

Общество с ограниченной ответственностью  
«5.25 Защитные решения»

АО "ГОРЭЛЕКТРОСЕТЬ" Г.НЕВИННОМЫССК

359300, Калмыкия Респ, м.р-н Юстинский,  
с.п.Цаганаманское, п Цаган Аман, ул Хомутникова,  
д. 17  
телефон и факс: 8 (495) 108-76-25  
www.5-25.ru  
ОГРН 1220800003511  
ИНН/КПП 0800005343/ 080001001

от 15/04/2024 № 223-24041515  
на № \_\_\_\_\_ от \_\_\_\_\_ / /

Тема:  
на запрос

Добрый день!

В целях достижения соответствия ФЗ-№152 от 27 июля 2006 года «О персональных данных», ФЗ-№149 от 27 июня 2006 года «Об информации, информационных технологиях и о защите информации», ПП РФ от 01 ноября 2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», предлагаю Вам воспользоваться предложением комплекса услуг по актуализации организационно-правовых требований и построению системы защиты персональных данных с учетом 1500 автоматизированного рабочего места, а также реализации требований Федерального закона от 26 июля 2017 г. № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации»:

Наименование	Описание	Стоимость, рублей
<b>1 этап. Обследование процессов обработки персональных данных с учетом 50-ти автоматизированных рабочих мест.</b>		
Цель работ	Определение текущей степени соответствия процессов обработки и защиты персональных данных действующим требованиям законодательства Российской Федерации в области персональных данных.	
Состав работ	<ul style="list-style-type: none"> <li>– анализ организационно-штатной структуры;</li> <li>– выявление и описание процессов обработки персональных данных;</li> <li>– определение состава обрабатываемых персональных данных;</li> <li>– выявление и описание информационных ресурсов, содержащих персональные данные;</li> <li>– описание технологий обработки персональных данных;</li> <li>– описание существующих организационных мер и технических средств, направленных на обеспечение защиты персональных данных;</li> <li>– описание имеющихся мер и средств защиты информации в информационных системах персональных данных;</li> <li>– определение перечня мероприятий необходимых для приведения процессов обработки и защиты персональных данных действующим требованиям законодательства российской федерации в области персональных данных;</li> <li>– анализ существующих мер защиты персональных данных.</li> </ul>	
Результат работ	Обследование и документация (см Приложение №2.1)	
<b>ИТОГО за документацию ФЗ-152:</b>		<b>147 000,00</b>
<b>2 этап. Обследование объектов КИИ.</b>		

Состав работ	Обследование критической информационной инфраструктуры (далее – КИИ) на соответствие требованиями законодательства: определим критические процессы, сформируем перечень объектов КИИ, подлежащих категорированию, определим актуальные угрозы и способы их устранения, разработаем план мероприятий по выполнению требований Ф3-18; категорирование объектов КИИ, сбор, оформление сведений о результатах присвоения объектам КИИ категории значимости для направления результатов категорирования объектов КИИ в ФСТЭК России; разработка системы защиты информационных систем и режимных мер; разработка организационно-распорядительной документации, регламентирующих правила и процедуры обеспечения безопасности объектов КИИ.	
Результат работ	Перечень объектов КИИ; Сведения о результатах категорирования объектов КИИ; Акты категорирования объектов КИИ; Сопроводительное письмо во ФСТЭК (документы см Приложение №2.2).	
ИТОГО за документацию КИИ:		328 000,00
ВСЕГО:		475 000,00

В комплекс услуг входит обучение ответственного за организацию безопасной обработки персональных данных, сопровождение 12 календарных месяцев: консультации пользователей информационных системах персональных данных, ответы на вопросы пользователей информационных системах персональных данных, бесплатное участие в семинарах по безопасности.

Приложение №1. Структура информационных услуг по обследованию

Приложение №2. Перечень проектов документов

Приложение №3. Предварительный расчет

Приложение №4. Ответственность за нарушение

Директор




Дейнека Д. О.

