризма
  - Противодействие наркомании и незаконному обороту наркотиков
- Выборы ректора

ФГБОУ ВО «УФИМСКИЙ ГОСУДАРСТВЕННЫЙ АВИАЦИОННЫЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ»

450008, Республика Башкортостан, г. Уфа, ул. К. Маркса, д. 12.

Отдел документационного обеспечения и архива:

+ 7 (347) 272-29-18 (факс)

Телефонный справочник УГАТУ

office@ugatu.su

ПРИЕМНАЯ КОМИССИЯ УГАТУ:

450008, Республика Башкортостан, г. Уфа, ул. К. Маркса, д. 12, корпус 8, ауд. 109.

Режим работы пн-пт с 9:00 до 18:00

+ 7 (347) 273-79-65

abit@ugatu.su

ЭЛЕКТРОННАЯ ПРИЕМНАЯ УГАТУ:

Вы можете задать вопрос администрации вуза, ректору, либо оставить свои пожелания и предложения

ПРИСОЕДИНЯЙТЕСЬ К НАМ В СОЦСЕТЯХ:

Сведения о доходах, об имуществе и обязательствах имущественного характера руководителя и членов его семьи

УФИМСКИЙ ГОСУДАРСТВЕННЫЙ АВИАЦИОННЫЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ

ФГБОУ ВО «УФИМСКИЙ ГОСУДАРСТВЕННЫЙ АВИАЦИОННЫЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ»

450008, Республика Башкортостан, г. Уфа, ул. К. Маркса, д. 12.

Отдел документационного обеспечения и архива:

+ 7 (347) 272-29-18 (факс)

Телефонный справочник УГАТУ

office@ugatu.su

ПРИЕМНАЯ КОМИССИЯ УГАТУ:

450008, Республика Башкортостан, г. Уфа, ул. К. Маркса, д. 12, корпус 8, ауд. 109.

Режим работы пн-пт с 9:00 до 18:00

+ 7 (347) 273-79-65

abit@ugatu.su

ЭЛЕКТРОННАЯ ПРИЕМНАЯ УГАТУ:

Вы можете задать вопрос администрации вуза, ректору, либо оставить свои пожелания и предложения

ПРИСОЕДИНЯЙТЕСЬ К НАМ В СОЦСЕТЯХ:

Сведения о доходах, об имуществе и обязательствах имущественного характера руководителя и членов его семьи

Актуальные вопросы

1. Зачем защищать персональные данные
2. Контроль и надзор. Основные нарушения Операторов ПДн
3. Нормативная база по защите персональных данных.
4. Постановление Правительства РФ № 687.
5. Специальные категории персональных данных
6. Биометрические персональные данные
7. Постановление Правительства РФ № 1119.
8. Приказ ФСТЭК № 21. Меры.
9. Защита информации в региональных информационных системах. Электронная очередь. ГИА и ЕГЭ.

Законодатель отнес любую информацию, относящуюся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных) (ст. 3 ФЗ о персональных данных). В силу такого широкого определения ПДн в законе, определить какие данные подпадают под охрану закона, а какие нет - дело не простое. Поэтому следует руководствоваться позицией регулятора - Роскомнадзора.

Пункт 2.5 Методических рекомендаций Роскомнадзора по уведомлению о начале обработки персональных данных раскрывает в скобках, какая это может быть информация: фамилия, имя, отчество, год, месяц, дата рождения, место рождения, адрес, семейное положение, социальное положение, имущественное положение, образование, профессия, доходы, другая информация, относящаяся к субъекту персональных данных.

Зачем заниматься защитой ПДн?

Снижение рисков выставления штрафов и других санкций регуляторов

Повышение доверия работников и партнеров

Повышение общего уровня ИБ

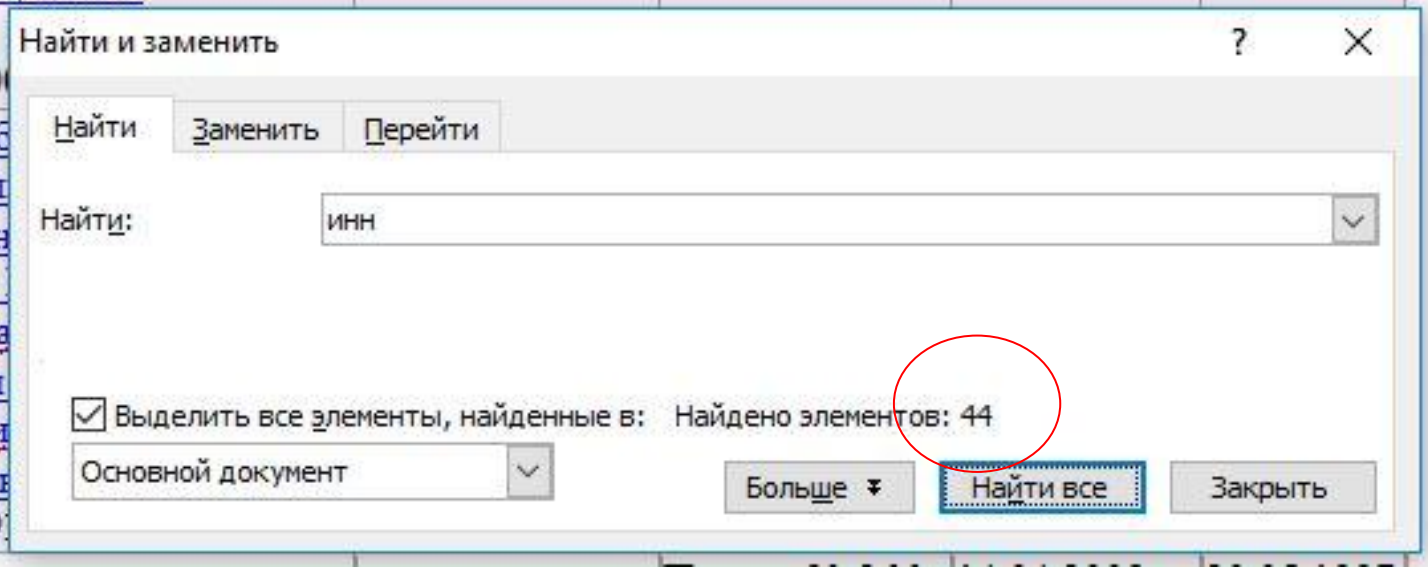
А что если не защищать свои персональные данные?

2-18-005985	МУНИЦИПАЛЬНОЕ АВТОНОМНОЕ УЧРЕЖДЕНИЕ "СПОРТИВНЫЙ ЦЕНТР "УФИМСКИЙ СОКОЛ" ГОРОДСКОГО ОКРУГА ГОРОД УФА РЕСПУБЛИКИ БАШКОРТОСТАН ИНН: 0258014304	юридическое лицо	Приказ № 180 от 19.07.2018	17.07.2018	06.03.2013
2-18-006351	МУНИЦИПАЛЬНОЕ КАЗЕННОЕ УЧРЕЖДЕНИЕ "ЦЕНТРАЛИЗОВАННАЯ БУХГАЛТЕРИЯ МУНИЦИПАЛЬНЫХ УЧРЕЖДЕНИЙ МУНИЦИПАЛЬНОГО РАЙОНА УФИМСКИЙ РАЙОН РЕСПУБЛИКИ БАШКОРТОСТАН" ИНН: 0245024129	юридическое лицо	Приказ № 327 от 14.12.2018	12.12.2018	06.12.2012

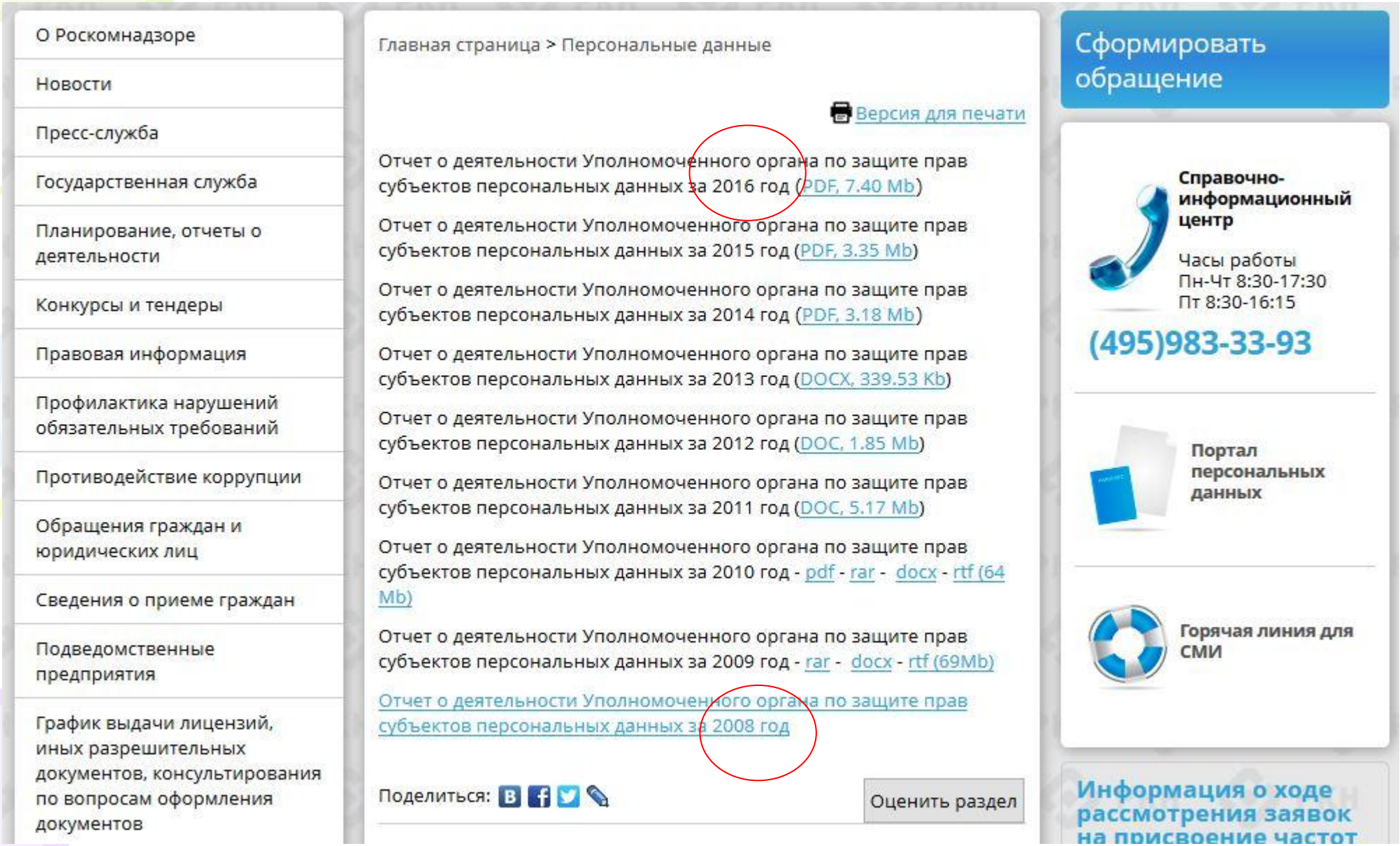
Всего: 56

А что если не защищать свои персональные данные?

Регистр. номер	Наименование оператора / ИНН	Тип оператора	Основания включения	Дата регистрации уведомления	Дата начала обработки
08-0004157	Муниципальное общеобразовательное бюджетное учреждение "Башкирская гимназия" городского округа город Нефтекамск Республики Башкортостан ИНН: 026405010	юридическое лицо	Приказ № 343 от 16.05.2008	07.12.2007	01.09.2010
08-0004161	муниципальное б общеобразовател башкирская гимн народного поэта Башкортостан На города Дюртюли района Дюртюли Республики Баш ИНН: 026000969				



А что если не защищать свои персональные данные?



О Роскомнадзоре
Новости
Пресс-служба
Государственная служба
Планирование, отчеты о деятельности
Конкурсы и тендеры
Правовая информация
Профилактика нарушений обязательных требований
Противодействие коррупции
Обращения граждан и юридических лиц
Сведения о приеме граждан
Подведомственные предприятия
График выдачи лицензий, иных разрешительных документов, консультирования по вопросам оформления документов

Главная страница > Персональные данные

Версия для печати

Отчет о деятельности Уполномоченного органа по защите прав субъектов персональных данных за 2016 год (PDF, 7.40 Mb)

Отчет о деятельности Уполномоченного органа по защите прав субъектов персональных данных за 2015 год (PDF, 3.35 Mb)

Отчет о деятельности Уполномоченного органа по защите прав субъектов персональных данных за 2014 год (PDF, 3.18 Mb)

Отчет о деятельности Уполномоченного органа по защите прав субъектов персональных данных за 2013 год (DOCX, 339.53 Kb)

Отчет о деятельности Уполномоченного органа по защите прав субъектов персональных данных за 2012 год (DOC, 1.85 Mb)

Отчет о деятельности Уполномоченного органа по защите прав субъектов персональных данных за 2011 год (DOC, 5.17 Mb)

Отчет о деятельности Уполномоченного органа по защите прав субъектов персональных данных за 2010 год - pdf - rar - docx - rtf (64 Mb)

Отчет о деятельности Уполномоченного органа по защите прав субъектов персональных данных за 2009 год - rar - docx - rtf (69Mb)

Отчет о деятельности Уполномоченного органа по защите прав субъектов персональных данных за 2008 год

Поделиться:

Оценить раздел

Сформировать обращение

Справочно-информационный центр

Часы работы
Пн-Чт 8:30-17:30
Пт 8:30-16:15

(495)983-33-93

Портал персональных данных

Горячая линия для СМИ

Информация о ходе рассмотрения заявок на присвоение частот

Лицам, нарушившим требования закона о персональных данных, в зависимости от конкретных обстоятельств и серьезности деяния может грозить не только административная и уголовная ответственность, но также гражданско-правовая и даже дисциплинарная (таблица). При этом административная ответственность с 1 июля 2017 года ужесточилась – вместо одного состава правонарушения ст. 13.11 КоАП РФ теперь предусматривает семь, а максимальный штраф составляет 75 тыс. руб.

Виды ответственности за нарушение закона о персональных данных

Вид ответственности	**Нарушение**	**Санкция**	**Норма**
Административная	Неправомерный отказ в предоставлении гражданину и (или) организации информации, предоставление которой предусмотрено законом, несвоевременное ее предоставление либо предоставление заведомо недостоверной информации	Административный штраф на должностных лиц в размере от 5 тыс. до 10 тыс. руб.	Статья 5.39 КоАП РФ
	Обработка персональных данных в случаях, не предусмотренных законом, либо обработка, несовместимая с целями сбора персональных данных	Предупреждение или административный штраф: на граждан – от 1 тыс. до 3 тыс. руб.; на должностных лиц – от 5 тыс. до 10 тыс. руб.; на юридических лиц – от 30 тыс. до 50 тыс. руб.	Часть 1 ст. 13.11 КоАП РФ
	Обработка персональных данных без письменного согласия субъекта, когда это необходимо, либо обработка данных с нарушением требований к составу сведений, включаемых в такое согласие	Административный штраф: на граждан – от 3 тыс. до 5 тыс. руб.; на должностных лиц – от 10 тыс. до 20 тыс. руб.; на юридических лиц – от 15 тыс. до 75 тыс. руб.	Часть 2 ст. 13.11 КоАП РФ

	Невыполнение оператором обязанности по опубликованию или обеспечению иным образом неограниченного доступа к политике обработки персональных данных	Предупреждение или административный штраф: на граждан – от 700 до 1 тыс. руб.; на должностных лиц – от 3 тыс. до 6 тыс. руб.; на индивидуальных предпринимателей – от 5 тыс. до 10 тыс. руб.; на юридических лиц – от 15 тыс. до 30 тыс. руб.	Часть 3 ст. 13.11 КоАП РФ
	Невыполнение оператором обязанности по предоставлению субъекту персональных данных информации, касающейся обработки его персональных данных	Предупреждение или административный штраф: на граждан – от 1 тыс. до 2 тыс. руб.; на должностных лиц – от 4 тыс. до 6 тыс. руб.; на индивидуальных предпринимателей – от 10 тыс. до 15 тыс. руб.; на юридических лиц – от 20 тыс. до 40 тыс. руб.	Часть 4 ст. 13.11 КоАП РФ
	Невыполнение оператором в установленные сроки требования субъекта персональных данных или его представителя либо Роскомнадзора об уточнении персональных данных, их блокировании или уничтожении (если данные являются неполными, устаревшими, неточными, незаконно полученными или не являются необходимыми для заявленной цели обработки)	Предупреждение или административный штраф: на граждан – от 1 тыс. до 2 тыс. руб.; на должностных лиц – от 4 тыс. до 10 тыс. руб.; на индивидуальных предпринимателей – от 10 тыс. до 20 тыс. руб.; на юр. лиц – от 25 тыс. до 45	Часть 5 ст. 13.11 КоАП РФ