Исп.: Балбаева Кулянжан Куспантаевна, начальник отдела  
Тел.: +7 (8512) 525 025; +7 800 3025 525  
e-mail: [ib@5-25.ru](mailto:ib@5-25.ru)

**Приложение №1.1. Структура информационных услуг по обследованию ИСПДн\*.**

Наименование	Кол-во
Сбор данных о техническом и программном составе защищаемой информационной системы	1
Сбор данных об архитектуре защищаемой информационной системы	1
Определение и анализ целей защиты информации по каждому типу персональных данных (далее ПДн)	1
Определение и анализ целей информационных потоков защищаемой системы, точек их обработки, пересечения, мест и способов хранения информации	1
Определение и анализ существующих организационных решений (регламентирующих документов, актов классификации и др. документов)	1
Определение форм представления, хранения, обработки и передачи информации	1
Определение, сопоставление между информацией и техническими составляющими информационной системы, участвующими в процессе её обработки, хранения и передачи	1
Определение, сопоставление между целями защиты информации и конкретной информацией и информационными потоками в защищаемой информационной системе	1
Сбор данных о технологических процессах в информационной системе	1
Сбор данных об организационной структуре	1
Определение используемых средств и механизмов защиты информации	1

\* результатом работ является Отчет со следующими данными: категории персональных данных, определенное множество информационных систем персональных данных, состав и структура определенных информационных систем персональных данных, модель информационных потоков, рекомендации по созданию системы организационно-технических мероприятий по обеспечению безопасности ПДн и т.д.

**Приложение №1.2.** Структура информационных услуг по категорированию объектов КИИ (установление соответствия объекта критической информационной инфраструктуры критериям значимости и показателям их значений, присвоение ему одной из категорий значимости, проверка сведений о результатах ее присвоения)\*.

Наименование	Кол-во
Определение перечня всех процессов, выполняемых в рамках деятельности субъекта КИИ.	1
Выявление критических процессов, то есть процессов, нарушение и (или) прекращение которых может привести к негативным социальным, политическим, экономическим, экологическим последствиям, последствиям для обеспечения обороны страны, безопасности государства и правопорядка.	1
Определение объектов КИИ, которые обрабатывают информацию, необходимую для обеспечения критических процессов, управления и контроля ими.	1
Формирование перечня объектов КИИ, подлежащих категорированию. Перечень объектов для категорирования после утверждения направляется во ФСТЭК России.	1
Оценка масштаба возможных последствий в случае возникновения компьютерных инцидентов на объектах КИИ в соответствии с показателями, указанных в Правилах. Всего предусматривается 14 показателей, определяющих социальную, политическую, экономическую значимость объекта КИИ, а также его значимость для обеспечения правопорядка, обороны и безопасности страны.	1
Присвоение каждому из объектов КИИ одной из категорий значимости в соответствии с наивысшим значением показателей, либо принятие решения об отсутствии необходимости присвоения категории.	1
Подготовка необходимого пакета организационно-распорядительной документации, предоставление проектов документов в электронном виде Заказчику.	1

\* категорирование будет проводиться как для существующих, так и для создаваемых или модернизируемых объектов КИИ и оформляется соответствующим актом, который в течение 10 дней после его утверждения, должен быть направлен во ФСТЭК России. Предоставленные материалы в тридцатидневный срок со дня получения проверяются регулятором на соответствие порядку осуществления категорирования, оценивается правильность присвоения категории. Максимальный срок категорирования объектов КИИ – 1 год со дня утверждения субъектом КИИ перечня объектов КИИ. Категория значимого объекта КИИ может быть изменена по мотивированному решению ФСТЭК России в рамках государственного контроля безопасности значимых объектов КИИ, в случае изменения самого объекта КИИ, а также в связи с реорганизацией субъекта КИИ (в том числе ликвидацией, изменением его организационно-правовой формы и т.д.).

**Приложение №2.1. Перечень проектов документов ФЗ-152\*.**

№	Наименование	Основание для создания документа
1	Акт обследования	Федеральный закон от 30.12.2020 N 519-ФЗ "О внесении изменений в Федеральный закон "О персональных данных"; ФЗ-№152 от 27 июля 2006 года «О персональных данных». ФЗ-№149 от 27 июня 2006 года «Об информации, информационных технологиях и о защите информации». Постановление Правительства РФ от 01 ноября 2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных». Постановление правительства РФ от 15 сентября 2008 года № 687 «Об утверждении положения об особенностях обработки персональных данных, осуществляемых без использования средств автоматизации». Постановление Правительства РФ от 21 марта 2012 № 211 «Об утверждении
2	Приказ Об организации работ по защите персональных данных	
3	Перечень сотрудников, допущенных в помещения, где ведётся обработка персональных данных	
4	Схема контролируемой зоны	
5	Приказ О назначении лиц, ответственных за обеспечение безопасности персональных данных	
6	Разрешительная система доступа сотрудников к ресурсам информационных систем персональных данных	
7	Акт определения уровня защищенности персональных данных при их обработке в информационной системе персональных данных	
8	Приказ Об утверждении внутренних нормативно-правовых актов по защите персональных данных	
9	Инструкция администратора информационных систем персональных данных по обеспечению безопасности персональных данных	
11	Инструкция о порядке резервирования и восстановления работоспособности технических средств, программного обеспечения и баз данных	
12	Инструкция ответственного за организацию обработки персональных данных	
13	Инструкция по организации антивирусной защиты	
14	Порядок учета, хранения и уничтожения материальных носителей персональных данных в информационной системе персональных данных	
15	Журнал учета машинных носителей персональных данных в ИСПДн	
16	Журнал учета съемных машинных носителей персональных данных в ИСПДн	
17	Журнал учета бумажных носителей персональных данных в ИСПДн	
18	Приказ о назначении комиссии по уничтожению материальных носителей информации	
19	Акт об уничтожении информации	
20	Инструкция пользователя информационных систем персональных данных по обеспечению безопасности персональных данных	
21	Положение об обработке персональных данных	
22	Перечень персональных данных	
23	Перечень должностей работников, допущенных к работе с персональными данными и замещение которых предусматривает осуществление обработки персональных данных либо осуществление доступа к персональным данным	
24	Обязательство о неразглашении персональных данных	
25	Образец Согласия на обработку персональных данных	
26	Перечень информационных систем персональных данных	
27	Порядок доступа сотрудников в помещения, где ведётся обработка персональных данных	
28	Правила работы с обезличенными персональными данными	
29	Регламент порядка действий сотрудников при обращении либо при получении запроса субъекта персональных данных или его законного представителя, а также уполномоченного органа по защите прав субъектов персональных данных	
30	Политика обработки персональных данных	
31	Инструкция администратора безопасности информационных систем персональных данных	
32	Инструкция пользователя по обеспечению безопасности обработки персональных данных при возникновении внештатных ситуаций	
33	Концепция информационной безопасности информационных систем	