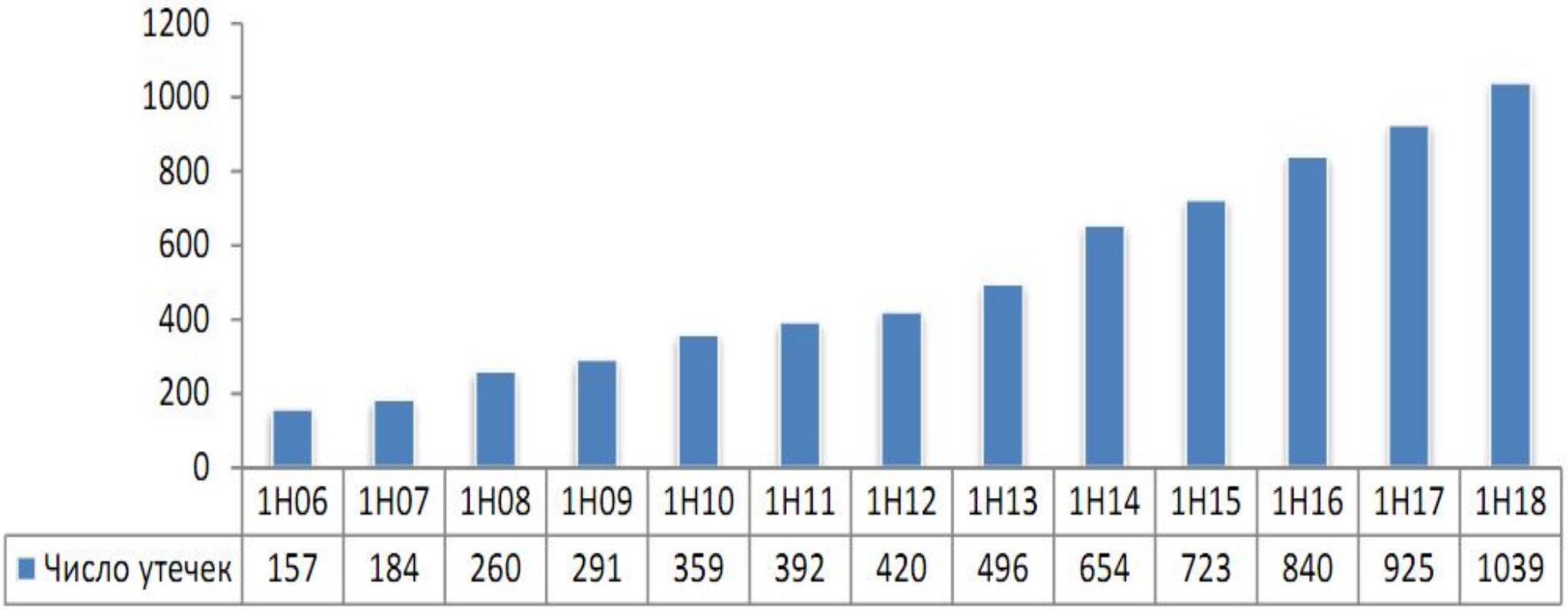
	Невыполнение оператором при обработке персональных данных без использования средств автоматизации обязанности по соблюдению условий, обеспечивающих их сохранность и исключающих несанкционированный к ним доступ, если это повлекло неправомерный или случайный доступ к данным, их уничтожение, изменение, блокирование, копирование, предоставление, распространение либо иные неправомерные действия в отношении них	Административный штраф: на граждан – от 700 до 2 тыс. руб.; на должн. лиц – от 4 -10 тыс. на инд. предпринимателей – от 10 тыс. до 20 тыс. руб.; на юридических лиц – от 25 тыс. до 50 тыс. руб.	Часть 6 ст. 13.11 КоАП РФ
	Невыполнение оператором, являющимся государственным или муниципальным органом, обязанности по обезличиванию персональных данных либо несоблюдение установленных для этого требований или методов	Предупреждение или наложение административного штрафа на должностных лиц в размере от 3 тыс. до 6 тыс. руб.	Часть 7 ст. 13.11 КоАП РФ
	Непредставление или несвоевременное представление в государственный или иной уполномоченный орган сведений, представление которых предусмотрено законом либо предоставление таких сведений в неполном объеме или в искаженном виде	Административный штраф: на граждан – от 100 до 300 руб.; на должностных лиц – от 300 до 500 руб.; на юридических лиц – от 3 тыс. до 5 тыс. руб.	Статья 19.7 КоАП РФ
Уголовная	Незаконное собирание или распространение сведений о частной жизни лица, составляющих его личную или семейную тайну, без его согласия либо распространение этих сведений в публичном выступлении, публично демонстрирующемся произведении или СМИ	Штраф до 200 тыс. руб., либо обязательныеработы на срок до 360 часов, либо исправительные работы на срок до 1 года, либо принудительные работы на срок до 2 лет (с лишением права занимать определенные должности на срок до трех лет или без такового), либо арест на срок до 4 месяцев, либо лишение свободы на срок до 2 лет.	Статья 137 Уголовного кодекса

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

	Неправомерный доступ к охраняемой законом компьютерной информации, если это повлекло ее уничтожение, блокирование, модификацию либо копирование	Штраф до 200 тыс. руб., либо исправительные работы на срок до одного года, либо ограничение свободы на срок до двух лет, либо принудительные работы на срок до двух лет, либо лишение свободы на тот же срок	Статья 272 УК РФ
Гражданско-правовая	Причинение лицу убытков в результате нарушения правил обработки его персональных данных. Под убытками при этом понимаются: расходы, которые лицо произвело или должно будет произвести для восстановления нарушенного права; утрата или повреждение его имущества; неполученные доходы, которые лицо получило бы, не будь его право нарушено.	Возмещение убытков	Статья 15 Гражданского кодекса
	Причинение гражданину морального вреда (нравственных страданий) вследствие нарушения правил обработки персональных данных	Компенсация морального вреда (независимо от возмещения имущественного вреда и понесенных субъектом убытков)	Статья 24 закона о персональных данных, ст. 151 ГК РФ
Дисциплинарная	Разглашение одним работником персональных данных другого, если они стали известны ему в связи с исполнением трудовых обязанностей	Увольнение	Подпункт "в" п. 6 ч. 1 ст. 81 Трудового кодекса
	Иные нарушения в области персональных данных при их обработке	Замечание или выговор	Статья 90, ст. 192 ТК РФ

Утечки информации в 2018 году

За I полугодие 2018 года Аналитическим центром InfoWatch было зарегистрировано 1039 случаев утечки конфиденциальной информации (см. Рисунок 1). Это на 12% больше, чем за аналогичный период 2017 года (925 утечек).



	1H06	1H07	1H08	1H09	1H10	1H11	1H12	1H13	1H14	1H15	1H16	1H17	1H18
Число утечек	157	184	260	291	359	392	420	496	654	723	840	925	1039

Утечки информации в 2018 году*

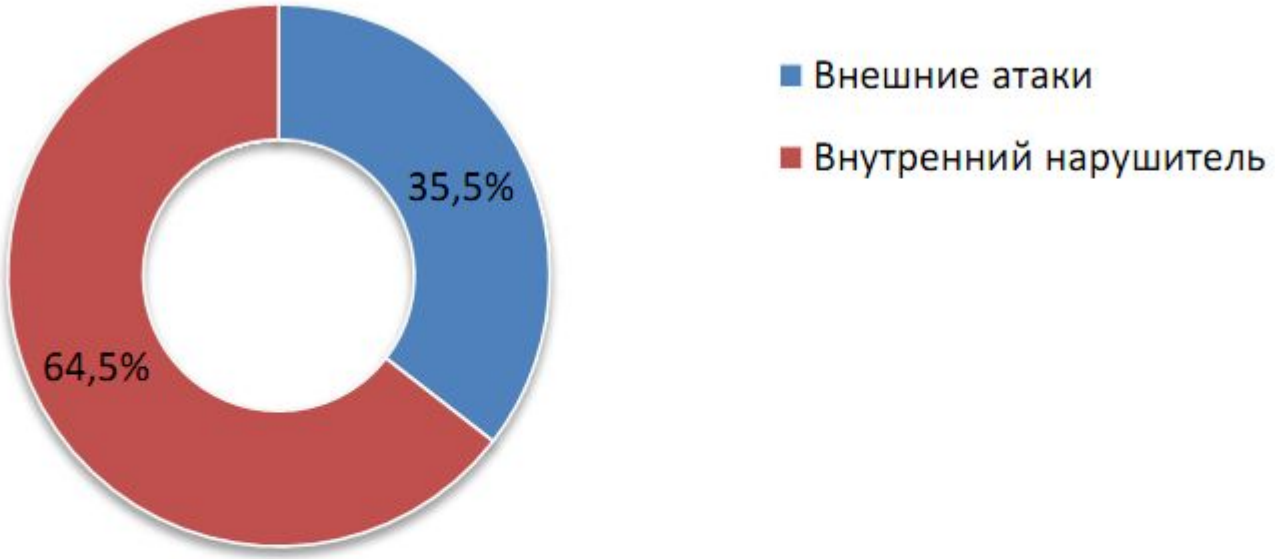


Рисунок 2. Распределение утечек по вектору воздействия[10], ½ 2018 г.

[10] Вектор воздействия – признак действий лиц, спровоцировавших утечку. Различаются действия внешних злоумышленников, направленные «внутрь» компании, воздействующие на веб-ресурсы, информационную инфраструктуру с целью компрометации

* - по данным исследования Аналитического центра Infowatch

Утечки информации в 2018 году*

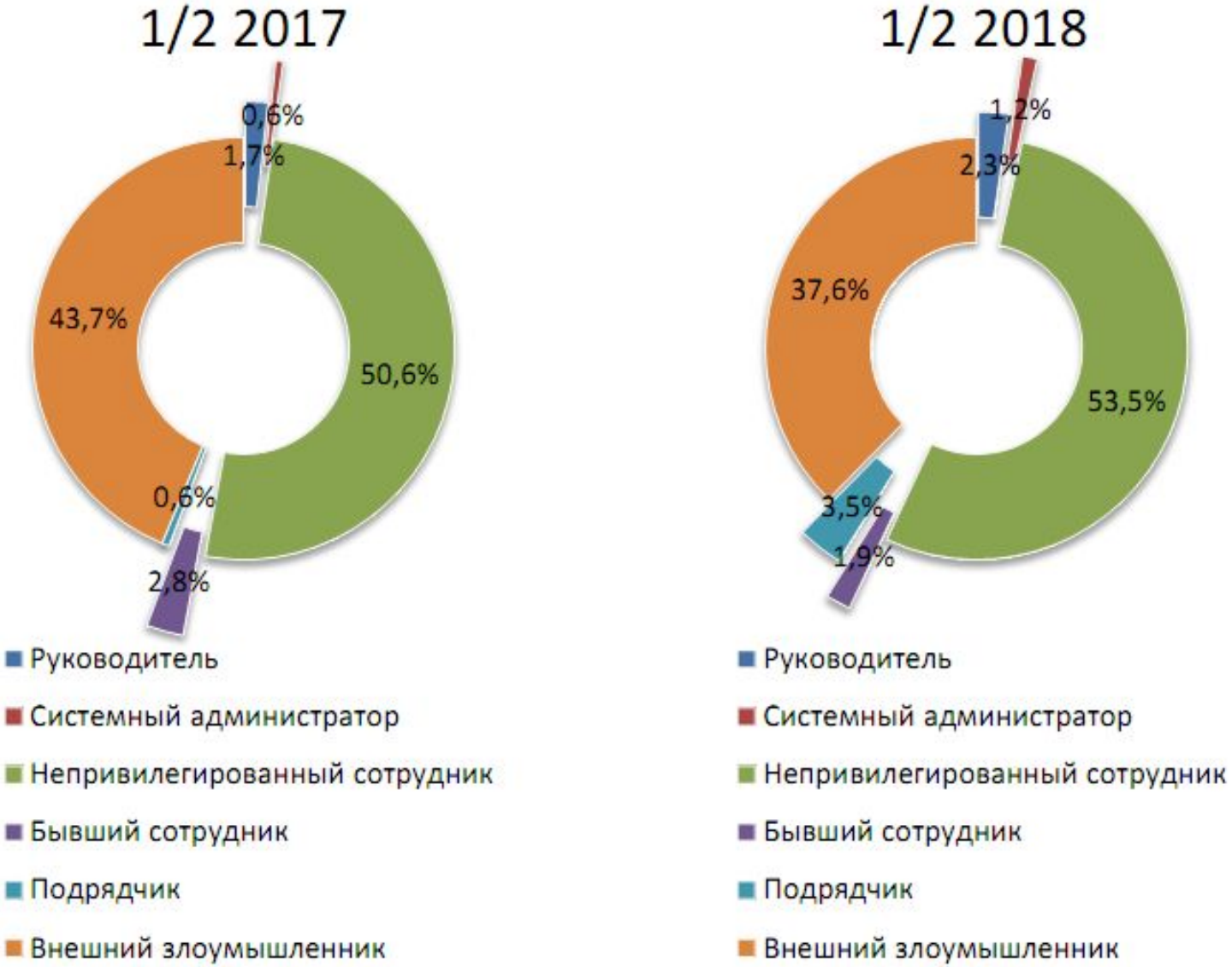


Рисунок 3. Распределение утечек по источнику (виновнику), ½ 2017 – ½ 2018 гг.

* - по данным исследования Аналитического центра Infowatch

Утечки информации в 2018 году*

Рисунок 4. Распределение утечек по типам данных, ½ 2017 – ½ 2018 гг.

* - по данным исследования Аналитического центра Infowatch

Утечки информации в 2018 году*

Рисунок 5. Распределение утечек по характеру, ½ 2017 – ½ 2018 гг.

* - по данным исследования Аналитического центра Infowatch

Утечки информации в 2018 году*

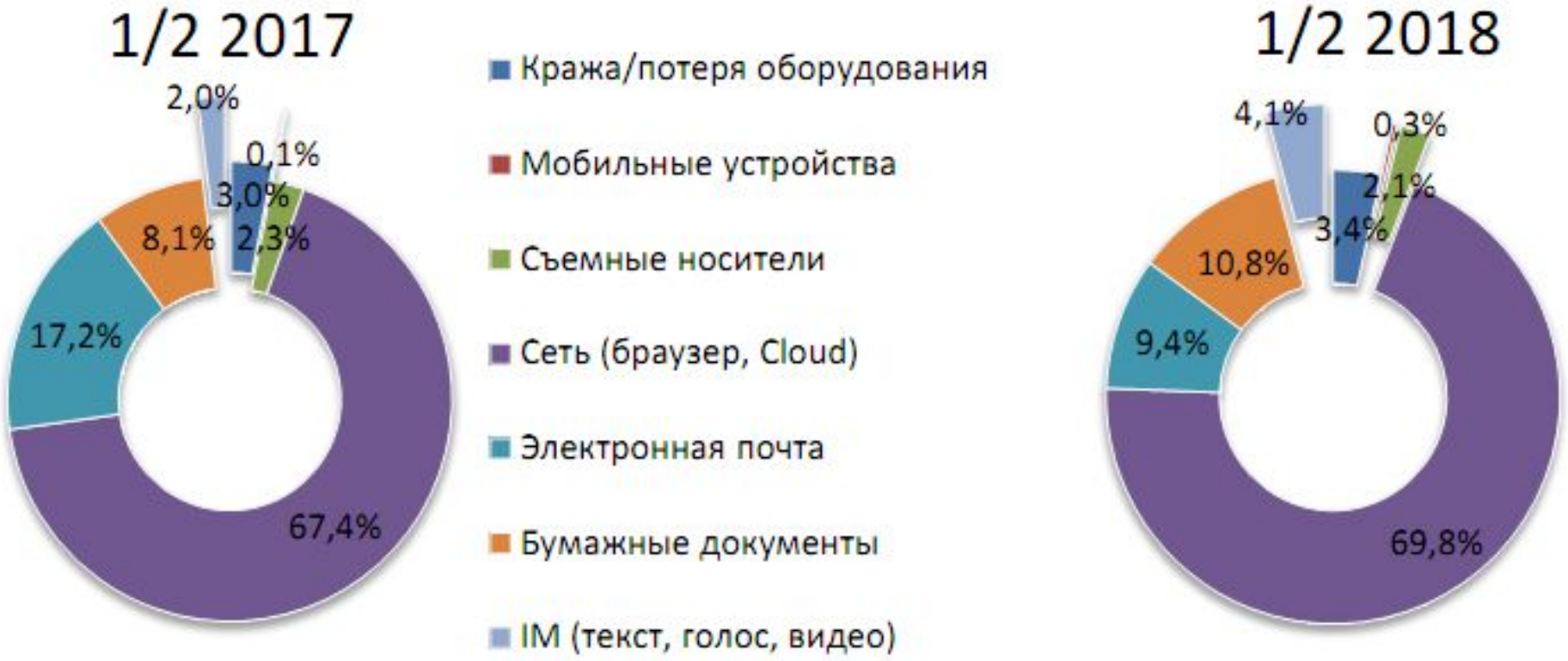
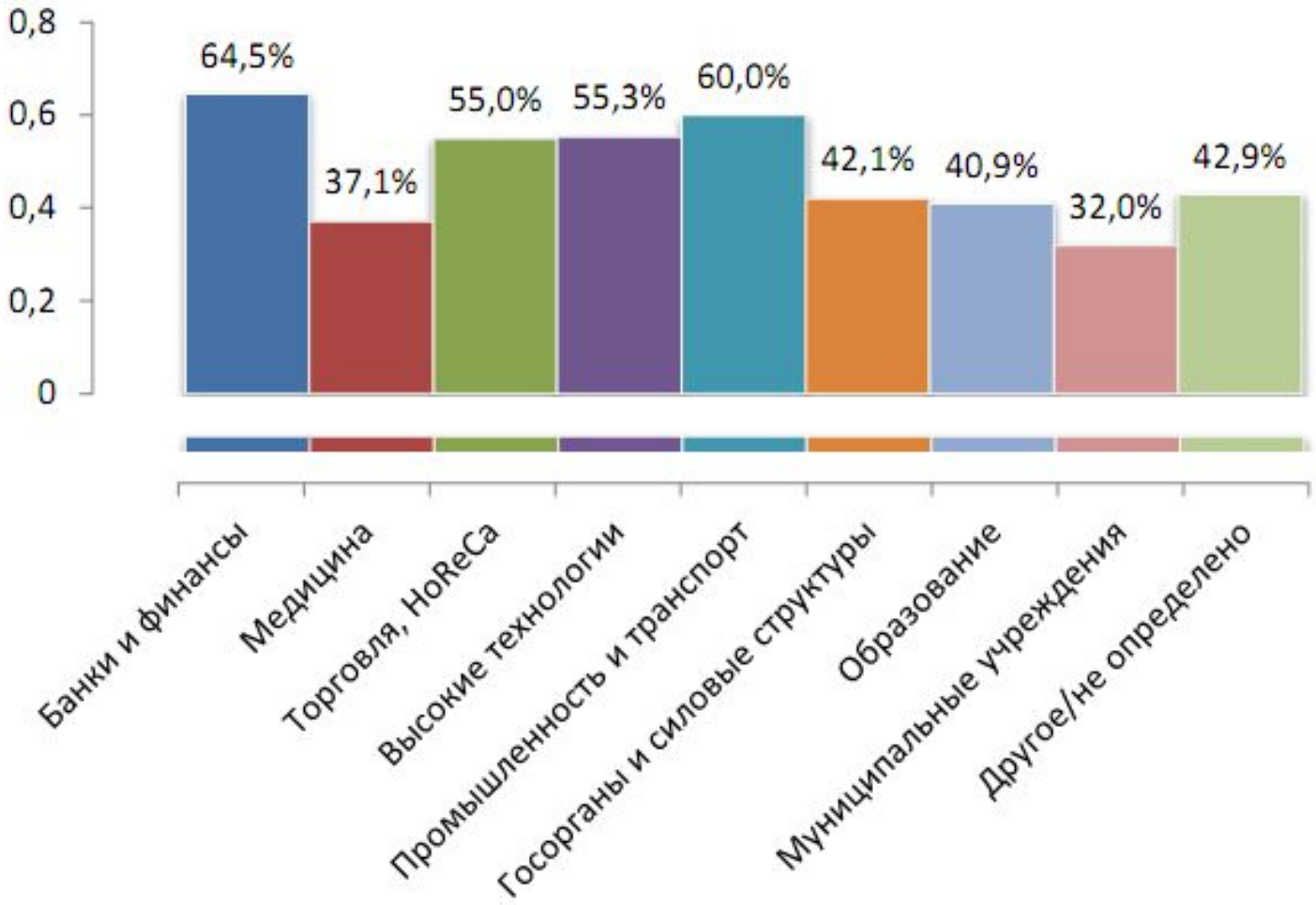


Рисунок 6. Распределение утечек по каналам, ½ 2017 – ½ 2018 гг.

* - по данным исследования Аналитического центра Infowatch

Утечки информации в 2018 году*



Доля умышленных утечек ПДн от общего количества утечек ПДн по отраслям, ½ 2018 г.

Чем проще конвертировать украденную информацию в деньги, тем «привлекательнее» сегмент.

* - по данным исследования Аналитического центра Infowatch

Утечки информации в 2018 году*

Основные риски бизнеса в настоящее время связаны не с внешним воздействием, а с внутренними утечками. Речь идет как о ненамеренных ошибках, так и о злоумышленных действиях сотрудников и руководителей компаний, направленных на компрометацию охраняемых данных, манипулирование информацией ограниченного доступа (в том числе инсайдерской информацией), корыстное использование полученных данных в мошеннических целях.

Учитывая отмеченную в 2017 году тенденцию на укрупнение корпоративных и государственных хранилищ данных, развитие технологий обработки больших объемов информации, не стоит удивляться, что конкретные факты применения таких технологий в ущерб владельцам данных все чаще становятся достоянием общественности. Это выводит на первый план проблему юридического регулирования режима больших пользовательских данных, ставит вопрос о том, кому же принадлежит собранная база данных и знания, извлеченные на основе ее анализа, кто отвечает за утечку данных, если она произошла.

* - по данным исследования Аналитического центра Infowatch

Проблематика вопроса

СООТНОШЕНИЕ НАЗНАЧЕНИЯ И ВИДА ОБЪЕКТА ЗАЩИТЫ

Виды работ, запланированных в защищаемых помещениях	**Защищаемые помещения (ЗП)**		
	Режимные помещения **(РП)**	Объекты информатизации **(ОИ)**	Выделенные помещения **(ВП)**
хранение	+		
рукопись	+		
хранение крипто-средств	+		
эксплуатация ТСПИ	+	+	
обсуждение	+	+	+
организация спецсвязи	+	+	+

* - по данным исследования Аналитического центра Infowatch

Проблематика вопроса

В итоге на каждое помещение, предназначенное для производства работ с конфиденциальной информацией, требуется оформление набора документов, как минимум включающего:

1. Акт осмотра помещения;
2. Акт категорирования помещения;
3. Акт классификации ОИ по требованиям зашиты информации;
5. Технический паспорт на объект информатизации включающий:
- состав технических и программных средств, входящих в АС;
- планы размещения основных и вспомогательных технических средств и систем;
- состав и схемы размещения средств защиты информации;
- сертификаты соответствия требованиям по безопасности информации на средства и системы обработки и передачи информации, используемые средства зашиты информации;
- план контролируемой зоны предприятия (учреждения);
- схемы прокладки линий передачи данных;
- схемы и характеристики систем электропитания и заземления объекта информатизации;
- описание технологического процесса обработки информации в АС;
- модель угроз информационной безопасности;
6. Организационно-распорядительная документация:
- список должностных лиц допускаемых на объект информатизации
- технологические инструкции пользователям АС и администратору безопасности информации;
- инструкции по эксплуатации средств защиты информации;
- инструкции по организации антивирусной защиты;
- нормативная и методическая документация по защите информации (приказы, руководства и инструкции);
7. Приемо-сдаточная документация на объект информатизации (приказ о вводе в эксплуатацию);
8. Техническое задание по организации средств защиты информации

Надзорные органы

- **Федеральная служба по надзору в сфере связи и массовых коммуникаций** (**РОСКОМНАДЗОР**) –ведет реестр операторов персональных данных, контролирует обработку персональных данных операторами и рассматривает обращения субъектов персональных данных.

- **ФСТЭК России** (Федеральная служба по техническому и экспортному контролю РФ) – регулирует техническую сферу обработки персональных данных

- **ФСБ России** (Федеральная служба безопасности РФ) – регулирует сферу использования криптографических (шифровальных) средств защиты информации при обработке персональных данных

Надзорные органы

А еще:

Прокуратура – защита прав граждан;

- **Рособрнадзор** – обработка персональных данных работников, детей и их законных представителей (заключили соглашение с РОСКОМНАДЗОРом о сотрудничестве);
- **Государственная инспекция труда** – обработка персональных данных работников
- **Роспотребнадзор –** обработка персональных данных граждан

Применяемые способы надзора

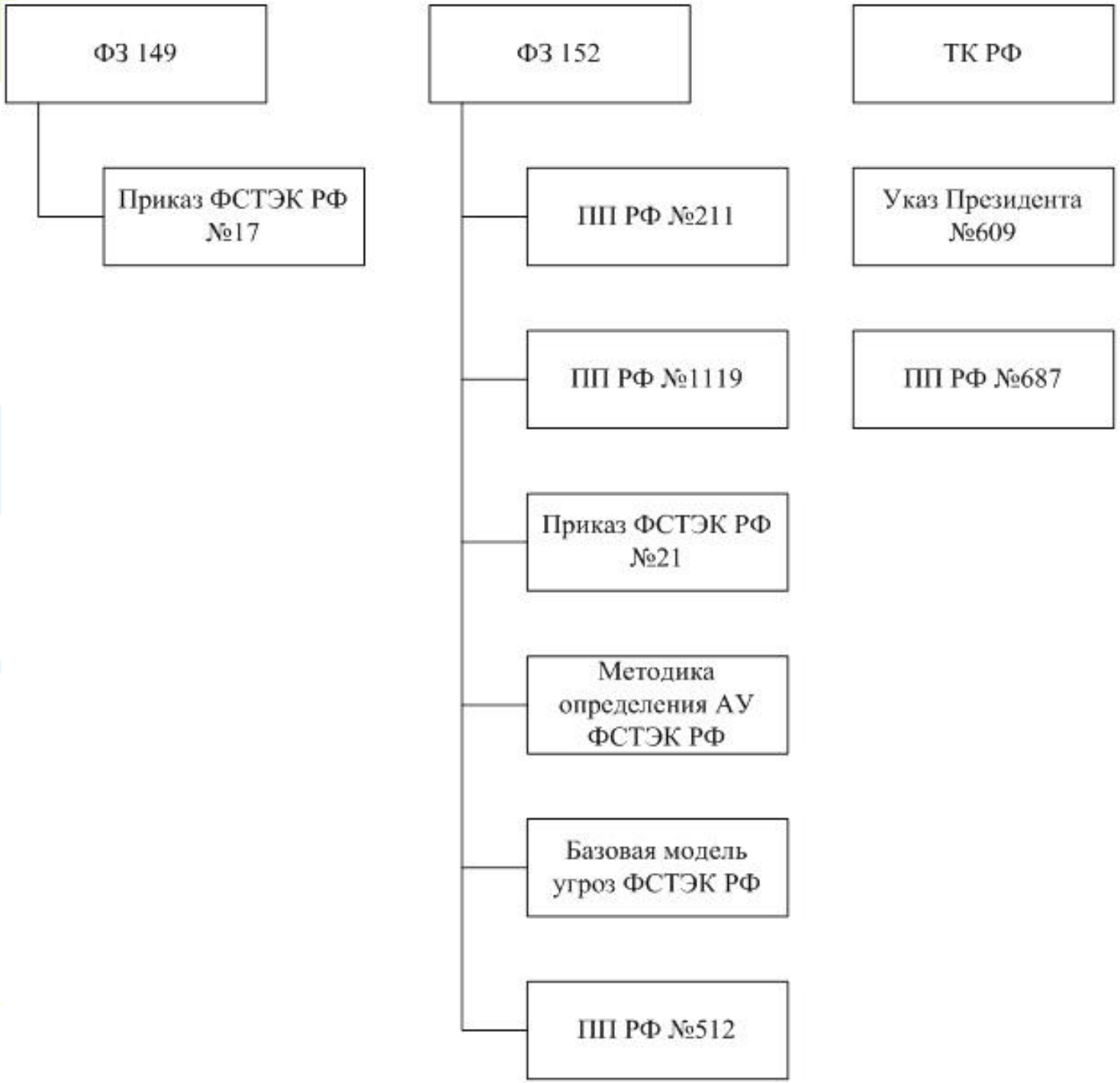
- Плановые проверки (план проверок размещен на сайтах Прокуратуры и РОСКОМНАДЗОР) ;
- Систематическое наблюдение :
- выявление организаций и учреждений не подавших уведомление в РКН;
- не предоставивших сведения об ответственном за организацию обработки ПДн;
- Не разместивших на сайте Политику в отношении обработки персональных данных;
- Обучение инспекторов РОСОБРНАДЗОРа выявлению обработки ПДн с нарушение требований 152-ФЗ;
- Внеплановые проверки (по жалобам)

Типовые ошибки операторов ПДн

1. Не предоставление или несвоевременное предоставление уведомления об обработке ПДн;
2. Предоставление уведомления об обработке ПДн в неполном объеме;
3. Отсутствие согласия на обработку ПДн;
4. Несоответствие содержания согласия требованиям законодательства:

- Неверно указана цель обработки ПДн;
- Указаны не все категории ПДн
- Не указаны или неверно указаны сроки прекращения обработки ПДн
- 5. Несоответствие типовых форм документов;
- 6. Незаконная передача третьим лицам (без согласия субъекта ПДн)
- 7. Несоблюдение требований по информированию сотрудников, осуществляющих обработку ПДн без использования средств автоматизации;
- 8. Отсутствие в тексте договора с лицом, осуществляющим обработку ПДн по поручению оператора, существенного условия об обеспечении конфиденциальности и безопасности ПДн
- 9. Отсутствие в тексте трудового договора существенного условия об обеспечении конфиденциальности ПДн
- 10. Наличие в анкете, предоставляемой при приеме на работу, требований по внесению информации сверх необходимой (сведения о судимости, сведения о персональных данных близких родственников, сведения о специальных категориях персональных данных – расовая, национальная принадлежность, политические взгляды, религиозные и философские убеждения, состояние здоровья, интимной жизни)
- 11. Сотрудники не ознакомлены с положение об обработке персональных данных (для всех сотрудников организации), инструкциями (только для участвующих в обработке)
- 12. Не утвержден перечень лиц, имеющих доступ к персональным данным
- 13. Обработка персональных данных (в том числе хранение) после достижения целей обработки.
- 14. Отсутствие политики в отношении обработки персональных данных
- 15. Не назначен ответственный за организацию обработки персональных данных
- 16. Не корректная передача дел в архив
- 17. Избыточные персональные данные в личных делах работников, учащихся

Правовая база по ПДн



1. Трудовой кодекс РФ (Глава 14, ст. 85-90).
2. Федеральный закон Российской Федерации от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации».
3. Федеральный закон Российской Федерации от 27 июля 2006 г. № 152-ФЗ «О персональных данных».
4. Перечень мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом "О персональных данных" и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами, утвержден постановлением Правительства Российской Федерации от 21 марта 2012 г. №211.
5. Положение о персональных данных государственного гражданского служащего Российской Федерации и ведении его личного дела, утверждено указом Президента Российской Федерации от 30 мая 2005 г. №609.
6. Требования к защите персональных данных при их обработке в информационных системах персональных данных, утвержденные постановлением Правительства Российской Федерации от 01 ноября 2012 г. № 1119.

7. Требования о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах, утверждены приказом ФСТЭК России от 11 февраля 2013 г. №17.
8. Состав и содержание организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных, утверждены приказом ФСТЭК от 18 февраля 2013 г. № 21.
9. Положение об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации, утверждено постановлением Правительства Российской Федерации от 15 сентября 2008 г. № 687.
10. Требования к материальным носителям биометрических персональных данных и технологиям хранения таких данных вне информационных систем персональных данных, утверждены постановлением Правительства Российской Федерации от 6 июля 2008 г. №512.
11. «Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных», утверждена Заместителем директора ФСТЭК России 14 февраля 2008

12. «Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных», утверждена Заместителем директора ФСТЭК России от 15 февраля 2008 г.

Документ «Состав и содержание организационных и технических мер по обеспечению безопасности персональных данных при их обработке в ИСПДн» (утверждён приказом ФСТЭК России от 18.2.2013 г. № 21):

- принят во исполнение ч. 4 ст. 19 Федерального закона от 27.07.2006 г. № 152-ФЗ «О персональных данных»;
- устанавливает перечень **обязательных мер по обеспечению безопасности ПДн, принимаемых** для защиты ПДн от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, предоставления, распространения а также от иных неправомерных действий;
- требования приказа носят **обязательный характер** для операторов или лиц, осуществляющих обработку персональных данных по поручению оператора.