	персональных данных	<p>перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственным и или муниципальными органами». Приказ федеральной службы по техническому и экспортному контролю России от 18 февраля 2013 года № 21 «Об утверждении Состав и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных». Специальные требования и рекомендации по технической защите конфиденциально й информации (СТР-К).</p>
34	Политика информационной безопасности информационных систем персональных данных	
35	Инструкция по организации парольной защиты информационных систем персональных данных	
36	Инструкция по организации защиты информации о событиях безопасности в информационных системах персональных данных	
37	Инструкция по установке, модификации и техническому обслуживанию программного обеспечения и аппаратных средств информационной системы персональных данных	
38	Инструкция по обеспечению защиты информации при выводе информационных систем персональных данных из эксплуатации или после принятия решения об окончании обработки информации	
39	Порядок уничтожения и блокирования персональных данных	
40	Положение об обработке персональных данных без использования средств автоматизации	
41	Лист ознакомления с положениями законодательства Российской Федерации о персональных данных, локальными актами по вопросам обработки персональных данных, требованиями к защите персональных данных	
42	Правила осуществления внутреннего контроля соответствия обработки персональных данных требованиям безопасности информации в информационной системе персональных данных	
43	Перечень мероприятий по контролю за обеспечением безопасности персональных данных в информационных системах персональных данных	
44	План мероприятий по контролю за обеспечением безопасности персональных данных в информационных системах персональных данных	
45	Журнал учета мероприятий по контролю за обеспечением защиты информации в ИСПДн	
46	Акт результатов проведения внутренней проверки обеспечения безопасности информации в ИСПДн	
47	Образец отзыва согласия на обработку персональных данных	
48	Форма разъяснения последствий отказа предоставить ПДн	
49	Журнал обращений субъектов персональных данных	
50	Журнал учета резервного копирования и восстановления данных	
51	Частная модель угроз безопасности персональных данных для информационных систем персональных данных	
52	Журнал учета проверок, проводимых органами государственного контроля (надзора), органами муниципального контроля	
53	Приказ О проведении мероприятий по оценке вреда, который может быть причинен субъектам персональных данных в случае нарушения требований федерального законодательства по защите персональных данных	
54	Акт оценки возможного вреда субъектам, чьи персональные данные обрабатываются в информационных системах	
55	Журнал приема (сдачи) под охрану помещений, хранилищ, сейфов	
56	Журнал учета сейфов (хранилищ) и ключей от них	
57	Журнал учета средств защиты информации	
58	Журнал учета пломбирования персональных компьютеров	
59	Приказ О проведении внутренней проверки соответствия обработки персональных данных требованиям к защите персональных данных	
60	Пояснительная записка по месту размещения баз информационных систем персональных данных	

\* точный перечень проектов организационно-распорядительных документов вытекает из необходимых организационных мероприятий, будет определен после обследования.



Приложение №2.2. Перечень проектов документов по КИИ Ф3-187.