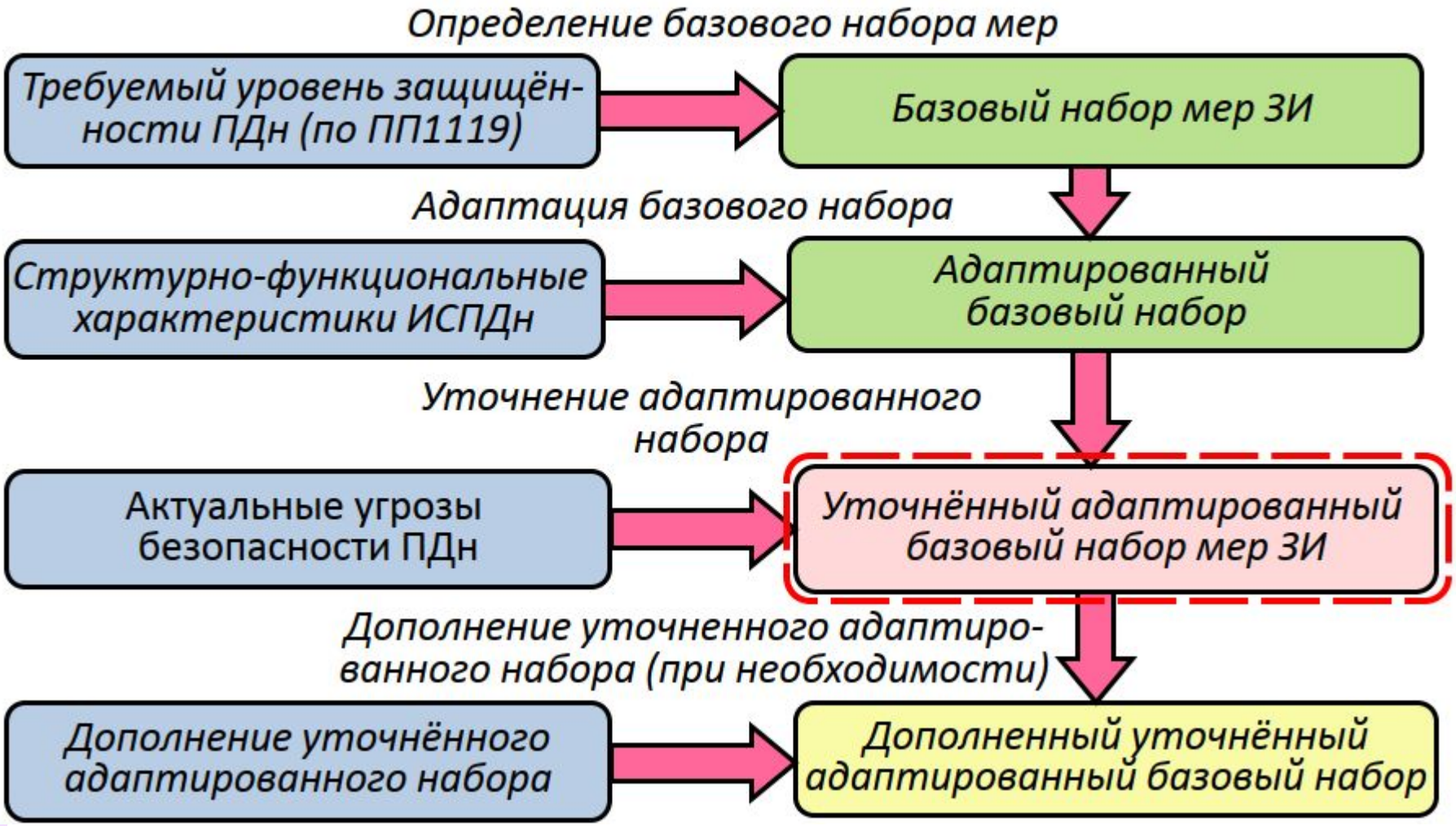
Что такое «мера защиты информации»? Группы мер защиты

Мера защиты = требование по защите информации - установленное правило или норма, которая должна быть выполнена при организации и осуществлении защиты информации.

Приказ № 21 ФСТЭК России предусматривает возможность применения 109 мер защиты сгруппированных в 15 групп:

1. Идентификация и аутентификация субъектов и объектов доступа (ИАФ).
2. Управление доступом субъектов к объектам доступа (УПД).
3. Ограничение программной среды (ОПС).
4. Защита машинных носителей информации (ЗНИ).
5. Регистрация событий безопасности (РСБ).
6. Антивирусная защита (АВЗ).
7. Обнаружение вторжений (СОВ).
8. Контроль (анализ) защищенности персональных данных (АНЗ).
9. Обеспечение целостности ИС и ПДн (ОЦЛ).
10. Обеспечение доступности ПДн (ОДТ).
11. Защита среды виртуализации (ЗСВ).
12. Защита технических средств (ЗТС).
13. Защита ИС, ее средств, систем связи и передачи данных (ЗИС).
14. Выявление инцидентов и реагирование на них (ИНЦ).
15. Управление конфигурацией ИС и СЗПДн (УКФ).

Как выбрать необходимые меры защиты?



Материалы для курсов ИСПДн в контакте, группа «консультация»

Выбор уровня защищённости ПДн

Категория ПДн	Тип угрозы				
	1-тип	2-тип		3-тип	
Специальные	УЗ-1	УЗ-1 при обраб-ке ПДн >100 тыс. др. субъектов	УЗ-2 при обр. ПДн сотрудников оператора или <100 тыс. др. субъектов	УЗ-2 при обраб-ке ПДн >100 тыс. др. субъектов	УЗ-3 при обр. ПДн сотрудников оператора или <100 тыс. др. субъектов
Биометрические	УЗ-1	УЗ-2		УЗ-3	
Иные категории	УЗ-1	УЗ-2 при обраб-ке ПДн >100 тыс. др. субъектов	УЗ-3 при обр. ПДн сотрудников оператора или <100 тыс. др. субъектов	УЗ-3 при обраб-ке ПДн>100 тыс. др. субъектов	УЗ-4 при обр. ПДн сотрудников оператора или <100 тыс. др. субъектов
Общедоступные	УЗ-2	УЗ-2 при обраб-ке ПДн >100 тыс. др. субъектов	УЗ-3 при обр. ПДн сотрудников оператора или <100 тыс. др. субъектов	УЗ-4	

Что такое «тип угроз»?

Тип угроз – характеристика нарушителя, который может реализовать угрозы и которому должна противостоять система защиты

Характеристика нарушителя		Тип угроз, которые может реализовать нарушитель	
Потенциал	**Возможности**		
Высокий (нарушитель государственного типа – *Спецслужбы ИГ*)	Создание способов, подготовка и проведение атак **с привлечением специалистов для реализации атак в области использования недокументированных (недекларированных) возможностей (НДВ) системного ПО**	**1 тип**	Угрозы, связанные с наличием недокументированных (недекларированных) возможностей в системном ПО, используемом в ИС.
Средний (нарушитель корпоративного типа – *Специализированные корпорации (Гугл, Оракл, IBM, SAP….)*	Создание способов, подготовка и проведение атак **с привлечением специалистов в области использования для реализации атак НДВ прикладного ПО**	**2 тип**	Угрозы, связанные с наличием недокументированных (недекларированных) возможностей в прикладном ПО, используемом в ИС.
Базовый (нарушитель физическое лицо или группа физических лиц – *хакер, криминал*)	Создание способов, подготовка и проведение атак **без привлечения специалистов в области разработки и анализа СЗИ (в т.ч. СКЗИ)**	**3 тип**	Угрозы не связанные с наличием недокументированных (недекларированных) возможностей в системном и прикладном ПО, используемом в ИС.

Наименование Угроз Безопасности Информации

1. Угроза автоматического распространения вредоносного кода в грид-системе (система, которая координирует распределенные ресурсы посредством стандартных, открытых, универсальных протоколов и интерфейсов)
2. Угроза агрегирования данных, передаваемых в грид-системе
3. Угроза анализа криптографических алгоритмов и их реализации
4. Угроза аппаратного сброса пароля BIOS
5. Угроза внедрения вредоносного кода в BIOS
6. Угроза внедрения кода или данных
7. Угроза воздействия на программы с высокими привилегиями
8. Угроза восстановления аутентификационной информации
9. Угроза восстановления предыдущей уязвимой версии BIOS

10. Угроза выхода процесса за пределы виртуальной машины
11. Угроза деавторизации санкционированного клиента беспроводной сети
12. Угроза деструктивного изменения конфигурации/среды окружения программ
13. Угроза деструктивного использования декларированного функционала BIOS
14. Угроза длительного удержания вычислительных ресурсов пользователями
15. Угроза доступа к защищаемым файлам с использованием обходного пути
16. Угроза доступа к локальным файлам сервера при помощи URL
17. Угроза доступа/перехвата/изменения HTTP cookies
18. Угроза загрузки нештатной операционной системы

19. Угроза заражения DNS-кеша
20. Угроза злоупотребления возможностями, предоставленными потребителям облачных услуг
21. Угроза злоупотребления доверием потребителей облачных услуг
22. Угроза избыточного выделения оперативной памяти
23. Угроза изменения компонентов системы
24. Угроза изменения режимов работы аппаратных элементов компьютера
25. Угроза изменения системных и глобальных переменных
26. Угроза искажения XML-схемы
27. Угроза искажения вводимой и выводимой на периферийные устройства информации
28. Угроза использования альтернативных путей доступа к ресурсам

29. Угроза использования вычислительных ресурсов суперкомпьютера «паразитными» процессами
30. Угроза использования информации идентификации/аутентификации, заданной по умолчанию
31. Угроза использования механизмов авторизации для повышения привилегий
32. Угроза использования поддельных цифровых подписей BIOS
33. Угроза использования слабостей кодирования входных данных
34. Угроза использования слабостей протоколов сетевого/локального обмена данными
35. Угроза использования слабых криптографических алгоритмов BIOS
36. Угроза исследования механизмов работы программы
37. Угроза исследования приложения через отчёты об ошибках

38. Угроза исчерпания вычислительных ресурсов хранилища больших данных
39. Угроза исчерпания запаса ключей, необходимых для обновления BIOS
40. Угроза конфликта юрисдикций различных стран
41. Угроза межсайтового скриптинга
42. Угроза межсайтовой подделки запроса
43. Угроза нарушения доступности облачного сервера
44. Угроза нарушения изоляции пользовательских данных внутри виртуальной машины
45. Угроза нарушения изоляции среды исполнения BIOS
46. Угроза нарушения процедуры аутентификации субъектов виртуального информационного взаимодействия
47. Угроза нарушения работоспособности грид-системы при нетипичной сетевой нагрузке

48. Угроза нарушения технологии обработки информации путём несанкционированного внесения изменений в образы виртуальных машин
49. Угроза нарушения целостности данных кеша
50. Угроза неверного определения формата входных данных, поступающих в хранилище больших данных
51. Угроза невозможности восстановления сессии работы на ПЭВМ при выводе из промежуточных состояний питания
52. Угроза невозможности миграции образов виртуальных машин из-за несовместимости аппаратного и программного обеспечения
53. Угроза невозможности управления правами пользователей BIOS
54. Угроза недобросовестного исполнения обязательств поставщиками облачных услуг
55. Угроза незащищённого администрирования облачных услуг

56. Угроза некачественного переноса инфраструктуры в облако
57. Угроза неконтролируемого копирования данных внутри хранилища больших данных
58. Угроза неконтролируемого роста числа виртуальных машин
59. Угроза неконтролируемого роста числа зарезервированных вычислительных ресурсов
60. Угроза неконтролируемого уничтожения информации хранилищем больших данных
61. Угроза некорректного задания структуры данных транзакции
62. Угроза некорректного использования прозрачного прокси-сервера за счёт плагинов браузера
63. Угроза некорректного использования функционала программного и аппаратного обеспечения

64. Угроза некорректной реализации политики лицензирования в облаке
65. Угроза неопределённости в распределении ответственности между ролями в облаке
66. Угроза неопределённости ответственности за обеспечение безопасности облака
67. Угроза неправомерного ознакомления с защищаемой информацией
68. Угроза неправомерного/некорректного использования интерфейса взаимодействия с приложением
69. Угроза неправомерных действий в каналах связи
70. Угроза непрерывной модернизации облачной инфраструктуры
71. Угроза несанкционированного восстановления удалённой защищаемой информации

72. Угроза несанкционированного выключения или обхода механизма защиты от записи в BIOS
73. Угроза несанкционированного доступа к активному и (или) пассивному виртуальному и (или) физическому сетевому оборудованию из физической и (или) виртуальной сети
74. Угроза несанкционированного доступа к аутентификационной информации
75. Угроза несанкционированного доступа к виртуальным каналам передачи
76. Угроза несанкционированного доступа к гипервизору из виртуальной машины и (или) физической сети
77. Угроза несанкционированного доступа к данным за пределами зарезервированного адресного пространства, в том числе выделенного под виртуальное аппаратное обеспечение

78. Угроза несанкционированного доступа к защищаемым виртуальным машинам из виртуальной и (или) физической сети
79. Угроза несанкционированного доступа к защищаемым виртуальным машинам со стороны других виртуальных машин
80. Угроза несанкционированного доступа к защищаемым виртуальным устройствам из виртуальной и (или) физической сети
81. Угроза несанкционированного доступа к локальному компьютеру через клиента грид-системы
82. Угроза несанкционированного доступа к сегментам вычислительного поля
83. Угроза несанкционированного доступа к системе по беспроводным каналам

84. Угроза несанкционированного доступа к системе хранения данных из виртуальной и (или) физической сети
85. Угроза несанкционированного доступа к хранимой в виртуальном пространстве защищаемой информации
86. Угроза несанкционированного изменения аутентификационной информации
87. Угроза несанкционированного использования привилегированных функций BIOS
88. Угроза несанкционированного копирования защищаемой информации
89. Угроза несанкционированного редактирования реестра
90. Угроза несанкционированного создания учётной записи пользователя
91. Угроза несанкционированного удаления защищаемой информации

92. Угроза несанкционированного удалённого внеполосного доступа к аппаратным средствам
93. Угроза несанкционированного управления буфером
94. Угроза несанкционированного управления синхронизацией и состоянием
95. Угроза несанкционированного управления указателями
96. Угроза несогласованности политик безопасности элементов облачной инфраструктуры
97. Угроза несогласованности правил доступа к большим данным
98. Угроза обнаружения открытых портов и идентификации привязанных к нему сетевых служб
99. Угроза обнаружения хостов
100. Угроза обхода некорректно настроенных механизмов аутентификации

101. Угроза общедоступности облачной инфраструктуры
102. Угроза опосредованного управления группой программ через совместно используемые данные
103. Угроза определения типов объектов защиты
104. Угроза определения топологии вычислительной сети
105. Угроза отказа в загрузке входных данных неизвестного формата хранилищем больших данных
106. Угроза отказа в обслуживании системой хранения данных суперкомпьютера
107. Угроза отключения контрольных датчиков
108. Угроза ошибки обновления гипервизора
109. Угроза перебора всех настроек и параметров приложения
110. Угроза перегрузки грид-системы вычислительными заданиями

111. Угроза передачи данных по скрытым каналам
112. Угроза передачи запрещённых команд на оборудование с числовым программным управлением
113. Угроза перезагрузки аппаратных и программно-аппаратных средств вычислительной техники
114. Угроза переполнения целочисленных переменных
115. Угроза перехвата вводимой и выводимой на периферийные устройства информации
116. Угроза перехвата данных, передаваемых по вычислительной сети
117. Угроза перехвата привилегированного потока
118. Угроза перехвата привилегированного процесса
119. Угроза перехвата управления гипервизором
120. Угроза перехвата управления средой виртуализации
121. Угроза повреждения системного реестра
122. Угроза повышения привилегий

123. Угроза подбора пароля BIOS
124. Угроза подделки записей журнала регистрации событий
125. Угроза подключения к беспроводной сети в обход процедуры аутентификации
126. Угроза подмены беспроводного клиента или точки доступа
127. Угроза подмены действия пользователя путём обмана
128. Угроза подмены доверенного пользователя
129. Угроза подмены резервной копии программного обеспечения BIOS
130. Угроза подмены содержимого сетевых ресурсов
131. Угроза подмены субъекта сетевого доступа
132. Угроза получения предварительной информации об объекте защиты

133. Угроза получения сведений о владельце беспроводного устройства
134. Угроза потери доверия к поставщику облачных услуг
135. Угроза потери и утечки данных, обрабатываемых в облаке
136. Угроза потери информации вследствие несогласованности работы узлов хранилища больших данных
137. Угроза потери управления облачными ресурсами
138. Угроза потери управления собственной инфраструктурой при переносе её в облако
139. Угроза преодоления физической защиты
140. Угроза приведения системы в состояние «отказ в обслуживании»
141. Угроза привязки к поставщику облачных услуг

142. Угроза приостановки оказания облачных услуг вследствие технических сбоев
143. Угроза программного выведения из строя средств хранения, обработки и (или) ввода/вывода/передачи информации
144. Угроза программного сброса пароля BIOS
145. Угроза пропуска проверки целостности программного обеспечения
146. Угроза прямого обращения к памяти вычислительного поля суперкомпьютера
147. Угроза распространения несанкционированно повышенных прав на всю грид-систему
148. Угроза сбоя автоматического управления системой разграничения доступа хранилища больших данных
149. Угроза сбоя обработки специальным образом изменённых файлов

150. Угроза сбоя процесса обновления BIOS
151. Угроза сканирования веб-сервисов, разработанных на основе языка описания WSDL
152. Угроза удаления аутентификационной информации
153. Угроза усиления воздействия на вычислительные ресурсы пользователей при помощи сторонних серверов
154. Угроза установки уязвимых версий обновления программного обеспечения BIOS
155. Угроза утраты вычислительных ресурсов
156. Угроза утраты носителей информации
157. Угроза физического выведения из строя средств хранения, обработки и (или) ввода/вывода/передачи информации
158. Угроза форматирования носителей информации
159. Угроза «форсированного веб-браузинга»

160. Угроза хищения средств хранения, обработки и (или) ввода/вывода/передачи информации
161. Угроза чрезмерного использования вычислительных ресурсов суперкомпьютера в ходе интенсивного обмена межпроцессорными сообщениями
162. Угроза эксплуатации цифровой подписи программного кода
163. Угроза перехвата исключения/сигнала из привилегированного блока функций
164. Угроза распространения состояния «отказ в обслуживании» в облачной инфраструктуре
165. Угроза включения в проект не достоверно испытанных компонентов
166. Угроза внедрения системной избыточности
167. Угроза заражения компьютера при посещении неблагонадёжных сайтов

168. Угроза «кражи» учётной записи доступа к сетевым сервисам
169. Угроза наличия механизмов разработчика
170. Угроза неправомерного шифрования информации
171. Угроза скрытного включения вычислительного устройства в состав бот-сети
172. Угроза распространения «почтовых червей»
173. Угроза «спама» веб-сервера
174. Угроза «фарминга»
175. Угроза «фишинга»
176. Угроза нарушения технологического/производственного процесса из-за временны́х задержек, вносимых средством защиты
177. Угроза неподтверждённого ввода данных оператором в систему, связанную с безопасностью