	Наименование документа	Основание для создания документа
1	Акт категорирования объекта КИИ.	Федеральный закон №187-ФЗ от 26.07.2017 «О безопасности КИИ РФ», Федеральный закон №193-ФЗ от 26.07.2017 «О внесении изменений в отдельные законодательные акты РФ в связи с принятием ФЗ «О безопасности КИИ РФ», Федеральный закон №194-ФЗ от 26.07.2017 «О внесении изменений в УК РФ и УПК РФ в связи с принятием ФЗ «О безопасности КИИ РФ», Постановление Правительства РФ №127 от 08.02.2018 «Об утверждении Правил категорирования объектов КИИ РФ, а также перечня показателей критериев значимости объектов КИИ РФ и их значений», Постановление Правительства РФ №162 от 17.02.2018 «Об утверждении Правил осуществления госконтроля в области обеспечения безопасности значимых объектов КИИ РФ», Постановление Правительства РФ №808 от 11.07.2018 «О внесении изменения в Правила организации повышения квалификации специалистов по СИ и должностных лиц, ответственных за организацию СИ в ОГВ, ОМС, организациях с госучастием и организациях ОПК», Указ Президента РФ №569 от 25.11.2017 «О внесении изменений в Положение о ФСТЭК», Указ Президента Российской Федерации от 22.12.2017 г. № 620 «О совершенствовании государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации», Приказ ФСТЭК России №227 от 06.12.2017 «Об утверждении Порядка ведения реестра значимых объектов КИИ РФ», Приказ ФСТЭК России №229 от 11.12.2017 «Об утверждении формы акта проверки, составляемого по итогам проведения госконтроля в области обеспечения безопасности значимых объектов КИИ РФ», Приказ ФСТЭК России №235 от 21.12.2017 «Об утверждении Требований к созданию систем безопасности значимых объектов КИИ РФ и обеспечению их функционирования», Приказ ФСТЭК России №236 от 22.12.2017 «Об утверждении формы направления сведений о результатах присвоения объекту КИИ одной из категорий значимости либо об отсутствии необходимости присвоения ему одной из таких категорий», Приказ ФСТЭК России №239 от 25.12.2017 «Об утверждении Требований по обеспечению безопасности значимых объектов КИИ РФ», Приказ ФСТЭК России №72 от 26.04.2018 «О внесении изменений в Регламент ФСТЭК», Информационное сообщение ФСТЭК России №240/22/2339 от 04.05.2018 «О методических документах по вопросам обеспечения безопасности информации в КИИ РФ»
2	Инструкция Администратора безопасности объектов КИИ.	
3	Инструкция Администратора объектов КИИ.	
4	Инструкция О порядке резервирования и восстановления данных с машинных носителей объектов КИИ.	
5	Инструкция По обеспечению защиты информации при выводе оборудования объекта КИИ из эксплуатации.	
6	Инструкция По проведению внутренних проверок в области обеспечения безопасности значимых объектов КИИ.	
7	Инструкция по реагированию на компьютерные инциденты.	
8	Инструкция Пользователя объектов КИИ.	
9	Инструкция Пользователя при возникновении внештатных ситуаций при работе с объектами КИИ.	
10	Концепция информационной безопасности.	
11	Модель угроз безопасности объектов КИИ.	
12	Перечень объектов КИИ.	
13	Перечень СЗИ в объектах КИИ.	
14	План мероприятий по категорированию объектов КИИ	
15	План мероприятий по обеспечению защиты объектов КИИ.	
16	Политика информационной безопасности.	
17	Порядок взаимодействия подразделений.	
18	Порядок взаимодействия субъекта КИИ с ГосСОПКОЙ	
19	Порядок доступа в помещения с объектами КИИ.	
20	Порядок информирования и обучения работников.	
21	Порядок проведения испытаний или приемки средств защиты информации.	
22	Порядок уничтожения и блокирования данных с машинных носителей объектов КИИ.	
23	Приказ о вводе в эксплуатацию объектов КИИ.	
24	Приказ о допуске сотрудников к объектам КИИ.	
25	Приказ о категорировании объектов КИИ.	
26	Приказ о назначении ответственного за безопасность объектов КИИ.	
27	Приказ о подразделении по защите объектов КИИ.	
28	Приказ О проведении внутренней проверки безопасности объектов КИИ.	
29	Приказ О проверке готовности и возможности ввода в эксплуатацию СЗИ.	
30	Приказ Об утверждении документов по вопросам обеспечения безопасности информации в объектах КИИ.	
31	Приказ об утверждении перечня объектов КИИ.	
32	Разрешительная система доступа к объектам КИИ.	
33	Сведения о результатах присвоения категории значимости.	
34	Журнал поэкземплярного учёта СЗИ в объектах КИИ.	
35	Журнал учёта машинных носителей объектов КИИ.	

**Приложение №3.1. Предварительный расчет, получаемый результат Ф3-152.**

Наименование этапа	Ссылка на закон	Получаемый результат	Дни
I и II ЭТАПы - Обследование и разработка административной части проекта системы защиты персональных данных			
Обследование информационной системы персональных данных		Отчет об обследовании включая: состав и структуру ИСПДн.	10
Разработка регламентирующих документов по ИСПДн. Согласование вариантов инженерно-технических, программно-аппаратных средств по защите ПДн.	ФЗ-№152 от 27 июля 2006 года «О персональных данных». ФЗ-№149 от 27 июля 2006 года «Об информации, информационных технологиях и о защите информации». Постановление Правительства РФ от 01 ноября 2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных». Постановление правительства РФ от 15 сентября 2008 года № 687 «Об утверждении положения об особенностях обработки персональных данных, осуществляемых без использования средств автоматизации». Постановление Правительства РФ от 21 марта 2012 № 211 «Об утверждении перечня 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». Приказ федеральной службы по техническому и экспортному контролю России от 18 февраля 2013 года № 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных». Специальные требования и рекомендации по технической защите конфиденциальной информации (СТР-К). Методический документ. Методика оценки угроз безопасности информации" (утв. ФСТЭК России 05.02.2021)	Утвержденные в организации документы, регламентирующие деятельность сотрудников с ПДн.	20
		Утвержденные Акты классификации ИСПДн. Утвержденные Модели угроз безопасности ПДн со списком актуальных угроз.	
		Положения, регламенты, инструкции, перечни, другие дополнительные документы.	
III ЭТАП – Обеспечение мероприятий поддержания системы защиты ПДн в актуальном состоянии			
Сопровождение пользователей ИСПДн - обеспечение мероприятий поддержания системы защиты ПДн в актуальном состоянии	Обучение регламентам ответственного за организацию безопасной обработки персональных данных, консультации пользователей ИСПДн, ответы на вопросы пользователей ИСПДн, бесплатное участие в семинарах по безопасности.		