178. Угроза несанкционированного использования системных и сетевых утилит
179. Угроза несанкционированной модификации защищаемой информации
180. Угроза отказа подсистемы обеспечения температурного режима
181. Угроза перехвата одноразовых паролей в режиме реального времени
182. Угроза физического устаревания аппаратных компонентов
183. Угроза перехвата управления автоматизированной системой управления технологическими процессами
184. Угроза агрегирования данных, обрабатываемых с помощью мобильного устройства
185. Угроза несанкционированного изменения параметров настройки средств защиты информации

186. Угроза внедрения вредоносного кода через рекламу, сервисы и контент
187. Угроза несанкционированного воздействия на средство защиты информации
188. Угроза подмены программного обеспечения
189. Угроза маскирования действий вредоносного кода
190. Угроза внедрения вредоносного кода за счет посещения зараженных сайтов в сети Интернет
191. Угроза внедрения вредоносного кода в дистрибутив программного обеспечения
192. Угроза использования уязвимых версий программного обеспечения
193. Угроза утечки информации за счет применения вредоносным программным обеспечением алгоритмов шифрования трафика
194. Угроза несанкционированного использования привилегированных функций мобильного устройства

195. Угроза удаленного запуска вредоносного кода в обход механизмов защиты операционной системы
196. Угроза контроля вредоносной программой списка приложений, запущенных на мобильном устройстве
197. Угроза хищения аутентификационной информации из временных файлов cookie
198. Угроза скрытной регистрации вредоносной программой учетных записей администраторов
199. Угроза перехвата управления мобильного устройства при использовании виртуальных голосовых ассистентов
200. Угроза хищения информации с мобильного устройства при использовании виртуальных голосовых ассистентов
201. Угроза утечки пользовательских данных при использовании функций автоматического заполнения аутентификационной информации в браузере
202. Угроза несанкционированной установки приложений на мобильные устройства

203. Угроза утечки информации с неподключенных к сети Интернет компьютеров
204. Угроза несанкционированного изменения вредоносной программой значений параметров программируемых логических контроллеров
205. Угроза нарушения работы компьютера и блокирования доступа к его данным из-за некорректной работы СЗИ
206. Угроза отказа в работе оборудования из-за изменения геолокационной информации о нем
207. Угроза несанкционированного доступа к параметрам настройки оборудования за счет использования «мастер-кодов» (инженерных паролей)
208. Угроза нецелевого использования вычислительных ресурсов средства вычислительной техники
209. Угроза несанкционированного доступа к защищаемой памяти ядра процессора

210. Угроза нарушения работы информационной системы, вызванного обновлением используемого в ней программного обеспечения
211. Угроза использования непроверенных пользовательских данных при формировании конфигурационного файла, используемого программным обеспечением администрирования информационных систем
212. Угроза перехвата управления информационной системой
213. Угроза обхода многофакторной аутентификации

Выбор средств защиты

Уровень защищённости ПДн	Класс защиты СЗИ									Уровень контроля ПО СЗИ на отсутствие НДВ
	СВТ	САВЗ		СОВ		МЭ		СДЗ		
		В случае актуальности угроз 2 типа или при взаимодействии ИСПДн с сетями МИО	В случае актуальности угроз 3 типа и отсутствии взаимодействия ИСПДн с сетями МИО	В случае актуальности угроз 2 типа или при взаимодействии ИСПДн с сетями МИО	В случае актуальности угроз 3 типа и отсутствии взаимодействия ИСПДн с сетями МИО	В случае актуальности угроз 1 или 2 типа или при взаимодействии ИСПДн с сетями МИО	В случае актуальности угроз 3 типа и отсутствии взаимодействия ИСПДн с сетями МИО	В случае актуальности угроз 1 или 2 типа или при взаимодействии ИСПДн с сетями МИО	В случае актуальности угроз 3 типа и отсутствии взаимодействия ИСПДн с сетями МИО	
УЗ-1	Не ниже 5 класса	Не ниже 4 класса		Не ниже 4 класса		Не ниже 3 класса	Не ниже 4 класса	Не ниже 4 класса		4 уровень
УЗ-2	Не ниже 5 класса	Не ниже 4 класса		Не ниже 4 класса		Не ниже 3 класса	Не ниже 4 класса	Не ниже 4 класса		4 уровень
УЗ-3	Не ниже 5 класса	Не ниже 4 класса	Не ниже 5 класса	Не ниже 4 класса	Не ниже 5 класса	Не ниже 3 класса	Не ниже 4 класса	Не ниже 4 класса	Не ниже 5 класса	4 уровень (в случае актуальности угроз 2-го типа)
УЗ-4	Не ниже 6 класса	Не ниже 5 класса		Не ниже 5 класса		Не ниже 5 класса		Не ниже 5 класса		Требования не предъявляются

Для каждого из типов САВЗ предусмотрены шесть классов защиты, требования ужесточаются от шестого класса к первому. Каждому классу защиты соответствует определенная категория информационных систем:

— САВЗ 6 класса защиты для информационных систем персональных данных 3 и 4 классов;

— САВЗ 5 класса защиты для информационных систем персональных данных 2 класса;

— САВЗ 4 класса защиты для информационных систем персональных данных 1 класса, информационных систем общего пользования 2 класса, а также для государственных информационных систем, в которых обрабатывается информация ограниченного доступа, не содержащая сведений, составляющих государственную тайну;

— САВЗ 3, 2 и 1 классов защиты для информационных систем, в которых обрабатывается информация, содержащая сведения, составляющие государственную тайну.

относятся сетевые атаки против уязвимых сервисов, атаки, направленные на повышение привилегий, неавторизованный доступторжений используются для обнаружения некоторых типов вредоносной активности, которая может нарушить безопасность компьютерной системы. К такой активности относятся сетевые атаки против уязвимых сервисов, атаки, направленные на повышение привилегий, неавторизованный доступ к важным файлам, а также действия вредоносного программного обеспечения (компьютерных вирусовторжений используются для обнаружения некоторых типов вредоносной активности, которая может нарушить безопасность компьютерной системы. К такой активности относятся сетевые атаки против уязвимых сервисов, атаки, направленные на повышение привилегий, неавторизованный доступ к важным файлам, а также действия вредоносного программного обеспечения (компьютерных вирусов, трояновторжений используются для обнаружения некоторых типов вредоносной активности, которая может нарушить безопасность компьютерной системы. К такой активности относятся сетевые

Средства Доверенной Загрузки.

В СДЗ должны быть реализованы следующие функции безопасности:

разграничение доступа к управлению СДЗ;

управление работой СДЗ;

управление параметрами СДЗ;

аудит безопасности СДЗ;

тестирование СДЗ, контроль целостности программного обеспечения и параметров СДЗ;

контроль компонентов СВТ;

блокирование загрузки операционной системы средством доверенной загрузки;

сигнализация средства доверенной загрузки.

Термины и определения

1) **персональные данные** — **ЛЮБАЯ ИНФОРМАЦИЯ, ОТНОСЯЩАЯСЯ К** прямо или косвенно определенному или определяемому **ФИЗИЧЕСКОМУ ЛИЦУ** (субъекту персональных данных);

2) **оператор** - государственный орган, муниципальный орган, юридическое или физическое лицо, самостоятельно или совместно с другими лицами организующие и (или) осуществляющие обработку персональных данных, а также определяющие **ЦЕЛИ** обработки персональных данных**, СОСТАВ** персональных данных, подлежащих обработке, **ДЕЙСТВИЯ (операции)**, совершаемые с персональными данными;

3) **обработка персональных данных** — **ЛЮБОЕ ДЕЙСТВИЕ** (операция) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств с персональными данными, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных;

4) **автоматизированная обработка персональных данных** - обработка персональных данных с помощью средств вычислительной техники;

5) **распространение персональных данных** - действия, направленные на раскрытие персональных данных неопределенному кругу лиц;

6) **предоставление персональных данных** - действия, направленные на раскрытие персональных данных определенному лицу или определенному кругу лиц;

Термины и определения

7) **блокирование персональных данных** - временное прекращение обработки персональных данных (за исключением случаев, если обработка необходима для уточнения персональных данных);

8) **уничтожение персональных данных** - действия, в результате которых становится невозможным восстановить содержание персональных данных в информационной системе персональных данных и (или) в результате которых уничтожаются материальные носители персональных данных;

9) **обезличивание персональных данных** - действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность персональных данных конкретному субъекту персональных данных;

10) **информационная система персональных данных** - **СОВОКУПНОСТЬ** содержащихся в **БАЗАХ** данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств;

11) с**пециальные категории персональных данны**х — персональные данные касающиеся расовой, **НАЦИОНАЛЬНОЙ** принадлежности, политических взглядов, **РЕЛИГИОЗНЫХ** или философских убеждений, **СОСТОЯНИЯ ЗДОРОВЬЯ**, интимной жизни;

12) **биометрические персональные данные —** сведения, которые характеризуют физиологические и биологические особенности человека, на основании которых **МОЖНО УСТАНОВИТЬ** его **ЛИЧНОСТЬ** и которые **ИСПОЛЬЗУЮТСЯ** оператором **ДЛЯ УСТАНОВЛЕНИЯ ЛИЧНОСТИ** субъекта персональных данных.

Существенные изменения в ФЗ-152

- Ст.9 п.1. Субъект персональных данных принимает решение о предоставлении его персональных данных и дает согласие на их обработку свободно, своей волей и в своем интересе. Согласие на обработку персональных данных должно быть конкретным, информированным и сознательным. **Согласие на обработку персональных данных может быть дано субъектом персональных данных или его представителем в любой позволяющей подтвердить факт его получения форме, если иное не установлено федеральным законом.** В случае получения согласия на обработку персональных данных от представителя субъекта персональных данных полномочия данного представителя на дачу согласия от имени субъекта персональных данных проверяются оператором.
- Ст.9 п.2. Согласие на обработку персональных данных может быть отозвано субъектом персональных данных. В **случае отзыва субъектом персональных данных согласия на обработку персональных данных оператор вправе продолжить обработку персональных данных без согласия субъекта персональных данных при наличии оснований, указанных в пунктах 2 - 11 части 1 статьи 6, части 2 статьи 10 и части 2 статьи 11 настоящего Федерального закона.**
- Ст.9 п.3. Обязанность предоставить доказательство получения согласия субъекта персональных данных на обработку его персональных данных или доказательство наличия оснований, указанных в пунктах 2 - 11 части 1 статьи 6, части 2 статьи 10 и части 2 статьи 11 настоящего Федерального закона, возлагается на оператора.

Существенные изменения в ФЗ-152

- Ст. 18.1 Меры, направленные на обеспечение выполнения оператором обязанностей, предусмотренных настоящим Федеральным законом
- 1. Оператор обязан принимать меры, необходимые и достаточные для обеспечения выполнения обязанностей, предусмотренных настоящим Федеральным законом и принятыми в соответствии с ним нормативными правовыми актами. Оператор самостоятельно определяет состав и перечень мер, необходимых и достаточных для обеспечения выполнения обязанностей, предусмотренных настоящим Федеральным законом и принятыми в соответствии с ним нормативными правовыми актами, если иное не предусмотрено настоящим Федеральным законом или другими федеральными законами. К таким мерам могут, в частности, относиться:
- 1) **назначение оператором, являющимся юридическим лицом, ответственного за организацию обработки персональных данных**;
- 2) издание оператором, являющимся юридическим лицом, документов, определяющих **политику оператора** в отношении обработки персональных данных, **локальных актов по вопросам обработки** персональных данных, а также **локальных актов, устанавливающих процедуры**, направленные на **предотвращение и выявление нарушений законодательства** Российской Федерации, **устранение последствий таких нарушений**;
- 3) применение правовых, организационных и технических **мер по обеспечению безопасности** персональных данных **в соответствии со статьей 19** настоящего Федерального закона;
- 4) осуществление **внутреннего контроля и (или) аудита соответствия** обработки персональных данных настоящему Федеральному закону и принятым в соответствии с ним нормативным правовым актам, требованиям к защите персональных данных, политике оператора в отношении обработки персональных данных, локальным актам оператора;
- 5) оценка вреда, который может быть причинен субъектам персональных данных в случае нарушения настоящего Федерального закона, соотношение указанного вреда и принимаемых оператором мер, направленных на обеспечение выполнения обязанностей, предусмотренных настоящим Федеральным законом;

Существенные изменения в ФЗ-152

- 6) **ознакомление работников оператора, непосредственно осуществляющих обработку** персональных данных, **с положениями законодательства Российской Федерации о персональных данных**, в том числе **требованиями к защите** персональных данных, **документами, определяющими политику оператора** в отношении обработки персональных данных, **локальными актами по вопросам обработки** персональных данных, и (или) **обучение** указанных работников.
- 2**. Оператор обязан опубликовать или иным образом обеспечить неограниченный доступ к документу, определяющему его политику в отношении обработки персональных данных, к сведениям о реализуемых требованиях к защите персональных данных.** Оператор, осуществляющий сбор персональных данных с использованием информационно-телекоммуникационных сетей, обязан опубликовать в соответствующей информационно-телекоммуникационной сети документ, определяющий его политику в отношении обработки персональных данных, и сведения о реализуемых требованиях к защите персональных данных, а также обеспечить возможность доступа к указанному документу с использованием средств соответствующей информационно-телекоммуникационной сети.
- 3. Правительство Российской Федерации устанавливает перечень мер, направленных на обеспечение выполнения обязанностей, предусмотренных настоящим Федеральным законом и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами.
- 4. **Оператор обязан представить документы и локальные акты, указанные в части 1 настоящей статьи, и (или) иным образом подтвердить принятие мер, указанных в части 1 настоящей статьи, по запросу уполномоченного органа по защите прав субъектов персональных данных.**

Существенные изменения в ФЗ-152

- Статья 19. Меры по обеспечению безопасности персональных данных при их обработке
- 2. Обеспечение безопасности персональных данных достигается, в частности:
- 1) **определением угроз безопасности** персональных данных при их обработке в информационных системах персональных данных;
- 2) применением организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных, необходимых для выполнения требований к защите персональных данных, исполнение которых обеспечивает установленные Правительством Российской Федерации уровни защищенности персональных данных;
- 3**) применением прошедших в установленном порядке процедуру оценки соответствия средств защиты информации**;
- 4**) оценкой эффективности принимаемых мер по обеспечению безопасности** персональных данных **до ввода в эксплуатацию** информационной системы персональных данных;
- 5) учетом машинных носителей персональных данных;
- 6) **обнаружением фактов несанкционированного доступа к персональным данным и принятием мер**;
- 7) **восстановлением персональных данных**, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;
- 8) **установлением правил доступа к персональным данным**, обрабатываемым в информационной системе персональных данных, а также **обеспечением регистрации и учета всех действий, совершаемых с персональными данными в информационной системе персональных данных**;
- 9) **контролем за принимаемыми мерами** по обеспечению безопасности персональных данных и уровня защищенности информационных систем персональных данных.

Существенные изменения в ФЗ-152

- Статья 22.1. Лица, ответственные за организацию обработки персональных данных в организациях
- 1. Оператор, являющийся юридическим лицом, назначает **лицо, ответственное за организацию обработки персональных данных**.
- 2. Лицо, ответственное за организацию обработки персональных данных, **получает указания непосредственно от исполнительного органа организации, являющейся оператором, и подотчетно ему**.
- 3. Оператор обязан предоставлять лицу, ответственному за организацию обработки персональных данных, сведения, указанные в части 3 статьи 22 настоящего Федерального закона. (для подачи уведомления)
- 4. Лицо, ответственное за организацию обработки персональных данных, в частности, обязано:
- 1) **осуществлять внутренний контроль за соблюдением оператором и его работниками законодательства** Российской Федерации о персональных данных, в том числе **требований к защите** персональных данных;
- 2) **доводить до сведения работников оператора положения законодательства** Российской Федерации о персональных данных, **локальных актов по вопросам обработки персональных данных, требований к защите персональных данных**;
- 3) **организовывать прием и обработку обращений и запросов субъектов** персональных данных или их представителей и (или) **осуществлять контроль за приемом и обработкой таких обращений и запросов**.

Постановление Правительства № 687

- Фиксация на одном материальном носителе персональных данных, цели обработки которых заведомо не совместимы;
- Лица, осуществляющие обработку персональных данных без использования средств автоматизации должны быть проинформированы о факте обработки ими персональных данных, категориях обрабатываемых персональных данных, а также об особенностях и правилах осуществления такой обработки, установленных нормативными правовыми актами федеральных органов исполнительной власти, органов исполнительной власти субъектов Российской Федерации, а также локальными правовыми актами организации;
- **Типовые формы документов (анкеты, заявления, журналы, личные карточки и т. п.) должны удовлетворять требованиям:**
  - Форма должна быть утверждена приказом или использоваться утвержденная на вышестоящем уровне;
  - должны содержать сведения о цели обработки персональных данных, осуществляемой без использования средств автоматизации, имя (наименование) и адрес оператора, фамилию, имя, отчество и адрес субъекта персональных данных, источник получения персональных данных, сроки обработки персональных данных, перечень действий с персональными данными, которые будут совершаться в процессе их обработки, общее описание используемых оператором способов обработки персональных данных;
  - типовая форма должна предусматривать поле, в котором субъект персональных данных может поставить отметку о своем согласии на обработку персональных данных, осуществляемую без использования средств автоматизации, - при необходимости получения письменного согласия на обработку персональных данных;
  - типовая форма должна быть составлена таким образом, чтобы каждый из субъектов персональных данных, содержащихся в документе, имел возможность ознакомиться со своими персональными данными, содержащимися в документе, не нарушая прав и законных интересов иных субъектов персональных данных;
  - типовая форма должна исключать объединение полей, предназначенных для внесения персональных данных, цели обработки которых заведомо не совместимы

Постановление Правительства № 687

- **Журнал однократного пропуска:**
- необходимость ведения такого журнала (реестра, книги) должна быть предусмотрена актом оператора, содержащим сведения о цели обработки персональных данных, осуществляемой без использования средств автоматизации, способы фиксации и состав информации, запрашиваемой у субъектов персональных данных, перечень лиц (поименно или по должностям), имеющих доступ к материальным носителям и ответственных за ведение и сохранность журнала (реестра, книги), сроки обработки персональных данных, а также сведения о порядке пропуска субъекта персональных данных на территорию, на которой находится оператор, без подтверждения подлинности персональных данных, сообщенных субъектом персональных данных;
- копирование содержащейся в таких журналах (реестрах, книгах) информации не допускается;
- персональные данные каждого субъекта персональных данных могут заноситься в такой журнал (книгу, реестр) не более одного раза в каждом случае пропуска субъекта персональных данных на территорию, на которой находится оператор;

- **Необходимые меры:**
- Учет мест хранения материальных носителей;
- Определение лиц, осуществляющих обработку ПДн;
- Отдельное хранение носителей ПДн с разными целями;
- Защита от несанкционированного доступа носителей Пдн

ПП РФ от 01.11.2012 № 1119
Типы информационных систем

- ИСПДн, обрабатывающей специальные категории персональных данных, если в ней обрабатываются персональные данные, касающиеся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, состояния здоровья, интимной жизни субъектов персональных данных (ИСПДн-С).
- ИСПДн, обрабатывающей биометрические персональные данные, если в ней обрабатываются сведения, которые характеризуют физиологические и биологические особенности человека, на основании которых можно установить его личность и которые используются оператором для установления личности субъекта персональных данных, и не обрабатываются сведения, относящиеся к специальным категориям персональных данных (ИСПДН-Б).
- ИСПДн, обрабатывающей общедоступные персональные данные, если в ней обрабатываются персональные данные субъектов персональных данных, полученные только из общедоступных источников персональных данных, созданных в соответствии со статьей 8 Федерального закона «О персональных данных» (ИСПДн-О).
- ИСПДн, обрабатывающей иные категории персональных данных, если в ней не обрабатываются персональные данные, указанные в абзацах первом - третьем настоящего пункта (ИСПДН-И).
- ИСПДн, обрабатывающей персональные данные сотрудников оператора, если в ней обрабатываются персональные данные только указанных сотрудников. В остальных случаях информационная система персональных данных является информационной системой, обрабатывающей персональные данные субъектов

ПП РФ от 01.11.2012 № 1119
Типы угроз

- Угрозы 1-го типа актуальны для информационной системы, если для нее в том числе актуальны угрозы, связанные с наличием **недокументированных (недекларированных) возможностей в системном программном обеспечении**, используемом в информационной системе – если используем нелицензионную ОС, свободное ПО.
- Угрозы 2-го типа актуальны для информационной системы, если для нее в том числе актуальны угрозы, связанные с наличием **недокументированных (недекларированных) возможностей в прикладном программном обеспечении**, используемом в информационной системе – если используем нелицензионное ПО, свободное ПО.
- Угрозы 3-го типа актуальны для информационной системы, если для нее актуальны угрозы, не связанные с наличием недокументированных (недекларированных) возможностей в системном и прикладном программном обеспечении, используемом в информационной системе – для всех.

Классификация ИСПДн по уровням защищенности

Тип ИСПДн	Сотрудники оператора	Количество субъектов	Тип актуальных угроз		
			1	2	3
ИСПДн-С	Нет	> 100 000	УЗ-1	УЗ-1	УЗ-2
	Нет	< 100 000	УЗ-1	УЗ-2	УЗ-3
	Да				
ИСПДн-Б			УЗ-1	УЗ-2	УЗ-3
ИСПДн-И	Нет	> 100 000	УЗ-1	УЗ-2	УЗ-3
	Нет	< 100 000	УЗ-2	УЗ-3	УЗ-4
	Да				
ИСПДн-О	Нет	> 100 000	УЗ-2	УЗ-2	УЗ-4
	Нет	< 100 000	УЗ-2	УЗ-3	УЗ-4
	Да				

Требования к обеспечению уровня защищенности

Требования	Уровни защищенности			
	1	2	3	4
Режим обеспечения безопасности помещений, где обрабатываются персональные данных	+	+	+	+
Обеспечение сохранности носителей персональных данных	+	+	+	+
Перечень лиц, допущенных к персональным данным	+	+	+	+
СЗИ, прошедшие процедуру оценки соответствия *в случае, когда применение таких средств необходимо для нейтрализации актуальных угроз*	+	+	+	+
Должностное лицо, ответственное за обеспечение безопасности персональных данных в ИСПДн	+	+	+	-
Ограничение доступа к содержанию электронного журнала сообщений	+	+	-	-
Автоматическая регистрация в электронном журнале безопасности изменения полномочий сотрудника оператора по доступу к персональным данным	+	-	-	-
Структурное подразделение, ответственное за обеспечение безопасности персональных данных	+	-	-	-
Контроль за выполнением требований ПП-1119 *оператором или лицензиатом ФСТЭК не реже 1 раза в 3 года*	+	+	+	+

Контроль за выполнением требований

1. П. 4 части 2 статьи 19 № 152-ФЗ «О персональных данных» - «обеспечение безопасности персональных данных достигается в частности оценкой эффективности принимаемых мер по обеспечению безопасности персональных данных до ввода в эксплуатацию информационной системы персональных данных»
2. В соответствии с пунктом 6 приказа ФСТЭК России № 21, оценка эффективности реализованных в рамках системы защиты персональных данных мер по обеспечению безопасности персональных данных проводится оператором самостоятельно или с привлечением на договорной основе лицензиатов ФСТЭК по ТЗКИ.
3. При этом приказом ФСТЭК России № 21, форма оценки эффективности, а также форма и содержание документов, разрабатываемых по результатам (в процессе) оценки, не установлены.
4. Таким образом, решение по форме оценки эффективности и документов, разрабатываемых по результатам (в процессе) оценки эффективности, принимается оператором самостоятельно и (или) по соглашению с лицензиатом привлекаемым для проведения оценки эффективности реализованных мер по обеспечению безопасности персональных данных.

- **Ремарка:**
- **Оценка эффективности реализованных мер может быть проведена в рамках работ по аттестации информационной системы персональных данных в соответствии с национальным стандартом ГОСТ РО 0043-003-2012 «Защита информации. Аттестация объектов информатизации. Общие положения».**
- В части **государственных информационных систем**, в которых обрабатываются персональные данные, оценка эффективности принимаемых мер по обеспечению безопасности персональных данных проводится в рамках **обязательной аттестации** государственной информационной системы по требованиям защиты информации в соответствии с Требованиями, утвержденными приказом ФСТЭК России от 11 февраля 2013 г. № 17, национальными стандартами ГОСТ РО 0043-003-2012 и ГОСТ РО 0043-004-2013 «Защита информации. Аттестация объектов информатизации. Программа и методики аттестационных испытаний».

Как определяются защитные меры

- Выбор мер по обеспечению безопасности ПДн, подлежащих реализации в системе защиты ПДн, включает
  - определение базового набора мер
  - адаптацию базового набора мер с учетом структурно-функциональных характеристик ИСПДн, ИТ, особенностей функционирования ИСПДн
  - уточнение адаптированного базового набора с учетом не выбранных ранее мер
  - дополнение уточненного адаптированного базового набора мер по обеспечению безопасности ПДн дополнительными мерами, установленными иными нормативными актами

Соответствие уровней защищенности классам сертифицированных СЗИ

Тип СЗИ / ПО	4 уровень	3 уровень	2 уровень	1 уровень
СВТ	Не ниже 6	Не ниже 5	Не ниже 5	Не ниже 5
IDS	Не ниже 5	4^{2} или Интернет 5^{3}	Не ниже 4	Не ниже 4
Антивирус	Не ниже 5	4^{2} или Интернет 5^{3}	Не ниже 4	Не ниже 4
МСЭ	5	3^{2} или Интернет 4^{3}	$3^{1\text{-}2}$ или Интернет 4^{3}	$3^{1\text{-}2}$ или Интернет 4^{3}
НДВ в СЗИ	-	Не ниже 4^{2}	Не ниже 4	Не ниже 4
Системное ПО	-	-	-	-
Прикладное ПО	-	-	-	-

Соответствие 21 и 58 приказов ФСТЭК

●Приказ ФСТЭК № 21	Приказ ФСТЭК № 58
•идентификация и аутентификация субъектов доступа и объектов доступа; •управление доступом субъектов доступа к объектам доступа;	•управление доступом;
•ограничение программной среды; •защита машинных носителей информации, на которых хранятся и (или) обрабатываются персональные данные (далее - машинные носители персональных данных); •регистрация событий безопасности; •антивирусная защита; •обнаружение (предотвращение) вторжений; •контроль (анализ) защищенности персональных данных;	•Регистрация и учет; •Безопасное межсетевое взаимодействие; •Учет и хранение съемных носителей информации;
•обеспечение целостности информационной системы и персональных данных;	•Антивирусная защита; •Обнаружение вторжений; •Периодическое тестирование (анализ защищенности); •Обеспечение целостности; •Наличие средств восстановления;
•обеспечение доступности персональных данных; •защита среды виртуализации; •защита технических средств; •защита информационной системы, ее средств, систем связи и передачи данных; •выявление инцидентов (одного события или группы событий), которые могут привести к сбоям или нарушению функционирования информационной системы и (или) к возникновению угроз безопасности персональных данных (далее - инциденты), и реагирование на них; •управление конфигурацией информационной системы и системы защиты персональных данных.	•Физическая охрана помещений;

Идентификация и аутентификация субъектов доступа и объектов доступа

- Меры по идентификации и аутентификации субъектов доступа и объектов доступа должны обеспечивать присвоение субъектам и объектам доступа уникального признака (идентификатора), сравнение предъявляемого субъектом (объектом) доступа идентификатора с перечнем присвоенных идентификаторов, а также проверку принадлежности субъекту (объекту) доступа предъявленного им идентификатора (подтверждение подлинности)

Условное обозначение и номер меры	Содержание мер по обеспечению безопасности персональных данных	Уровни защищенности персональных данных			
		4	3	2	1
I. Идентификация и аутентификация субъектов доступа и объектов доступа (ИАФ)					
ИАФ.1	Идентификация и аутентификация пользователей, являющихся работниками оператора	+	+	+	+
ИАФ.2	Идентификация и аутентификация устройств, в том числе стационарных, мобильных и портативных			+	+
ИАФ.3	Управление идентификаторами, в том числе создание, присвоение, уничтожение идентификаторов	+	+	+	+
ИАФ.4	Управление средствами аутентификации, в том числе хранение, выдача, инициализация, блокирование средств аутентификации и принятие мер в случае утраты и (или) компрометации средств аутентификации	+	+	+	+
ИАФ.5	Защита обратной связи при вводе аутентификационной информации	+	+	+	+
ИАФ.6	Идентификация и аутентификация пользователей, не являющихся работниками оператора (внешних пользователей)	+	+	+	+

Управление доступом субъектов доступа к объектам доступа

•Меры по управлению доступом субъектов доступа к объектам доступа должны обеспечивать управление правами и привилегиями субъектов доступа, разграничение доступа субъектов доступа к объектам доступа на основе совокупности установленных в информационной системе правил разграничения доступа, а также обеспечивать контроль за соблюдением этих правил

Условное обозначение и номер меры	Содержание мер по обеспечению безопасности персональных данных	Уровни защищенности персональных данных			
		4	3	2	1
II. Управление доступом субъектов доступа к объектам доступа (УПД)					
УПД.1	Управление (заведение, активация, блокирование и уничтожение) учетными записями пользователей, в том числе внешних пользователей	+	+	+	+
УПД.2	Реализация необходимых методов (дискреционный, мандатный, ролевой или иной метод), типов (чтение, запись, выполнение или иной тип) и правил разграничения доступа	+	+	+	+
УПД.3	Управление (фильтрация, маршрутизация, контроль соединений, однонаправленная передача и иные способы управления) информационными потоками между устройствами, сегментами информационной системы, а также между информационными системами	+	+	+	+
УПД.4	Разделение полномочий (ролей) пользователей, администраторов и лиц, обеспечивающих функционирование информационной системы	+	+	+	+
УПД.5	Назначение минимально необходимых прав и привилегий пользователям, администраторам и лицам, обеспечивающим функционирование информационной системы	+	+	+	+
УПД.6	Ограничение неуспешных попыток входа в информационную систему (доступа к информационной системе)	+	+	+	+

Управление доступом субъектов доступа к объектам доступа

Условное обозначение и номер меры	Содержание мер по обеспечению безопасности персональных данных	Уровни защищенности персональных данных			
		4	3	2	1
УПД.7	Предупреждение пользователя при его входе в информационную систему о том, что в информационной системе реализованы меры по обеспечению безопасности персональных данных, и о необходимости соблюдения установленных оператором правил обработки персональных данных				
УПД.8	Оповещение пользователя после успешного входа в информационную систему о его предыдущем входе в информационную систему				
УПД.9	Ограничение числа параллельных сеансов доступа для каждой учетной записи пользователя информационной системы				
УПД.10	Блокирование сеанса доступа в информационную систему после установленного времени бездействия (неактивности) пользователя или по его запросу		+	+	+
УПД.11	Разрешение (запрет) действий пользователей, разрешенных до идентификации и аутентификации		+	+	+
УПД.12	Поддержка и сохранение атрибутов безопасности (меток безопасности), связанных с информацией в процессе ее хранения и обработки				
УПД.13	Реализация защищенного удаленного доступа субъектов доступа к объектам доступа через внешние информационно-телекоммуникационные сети	+	+	+	+
УПД.14	Регламентация и контроль использования в информационной системе технологий беспроводного доступа	+	+	+	+
УПД.15	Регламентация и контроль использования в информационной системе мобильных технических средств	+	+	+	+
	Управление взаимодействием с информационными				

Ограничение программной среды

- Меры по ограничению программной среды должны обеспечивать установку и (или) запуск только разрешенного к использованию в информационной системе программного обеспечения или исключать возможность установки и (или) запуска запрещенного к использованию в информационной системе программного обеспечения

III. Ограничение программной среды (ОПС)					
ОПС.1	Управление запуском (обращениями) компонентов программного обеспечения, в том числе определение запускаемых компонентов, настройка параметров запуска компонентов, контроль за запуском компонентов программного обеспечения				
ОПС.2	Управление установкой (инсталляцией) компонентов программного обеспечения, в том числе определение компонентов, подлежащих установке, настройка параметров установки компонентов, контроль за установкой компонентов программного обеспечения			+	+
ОПС.3	Установка (инсталляция) только разрешенного к использованию программного обеспечения и (или) его компонентов				+
ОПС.4	Управление временными файлами, в том числе запрет, разрешение, перенаправление записи, удаление временных файлов				

Защита машинных носителей информации, на которых хранятся и (или) обрабатываются персональные данные

- Меры по защите машинных носителей персональных данных (средств обработки (хранения) персональных данных, съемных машинных носителей персональных данных) должны исключать возможность несанкционированного доступа к машинным носителям и хранящимся на них персональным данным, а также несанкционированное использование съемных машинных носителей персональных данных.

IV. Защита машинных носителей персональных данных (ЗНИ)					
ЗНИ.1	Учет машинных носителей персональных данных			+	+
ЗНИ. 2	Управление доступом к машинным носителям персональных данных			+	+
ЗНИ.3	Контроль перемещения машинных носителей персональных данных за пределы контролируемой зоны				
ЗНИ.4	Исключение возможности несанкционированного ознакомления с содержанием персональных данных, хранящихся на машинных носителях, и (или) использования носителей персональных данных в иных информационных системах				
ЗНИ.5	Контроль использования интерфейсов ввода (вывода) информации на машинные носители персональных данных				
ЗНИ.6	Контроль ввода (вывода) информации на машинные носители персональных данных				
ЗНИ.7	Контроль подключения машинных носителей персональных данных				
ЗНИ.8	Уничтожение (стирание) или обезличивание персональных данных на машинных носителях при их передаче между пользователями, в сторонние организации для ремонта или утилизации, а также контроль уничтожения (стирания) или обезличивания		+	+	+

Регистрация событий безопасности

- Меры по регистрации событий безопасности должны обеспечивать сбор, запись, хранение и защиту информации о событиях безопасности в информационной системе, а также возможность просмотра и анализа информации о таких событиях и реагирование на них.