**Приложение № 3.2. Предварительный расчет, получаемый результат ФЗ-187.**

Наименование этапа	Ссылка на закон	Получаемый результат	Дни
<b>Обследование и разработка административной части проекта системы защиты объектов КИИ</b>			
Обследование - сбор данных о техническом и программном составе объектов критической информационной инфраструктуры (ИС, ИТС, АСУ).		Отчет об обследовании включая: состав и структуру КИИ.	3
Разработка регламентирующих документов по безопасности объектов КИИ. Консультации пользователей объектов КИИ, ответы на вопросы пользователей объектов КИИ.	<p>Федеральный закон №187-ФЗ от 26.07.2017 «О безопасности КИИ РФ», Федеральный закон №193-ФЗ от 26.07.2017 «О внесении изменений в отдельные законодательные акты РФ в связи с принятием ФЗ «О безопасности КИИ РФ»,</p> <p>Федеральный закон №194-ФЗ от 26.07.2017 «О внесении изменений в УК РФ и УПК РФ в связи с принятием ФЗ «О безопасности КИИ РФ»,</p> <p>Постановление Правительства РФ №127 от 08.02.2018 «Об утверждении Правил категорирования объектов КИИ РФ, а также перечня показателей критериев значимости объектов КИИ РФ и их значений»,</p> <p>Постановление Правительства РФ №162 от 17.02.2018 «Об утверждении Правил осуществления госконтроля в области обеспечения безопасности значимых объектов КИИ РФ»,</p> <p>Постановление Правительства РФ №808 от 11.07.2018 «О внесении изменения в Правила организации повышения квалификации специалистов по ЗИ и должностных лиц, ответственных за организацию ЗИ в ОГВ, ОМС, организациях с госучастием и организациях ОПК»,</p> <p>Указ Президента РФ №569 от 25.11.2017 «О внесении изменений в Положение о ФСТЭК»,</p> <p>Указ Президента Российской Федерации от 22.12.2017 г. № 620 «О совершенствовании государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации»,</p> <p>Приказ ФСТЭК России №227 от 06.12.2017 «Об утверждении Порядка ведения реестра значимых объектов КИИ РФ»,</p> <p>Приказ ФСТЭК России №229 от 11.12.2017 «Об утверждении формы акта проверки, составляемого по итогам проведения госконтроля в области обеспечения безопасности значимых объектов КИИ РФ»,</p> <p>Приказ ФСТЭК России №235 от 21.12.2017 «Об утверждении Требований к созданию систем безопасности значимых объектов КИИ РФ и обеспечению их функционирования»,</p> <p>Приказ ФСТЭК России №236 от 22.12.2017 «Об утверждении формы направления сведений о результатах присвоения объекту КИИ одной из категорий значимости либо об отсутствии необходимости присвоения ему одной из таких категорий»,</p> <p>Приказ ФСТЭК России №239 от 25.12.2017 «Об утверждении Требований по обеспечению безопасности значимых объектов КИИ РФ»,</p> <p>Приказ ФСТЭК России №72 от 26.04.2018 «О внесении изменений в Регламент ФСТЭК», Информационное сообщение ФСТЭК России №240/22/2339 от 04.05.2018 «О методических документах по вопросам обеспечения безопасности информации в КИИ РФ».</p>	<p>Утвержденные в организации документы, регламентирующие деятельность сотрудников со значимыми объектами КИИ</p>	24