V. Регистрация событий безопасности (РСБ)					
РСБ.1	Определение событий безопасности, подлежащих регистрации, и сроков их хранения	+	+	+	+
РСБ.2	Определение состава и содержания информации о событиях безопасности, подлежащих регистрации	+	+	+	+
РСБ.3	Сбор, запись и хранение информации о событиях безопасности в течение установленного времени хранения	+	+	+	+
РСБ.4	Реагирование на сбои при регистрации событий безопасности, в том числе аппаратные и программные ошибки, сбои в механизмах сбора информации и достижение предела или переполнения объема (емкости) памяти				
РСБ.5	Мониторинг (просмотр, анализ) результатов регистрации событий безопасности и реагирование на них			+	+
РСБ.6	Генерирование временных меток и (или) синхронизация системного времени в информационной системе				
РСБ. 7	Защита информации о событиях безопасности	+	+	+	+

Антивирусная защита, обнаружение (предотвращение) вторжений

- Меры по антивирусной защите должны обеспечивать обнаружение в информационной системе компьютерных программ либо иной компьютерной информации, предназначенной для несанкционированного уничтожения, блокирования, модификации, копирования компьютерной информации или нейтрализации средств защиты информации, а также реагирование на обнаружение этих программ и информации.
- Меры по обнаружению (предотвращению) вторжений должны обеспечивать обнаружение действий в информационной системе, направленных на несанкционированный доступ к информации, специальные воздействия на информационную систему и (или) персональные данные в целях добывания, уничтожения, искажения и блокирования доступа к персональным данным, а также реагирование на эти действия.

VI. Антивирусная защита (АВЗ)					
АВЗ.1	Реализация антивирусной защиты	+	+	+	+
АВЗ.2	Обновление базы данных признаков вредоносных компьютерных программ (вирусов)	+	+	+	+
VII. Обнаружение вторжений (СОВ)					
СОВ.I	Обнаружение вторжений			+	+
СОВ.2	Обновление базы решающих правил			+	+

Контроль (анализ) защищенности персональных данных

- Меры по контролю (анализу) защищенности персональных данных должны обеспечивать контроль уровня защищенности персональных данных, обрабатываемых в информационной системе, путем проведения систематических мероприятий по анализу защищенности информационной системы и тестированию работоспособности системы защиты персональных данных.

VIII. Контроль (анализ) защищенности персональных данных (АНЗ)					
АНЗ.1	Выявление, анализ уязвимостей информационной системы и оперативное устранение вновь выявленных уязвимостей		+	+	+
АНЗ.2	Контроль установки обновлений программного обеспечения, включая обновление программного обеспечения средств защиты информации	+	+	+	+
АНЗ.3	Контроль работоспособности, параметров настройки и правильности функционирования программного обеспечения и средств защиты информации		+	+	+
АНЗ.4	Контроль состава технических средств, программного обеспечения и средств защиты информации		+	+	+
АНЗ.5	Контроль правил генерации и смены паролей пользователей, заведения и удаления учетных записей пользователей, реализации правил разграничения доступа, полномочий пользователей в информационной системе			+	+

Обеспечение целостности информационной системы и персональных данных

- Меры по обеспечению целостности информационной системы и персональных данных должны обеспечивать обнаружение фактов несанкционированного нарушения целостности информационной системы и содержащихся в ней персональных данных, а также возможность восстановления информационной системы и содержащихся в ней

IX.Обеспечение целостности информационной системы и персональных данных (ОЦЛ)					
ОЦЛ.1	Контроль целостности программного обеспечения, включая программное обеспечение средств защиты информации			+	+
ОЦЛ.2	Контроль целостности персональных данных, содержащихся в базах данных информационной системы				
ОЦЛ.3	Обеспечение возможности восстановления программного обеспечения, включая программное обеспечение средств защиты информации, при возникновении нештатных ситуаций				
ОЦЛ.4	Обнаружение и реагирование на поступление в информационную систему незапрашиваемых электронных сообщений (писем, документов) и иной информации, не относящихся к функционированию информационной системы (защита от спама)			+	+
ОЦЛ. 5	Контроль содержания информации, передаваемой из информационной системы (контейнерный, основанный на свойствах объекта доступа, и (или) контентный, основанный на поиске запрещенной к передаче информации с использованием сигнатур, масок и иных методов),методов), и исключение неправомерной передачи информации из информационной системы				
ОЦЛ.6	Ограничение прав пользователей по вводу информации в информационную систему				
ОЦЛ.7	Контроль точности, полноты и правильности данных, вводимых в информационную систему				
ОЦЛ.8	Контроль ошибочных действий пользователей по вводу и (или) передаче персональных данных и предупреждение пользователей об ошибочных действиях				

Обеспечение доступности персональных данных

- Меры по обеспечению доступности персональных данных должны обеспечивать авторизованный доступ пользователей, имеющих права по доступу, к персональным данным, содержащимся в информационной системе, в штатном режиме функционирования информационной системы.

X. Обеспечение доступности персональных данных (ОДТ)					
ОДТ.1	Использование отказоустойчивых технических средств				
ОДТ.2	Резервирование технических средств, программного обеспечения, каналов передачи информации, средств обеспечения функционирования информационной системы				
ОДТ.3	Контроль безотказного функционирования технических средств, обнаружение и локализация отказов функционирования, принятие мер по восстановлению отказавших средств и их тестирование				+
ОДТ.4	Периодическое резервное копирование персональных данных на резервные машинные носители персональных данных			+	+
ОДТ. 5	Обеспечение возможности восстановления персональных данных с резервных машинных носителей персональных данных (резервных копий) в течение установленного временного интервала			+	+

Защита среды виртуализации

- Меры по защите среды виртуализации должны исключать несанкционированный доступ к персональным данным, обрабатываемым в виртуальной инфраструктуре, и к компонентам виртуальной инфраструктуры и (или) воздействие на них, в том числе к средствам управления виртуальной инфраструктурой, монитору виртуальных машин (гипервизору), системе хранения данных (включая систему хранения образов виртуальной инфраструктуры), сети передачи данных через элементы виртуальной или физической инфраструктуры, гостевым операционным системам, виртуальным машинам (контейнерам), системе и сети репликации, терминальным и виртуальным устройствам, а

XI. Защита среды виртуализации (ЗСВ)					
ЗСВ.1	Идентификация и аутентификация субъектов доступа и объектов доступа в виртуальной инфраструктуре, в том числе администраторов управления средствами виртуализации	+	+	+	+
ЗСВ.2	Управление доступом субъектов доступа к объектам доступа в виртуальной инфраструктуре, в том числе внутри виртуальных машин	+	+	+	+
ЗСВ.3	Регистрация событий безопасности в виртуальной инфраструктуре		+	+	+
ЗСВ.4	Управление (фильтрация, маршрутизация, контроль соединения, однонаправленная передача) потоками информации между компонентами виртуальной инфраструктуры, а также по периметру виртуальной инфраструктуры				
ЗСВ.5	Доверенная загрузка серверов виртуализации, виртуальной машины (контейнера), серверов управления виртуализацией				
ЗСВ.6	Управление перемещением виртуальных машин (контейнеров) и обрабатываемых на них данных			+	+
ЗСВ.7	Контроль целостности виртуальной инфраструктуры и ее конфигураций			+	+
ЗСВ. 8	Резервное копирование данных, резервирование технических средств, программного обеспечения виртуальной инфраструктуры, а также каналов связи внутри виртуальной инфраструктуры			+	+
	Реализация и управление антивирусной защитой в				

Защита технических средств

- Меры по защите технических средств должны исключать несанкционированный доступ к стационарным техническим средствам, обрабатывающим персональные данные, средствам, обеспечивающим функционирование информационной системы (далее - средства обеспечения функционирования), и в помещения, в которых они постоянно расположены, защиту технических средств от внешних воздействий, а также защиту персональных данных, представленных в виде информативных электрических сигналов и физических полей.

XII. Защита технических средств (ЗТС)					
ЗТС.1	Защита информации, обрабатываемой техническими средствами, от ее утечки по техническим каналам				
ЗТС.2	Организация контролируемой зоны, в пределах которой постоянно размещаются стационарные технические средства, обрабатывающие информацию, и средства защиты информации, а также средства обеспечения функционирования				
ЗТС.3	Контроль и управление физическим доступом к техническим средствам, средствам защиты информации, средствам обеспечения функционирования, а также в помещения и сооружения, в которых они установлены, исключающие несанкционированный физический доступ к средствам обработки информации, средствам защиты информации и средствам обеспечения функционирования информационной системы, в помещения и сооружения, в которых они установлены	+	+	+	+
ЗТС.4	Размещение устройств вывода (отображения) информации, исключающее ее несанкционированный просмотр	+	+	+	+
ЗТС.5	Защита от внешних воздействий (воздействий окружающей среды, нестабильности электроснабжения, кондиционирования и иных внешних факторов)				

Защита информационной системы, ее средств, систем связи и передачи данных

- Меры по защите информационной системы, ее средств, систем связи и передачи данных должны обеспечивать защиту персональных данных при взаимодействии информационной системы или ее отдельных сегментов с иными информационными системами и информационно-телекоммуникационными сетями посредством применения архитектуры информационной системы и проектных решений, направленных на обеспечение безопасности персональных данных.

XIII. Защита информационной системы, ее средств, систем связи и передачи данных (ЗИС)					
ЗИС.1	Разделение в информационной системе функций по управлению (администрированию) информационной системой, управлению (администрированию) системой защиты персональных данных, функций по обработке персональных данных и иных функций информационной системы				+
ЗИС.2	Предотвращение задержки или прерывания выполнения процессов с высоким приоритетом со стороны процессов с низким приоритетом				
ЗИС.3	Обеспечение защиты персональных данных от раскрытия, модификации и навязывания (ввода ложной информации) при ее передаче (подготовке к передаче) по каналам связи, имеющим выход за пределы контролируемой зоны, в том числе беспроводным каналам связи	+	+	+	+
ЗИС.4	Обеспечение доверенных канала, маршрута между администратором, пользователем и средствами защиты информации (функциями безопасности средств защиты информации)				
ЗИС. 5	Запрет несанкционированной удаленной активации видеокамер, микрофонов и иных периферийных устройств, которые могут активироваться удаленно, и оповещение пользователей об активации таких устройств				
	Передача и контроль целостности атрибутов безопасности (меток безопасности), связанных с				

Защита информационной системы, ее средств, систем связи и передачи данных

XIII. Защита информационной системы, ее средств, систем связи и передачи данных (ЗИС)					
ЗИС. 7	Контроль санкционированного и исключение несанкционированного использования технологий мобильного кода, в том числе регистрация событий, связанных с использованием технологий мобильного кода, их анализ и реагирование на нарушения, связанные с использованием технологий мобильного кода				
ЗИС. 8	Контроль санкционированного и исключение несанкционированного использования технологий передачи речи, в том числе регистрация событий, связанных с использованием технологий передачи речи, их анализ и реагирование на нарушения, связанные с использованием технологий передачи речи				
ЗИС.9	Контроль санкционированной и исключение несанкционированной передачи видеоинформации, в том числе регистрация событий, связанных с передачей видеоинформации, их анализ и реагирование на нарушения, связанные с передачей видеоинформации				
ЗИС.10	Подтверждение происхождения источника информации, получаемой в процессе определения сетевых адресов по сетевым именам или определения сетевых имен по сетевым адресам				
ЗИС.11	Обеспечение подлинности сетевых соединений (сеансов взаимодействия), в том числе для защиты от подмены сетевых устройств и сервисов			+	+
	Исключение возможности отрицания пользователем факта отправки персональных данных другому				

Защита информационной системы, ее средств, систем связи и передачи данных

XIII. Защита информационной системы, ее средств, систем связи и передачи данных (ЗИС)					
ЗИС.13	Исключение возможности отрицания пользователем факта получения персональных данных от другого пользователя				
ЗИС.14	Использование устройств терминального доступа для обработки персональных данных				
ЗИС.15	Защита архивных файлов, параметров настройки средств защиты информации и программного обеспечения и иных данных, не подлежащих изменению в процессе обработки персональных данных			+	+
ЗИС.16	Выявление, анализ и блокирование в информационной системы скрытых каналов передачи информации в обход реализованных мер или внутри разрешенных сетевых протоколов				
ЗИС.17	Разбиение информационной системы на сегменты (сегментирование информационной системы) и обеспечение защиты периметров сегментов информационной системы			+	+
ЗИС.18	Обеспечение загрузки и исполнения программного обеспечения с машинных носителей персональных данных, доступных только для чтения, и контроль целостности данного программного обеспечения				
ЗИС.19	Изоляция процессов (выполнение программ) в выделенной области памяти				
ЗИС.20	Защита беспроводных соединений, применяемых в информационной системе		+	+	+

Защита выявление инцидентов, которые могут привести к сбоям или нарушению функционирования информационной системы и (или) к возникновению угроз безопасности персональных данных и реагирование на них

- Меры по выявлению инцидентов и реагированию на них должны обеспечивать обнаружение, идентификацию, анализ инцидентов в информационной системе, а также принятие мер по устранению и предупреждению инцидентов.

XIV. Выявление инцидентов и реагирование на них (ИНЦ)					
ИНЦ.1	Определение лиц, ответственных за выявление инцидентов и реагирование на них			+	+
ИНЦ.2	Обнаружение, идентификация и регистрация инцидентов			+	+
ИНЦ.3	Своевременное информирование лиц, ответственных за выявление инцидентов и реагирование на них, о возникновении инцидентов в информационной системе пользователями и администраторами			+	+
ИНЦ.4	Анализ инцидентов, в том числе определение источников и причин возникновения инцидентов, а также оценка их последствий			+	+
ИНЦ. 5	Принятие мер по устранению последствий инцидентов			+	+
ИНЦ. 6	Планирование и принятие мер по предотвращению повторного возникновения инцидентов			+	+

Управление конфигурацией информационной системы и системы защиты персональных данных

- Меры по выявлению инцидентов и реагированию на них должны обеспечивать обнаружение, идентификацию, анализ инцидентов в информационной системе, а также принятие мер по устранению и предупреждению инцидентов.

XV. Управление конфигурацией информационной системы и системы защиты персональных данных (УКФ)					
УКФ.1	Определение лиц, которым разрешены действия по внесению изменений в конфигурацию информационной системы и системы защиты персональных данных		+	+	+
УКФ.2	Управление изменениями конфигурации информационной системы и системы защиты персональных данных		+	+	+
УКФ.3	Анализ потенциального воздействия планируемых изменений в конфигурации информационной системы и системы защиты персональных данных на обеспечение защиты персональных данных и согласование изменений в конфигурации информационной системы с должностным лицом (работником), ответственным за обеспечение безопасности персональных данных		+	+	+
УКФ.4	Документирование информации (данных) об изменениях в конфигурации информационной системы и системы защиты персональных данных		+	+	+

Что подлежит лицензированию ФСТЭК и ФСБ

- **Федеральный закон Российской Федерации от 4 мая 2011 г. N 99-ФЗ "О лицензировании отдельных видов деятельности"**
- **Глава 2. Статья 12. п. 1.** В соответствии с настоящим Федеральным законом лицензированию подлежат следующие виды деятельности:

1) разработка, производство, распространение шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, выполнение работ, оказание услуг в области шифрования информации, техническое обслуживание шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (крипто графических) средств (за исключением случая, если техническое обслуживание шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, осуществляется для обеспечения собственных нужд юридического лица или индивидуального предпринимателя);

5) деятельность по технической защите конфиденциальной информации;

- **Положение о лицензировании деятельности по технической защите конфиденциальной информации, утв. Постановлением Правительства РФ от 03 февраля 2012г № 79.**

Положение о лицензировании деятельности по технической защите конфиденциальной информации, утв. Постановлением Правительства РФ от 03 февраля 2012г № 79.

- 4. При осуществлении деятельности по технической защите конфиденциальной информации лицензированию подлежат следующие виды работ и услуг:
- а) контроль защищенности конфиденциальной информации от утечки по техническим каналам в: …

- б) контроль защищенности конфиденциальной информации от несанкционированного доступа и ее модификации в средствах и системах информатизации;

- в) сертификационные испытания на соответствие требованиям по безопасности информации продукции…;

- г) аттестационные испытания и аттестация на соответствие требованиям по защите информации:
- средств и систем информатизации;
- помещений со средствами (системами) информатизации, подлежащими защите;
- защищаемых помещений;

- д) **проектирование в защищенном исполнении**:
- **средств и систем информатизации; `разработка технического задания на создание системы защиты ПДн, проект, описание`**
- помещений со средствами (системами) информатизации, подлежащими защите;
- защищаемых помещений;

- е) **установка, монтаж, испытания, ремонт средств защиты информации** (технических средств защиты информации, защищенных технических средств обработки информации, технических средств контроля эффективности мер защиты информации, программных (программно-технических) средств защиты информации, защищенных программных (программно-технических) средств обработки информации, программных

Показательный пример (электронная очередь «детские сады»)

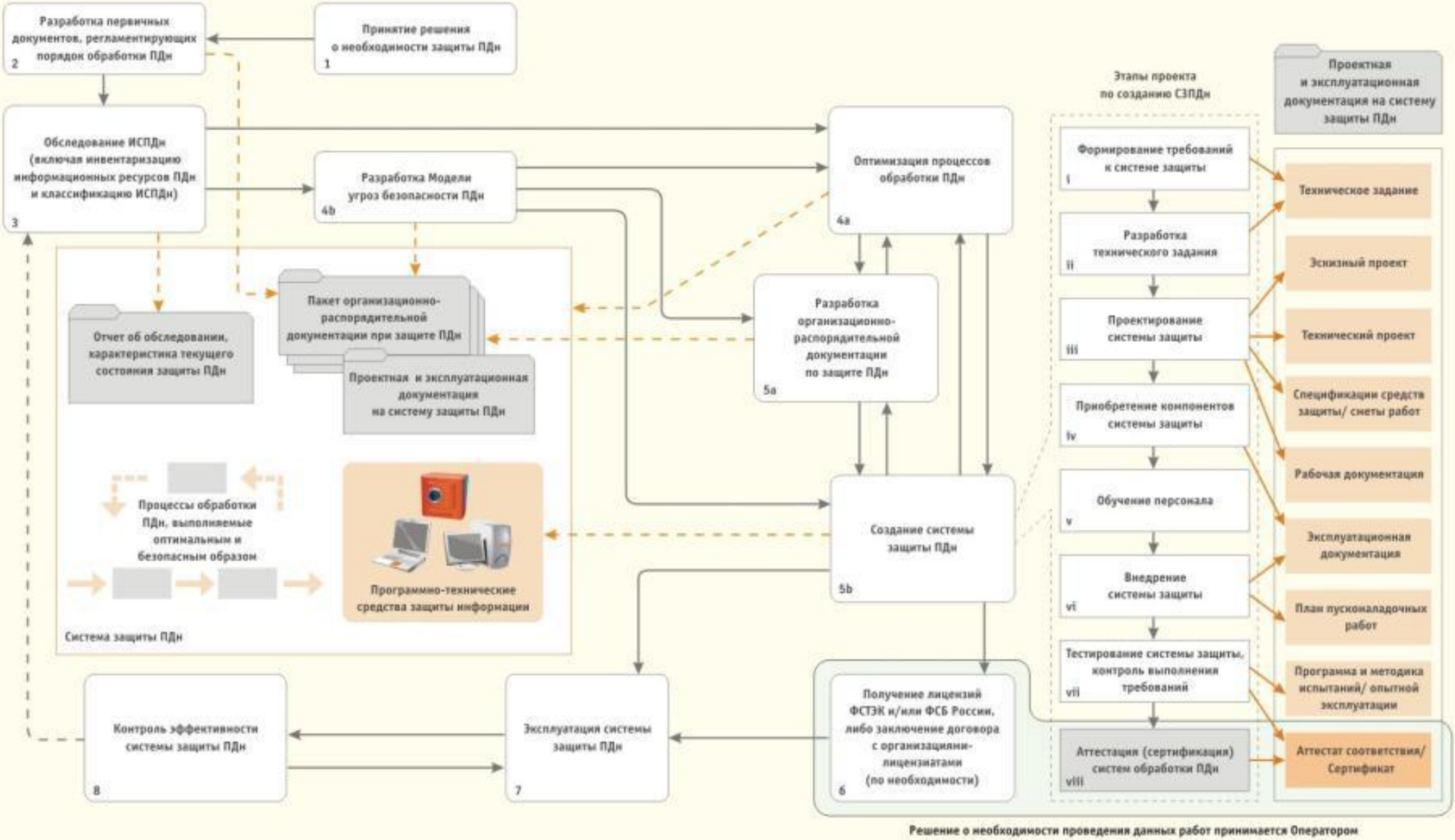
№ п/п	Наименование	Цена, руб./ед.	Кол-во, ед.	Итого, руб.
Сертифицированное средство защиты информации от несанкционированного доступа				
1	КСЗИ «Панцирь-К»	4 500,00	1	**4 500,00**
Сертифицированный межсетевой экран с функцией обнаружения вторжений, антивирус				
2	Право на использование Средств защиты информации Security Studio Endpoint Protection: Antivirus, Personal Firewall, HIPS.	2 900,00	1	2 900,00
3	Установочный комплект Security Studio Endpoint Protection: Antivirus, Personal Firewall, HIPS.	250,00	1	250,00
4	Установка и настройка, год гарантии	3 840,00	1	3 840,00
	Общая стоимость			**11 490,00**

11 шагов по выполнению требования закона «О персональных данных»

- **Предпроектное обследование**
- Шаг 1. Определить должностное лицо, ответственное за организацию обработки ПДн
- Шаг 2. Определить состав обрабатываемых ПДн, цели и условия обработки. Определить срок хранения ПДн
- Шаг 3. Получить согласие субъекта на обработку его ПДн, в том числе в письменной форме
- Шаг 4. Определить порядок реагирования на запросы со стороны субъектов ПДн
- Шаг 5. Оптимизировать процесс обработки ПДн
- Шаг 6. Разработать модель угроз ПДн при обработке в ИСПДн. Классифицировать ИСПДн
- Шаг 7. Определить необходимость уведомления уполномоченного органа по защите ПДн о начале обработки ПДн. Если необходимость есть, то составить и отправить уведомление
- Шаг 8. Определить перечень мер по защите ПДн, обрабатываемых без использования средств автоматизации
- **Проектирование и внедрение системы защиты персональных данных**
- Шаг 9. Спроектировать и реализовать систему защиты ПДн
- **Оценка соответствия системы защиты ПДн заявленным требованиям**
- Шаг 10. Провести оценку эффективности принимаемых мер по обеспечению безопасности ПДн до ввода в эксплуатацию ИСПДн
- **Эксплуатация системы защиты ПДн**
- Шаг 11. Обеспечить постоянный контроль защищенности ПДн

Схема осуществления защиты ПДн

Последовательность шагов по выполнению требований ФЗ «О персональных данных»



Шаг 1. Определить должностное лицо, ответственное за организацию обработки ПДн

- Назначить приказом должностное лицо, ответственное за организацию обработки ПДн. Им может быть:
- Руководитель организации;
- Заместитель руководителя;
- Начальник структурного подразделения, осуществляющего обработку ПДн или ответственного за обеспечение безопасности Пдн

Шаг 2. Определить состав обрабатываемых ПДн, цели и условия обработки. Определить срок хранения ПДн

- 1. Приказом утвердить комиссию по проведению работ по организации системы защиты персональных данных и возложить на нее обязанности по проведению внутренней проверки.
- 2. Провести внутреннюю проверку или обследования сторонней организацией (лицензиатом) с подготовкой:
- акта обследования информационной системы;
- перечня ИСПДн;
- перечня ПДн;
- матрицы доступа сотрудников к ПДн;
- Приказа об установлении границ контролируемой зоны;
- Приказа об утверждении мест хранения материальных носителей ПДн;
- План по приведению ИСПДн в соответствие с требованиями ФЗ «О персональных данных»;
- Предварительный список лиц (категорий лиц), допущенных к работе с ПДн;
- Разработать и получить с сотрудников обязательство о неразглашении конфиденциальной информации

Шаг 3. Получить согласие субъекта на обработку его ПДн, в том числе в письменной форме

1. Определить необходимость получения согласия на обработку ПДн субъекта на основании действующих законов и подзаконных актах;
2. Разработать типовую форму согласия на обработку ПДн или проект внесения изменений в договора и(или) положения учреждения (если необходимо);
3. Получить согласие субъектов на обработку ПДн (утвердить и ознакомить субъектов ПДн с изменениями в договорах и положении учреждения);

- **Когда не нужно брать отдельное согласие на обработку ПДн:**

1. Участие в ЕГЭ (ПП-36);
2. Прием граждан в ВУЗ (Приказ Минобрнауки № 2895)

- 3. Обработка ПДн:
- для осуществления и выполнения возложенных законодательством Российской Федерации на оператора функций, полномочий и обязанностей;
- для исполнения договора, стороной которого либо выгодоприобретателем или поручителем по которому является субъект ПДн, а также для заключения договора по инициативе субъекта ПДн или договора, по которому субъект ПДн будет являться выгодоприобретателем или поручителем;
- о персональном составе работников с указанием уровня образования и квалификации.

- **Шаг 4. Определить порядок реагирования на запросы со стороны субъектов ПДн**

1. Определить лиц, ответственных за соблюдение требований ФЗ «О персональных данных» в части реагирования на запросы субъектов ПДн (кто и в каких случаях будет отвечать на запросы субъектов);
2. Определить регламент реагирования на запросы субъектов ПДн (может осуществляться согласно действующих регламентных процедур);
3. Разработать журнал учета обращений субъектов ПДн о выполнении их законных прав

Шаг 5. Оптимизировать процесс обработки ПДн

- Отдельный слайд

Шаг 6. Разработать модель угроз ПДн при обработке в ИСПДн. Классифицировать ИСПДн

1. Согласно полученных при обследовании данных разработать модель угроз безопасности ПДн при их обработке в ИСПДн согласно нормативных документов ФСТЭК и ФСБ или поручить такую разработку лицензиату ФСТЭК.
2. Утвердить модель угроз ПДн
3. Комиссией из 3-х человек, назначенных приказом провести классификацию ИСПДн

Шаг 7. Определить необходимость уведомления уполномоченного органа по защите ПДн о начале обработки ПДн. Если необходимость есть, то составить и отправить уведомление

1. Зайти на сайт РОСКОМНАДЗОРА и ознакомится с рекомендациями по заполнению образца уведомления http://www.pd.rsoc.ruhttp://www.pd.rsoc.ru/http://www.pd.rsoc.ru/operators-registry/operators-registry-documents/
2. Подготовить уведомление по шаблону или через электронную форму http://www.pd.rsoc.ru/operators-registry/notification/
3. Распечатать уведомление, подписать, заверить печатью и отправить почтой или нарочным в Управление РОСКОМНАДЗОРа по РБ (450005, Республика Башкортостан, г. Уфа, ул. 50 лет Октября, 20/1)
4. Если уведомление уже подано, то у Вас есть срок до 1 января 2013 года отправить изменения к уведомлению
5. В случае, если Вы проводите изменения в обработке ПДн, изменения в системе защите ПДн Вы также обязаны в течение 14 дней с момента изменений внести изменения в уведомление и отправить в РОСКОМНАДЗОР.

Шаг 8. Определить перечень мер по защите ПДн, обрабатываемых без использования средств автоматизации

1. Список лиц, допущенных к обработке ПДн;
2. Перечень материальных носителей ПДн;
3. Перечень мест хранения материальных носителей ПДн;
4. Инструкция по обработке ПДн в неавтоматизированном виде (доступ, хранение, внесение уточнений, защита от утечек по видовым каналам);

Шаг 9. Спроектировать и реализовать систему защиты ПДн

1. Формирование требований к системе защиты ПДн;
2. Разработка технического задания на создание системы защиты ПДн;
3. Разработка комплекта организационно-распорядительной документации по защите ПДн;
4. Оптимизация процесса обработки ПДн;
5. Проектирование системы защиты ПДн;
6. Приобретение компонентов системы защиты;
7. Внедрение компонентов защиты;
8. Обучение персонала;
9. Тестирование системы защиты;

Шаг 10. Провести оценку эффективности принимаемых мер по обеспечению безопасности ПДн до ввода в эксплуатацию ИСПДн

- 1. Для государственных информационных систем (ЕГЭ) - аттестация (требования СТР-К);
- 2. Для муниципальных информационных систем (кадры УО, данные в РИС, МИС) – рекомендовано проводить оценку также как и для государственных информационных систем.

Шаг 11. Обеспечить постоянный контроль защищенности ПДн

- 1. Осуществление внутреннего контроля и (или) аудита соответствия обработки персональных данных ФЗ-152 «О персональных данных» и принятыми в соответствие с ним нормативным правовым актам, требованиям к защите персональных данных, политике оператора в отношении обработки персональных данных, локальным актам оператора (п.п. 4 п. 1 ст 18.1 Фз-152);
- 2. Контроль за принимаемыми мерами по обеспечению безопасности персональных данных и уровня защищенности информационных систем персональных данных;
- 3. Доводить до сведения работников оператора положения законодательства Российской Федерации о персональных данных, локальных актов по вопросам обработки персональных данных, требований к защите персональных данных;

Примерный перечень документов в по обработке ПДн

- Техническая документация:

1. Акт обследования информационной системы
2. Модель угроз безопасности ПДн
3. Акт определения уровня защищенности ПДн
4. Техническое задание на создание системы защиты ПДн
5. Описание системы защиты ПДн
6. Технический паспорт

- Организационно-распорядительные документы:

1. Приказ о назначении ответственного за обработку персональных данных
2. План по приведению в соответствие ИСПДн требованиям ФЗ «О персональных данных»
3. Приказ о создании комиссии по определению уровня защищенности персональных данных
4. Список лиц (категорий лиц), допущенных к работе с ПДн
5. Матрица доступа сотрудников
6. Приказ об установлении границ контролируемой зоны
7. План внутренних проверок состояния системы защиты персональных данных
8. Приказ об установлении мест хранения материальных носителей
9. Перечень ИСПДн
10. Перечень персональных данных, обрабатываемых в ИСПДн
11. Политика обработки персональных данных
12. Положение о порядке обработки персональных данных
13. Форма акта об уничтожении персональных данных
14. Обязательство о конфиденциальности
15. Типовая форма согласия субъекта на обработку персональных данных
16. Уведомление об обработке персональных данных

Примерный перечень документов по обработке ПДн

18. Инструкция ответственного за обеспечение безопасности персональных данных
19. Инструкция пользователя информационной системы персональных данных
20. Инструкция по организации парольной защиты
21. Инструкция по антивирусной защите
22. Регламент резервного копирования
23. Инструкция по неавтоматизированной обработке персональных данных
24. Правила рассмотрения обращений граждан с типовыми формами запросов и ответов
25. Формы дополнительных соглашений с третьими лицами

- Журналы:

1. Перечень по учету применяемых средств защиты информации, эксплуатационной и технической документации к ним.
2. Журнал учета машинных носителей персональных данных
3. Журнал учёта обращений субъектов ПДн о выполнении их законных прав
4. Журнал учета ремонтно-восстановительных работ на основных технических средствах
5. Журнал регистрации попыток к несанкционированного доступа к информации
6. Журнал поэкземплярного учета СКЗИ
7. Технический (аппаратный) журнал

- Документы по установки средств защиты информации и средств криптографической защиты информации:

1. Заключение о возможности эксплуатации
2. Журнал учета используемых криптосредств, эксплуатационной и технической документации к ним
3. Инструкция по обеспечению безопасности с использованием СКЗИ
4. Лицевой счет пользователя СКЗИ
5. Приказ о допуске сотрудников к работе с СКЗИ
6. Приказ о назначении ответственного пользователя СКЗИ
7. Программа обучения
8. Инструкция ответственного пользователя СКЗИ

Факторы, влияющие на построение системы защиты персональных данных

- Отсутствие технологических карт процессов обработки персональных данных;
- Отсутствие единого подхода к построению ИС учреждения;
- Подключение к сетям общего пользования;
- Доступ обучающихся к сегментам ИСПДн;
- Трудности отслеживания хранения ПДн у учителей.

Оптимизация затрат на техническую защиту ПДн. Что необходимо?

- Когда Вы уже сделали акт обследования, модель угроз, техническое задание и расчет стоимости внедрения системы защиты можно осуществлять оптимизацию.
- Что для этого необходимо:

1. Составить технологические карты процессов обработки персональных данных;
2. Выявить узкие места в обработке персональных данных (самые затратные);
3. Определить пути оптимизации процессов обработки;
4. Провести тестирование новых процессов на отдельных участках ИСПДн;
5. Утвердить полученные результаты, разработать документы регламентирующие новые процессы обработки ПДн;
6. Разработать технический проект на АС в защищенном исполнении.

Оптимизация затрат на техническую защиту ПДн. 8 законных способов снижения стоимости технической защиты персональных данных

- Переход на неавтоматизированную обработку ПДн

1. Объединение / разделение ИСПДн
2. Снижение категории ПДн
3. Снижение объема обрабатываемых ПДн на ПК
4. Снижение числа ПК, обрабатывающих ПДн
5. Снижение числа точек подключения к СОП
6. Обезличивание ПДн
7. Выделение ИСПДн из общей локальной сети в отдельную подсеть
8. Снижение класса ИСПДн путем сегментирования (Сервера класс К1/К2, АРМ – К3)

Рекомендации по внедрению новых программных комплексов

- Необходимо учитывать:

1. Какие ПДн будут обрабатываться;
2. Кто будет иметь доступ к программному комплексу;
3. Есть ли встроенные СЕРТИФИЦИРОВАННЫЕ ФСТЭК или ФСБ механизмы защиты;

- Правильнее всего при выборе программных комплексов проводить экспертизу сторонней компанией, специализирующей на защите информации, чтобы определить возможность безопасной эксплуатации данной ИСПДн, стоимость защиты, и возможные варианты снижения стоимости.
- Почему сторонней компанией – не заинтересована в продаже конкретного программного комплекса.

Обязанности ответственного за организацию обработки персональных данных

Знать:

Все нормативные акты в области персональных данных, включая технические документы ФСТЭК и ФСБ;

Уметь:

Разрабатывать технологические карты обработки персональных данных;

Разрабатывать организационно-распорядительные документы по обработке и защите персональных данных;

Определять актуальные угрозы безопасности персональных данных;

Администрировать средства защиты информации;

Проводить разбирательства в случае несанкционированного доступа к персональным данным;

Делать:

Постоянно осуществлять мониторинг появления новых нормативных актов в области информационной безопасности и обработке персональных данных;

Проводить мероприятия в соответствие с планом внутренних проверок;

Информировать сотрудников о положениях законодательства и внутренних актах;

Участвовать в проведении проверок РОСКОМНАДЗОРа.