**Приложение №4.1. Ответственность за нарушение ФЗ-152.**
**▪ Уголовная ответственность**

Статья	Нарушение	Максимальная мера наказания
137 УК РФ	Нарушение неприкосновенности частной жизни	<ul style="list-style-type: none"> <li>• Штраф 300 000 рублей</li> <li>• Лишение права занимать определенные должности или заниматься определенной деятельностью на срок от 2 до 5 лет</li> <li>• Арест на срок до 6 месяцев</li> <li>• Лишение свободы на срок до 4 лет с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до 5 лет</li> </ul>
140 УК РФ	Отказ в предоставлении гражданину информации о его персональных данных	<ul style="list-style-type: none"> <li>• Штраф 200 000 рублей</li> <li>• Лишение права занимать определенные должности или заниматься определенной деятельностью на срок от 2 до 5 лет</li> </ul>
272 УК РФ	Неправомерный доступ к охраняемой законом компьютерной информации	<ul style="list-style-type: none"> <li>• Штраф 200 000 рублей</li> <li>• Обязательные работы на срок 120 до 180 часов</li> <li>• Исправительные работы на срок до 1 года</li> <li>• Лишение свободы на срок до 2 лет</li> </ul>

**▪ Административная ответственность**

Статья	Нарушение	Максимальная мера наказания
5.27 КоАП РФ	Нарушение законодательства о труде и об охране труда	<ul style="list-style-type: none"> <li>• Штраф 50 000 руб. или приостановление деятельности на срок до 90 суток</li> </ul>
13.11 КоАП РФ	Нарушение порядка сбора, хранения, использования или распространения информации о гражданах (персональных данных, далее - ПДн)	<ul style="list-style-type: none"> <li>• Максимальный размер штрафа 75 000 руб (в соответствии с Федеральным законом от 07.02.2017 № 13-ФЗ). При этом, если раньше в КоАП существовал только один, общий для всех случаев состав правонарушения в области ПДн (ст.13.11 КоАП РФ), то теперь в данной статье появилось семь составов.</li> </ul>
13.12 КоАП РФ	Нарушение правил защиты информации	<ul style="list-style-type: none"> <li>• Штраф 20 000 руб. с конфискацией средств защиты информации</li> </ul>
19.5 КоАП РФ	Невыполнение в срок требований надзорного органа или ФСТЭК РФ (при повторной проверке)	<ul style="list-style-type: none"> <li>• Штраф 500 000 руб. и дисквалификация должностного лица до 3-х лет</li> </ul>
20.25 КоАП РФ	Неуплата административного штрафа	<ul style="list-style-type: none"> <li>• Штраф в двукратном размере суммы неуплаченного штрафа либо арест на срок до пятнадцати суток.</li> </ul>

**▪ Ответственность согласно Федерального закона № 152-ФЗ "О персональных данных"**

Статья	Нарушение	Максимальная мера наказания
23 ч.3 п.3 152-ФЗ	Обработка ПДн, полученных незаконным путем	<ul style="list-style-type: none"> <li>• Блокирование или уничтожение системы ПДн</li> </ul>
23 ч.3 п.6 152-ФЗ	Передача ПДн третьим лицам без согласия субъекта	<ul style="list-style-type: none"> <li>• Отзыв лицензии на осуществление определенного вида деятельности</li> </ul>

**• Ответственность согласно Трудового кодекса РФ**

Статья	Нарушение	Максимальная мера наказания
90 ТК РФ	Нарушение норм, регулирующих обработку и защиту ПДн работника	<ul style="list-style-type: none"> <li>• Штраф 300 000 рублей</li> <li>• Лишение права занимать определенные должности или заниматься определенной деятельностью на срок от 2 до 5 лет</li> <li>• Арест на срок до 6 месяцев</li> <li>• Лишение свободы на срок до 4 лет с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до 5 лет (ст. 137 УК РФ)</li> </ul>

Статья	Нарушение	Максимальная мера наказания
Уголовный Кодекс РФ, ст. 274.1.	Несоблюдение установленных правил эксплуатации технических средств объекта КИИ или нарушение порядка доступа к ним.	<ul style="list-style-type: none"> <li>• Лишение свободы на срок от 3 до 8 лет с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до трех лет или без такового</li> <li>• Лишение свободы на срок от 5 до 10 лет с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до пяти лет или без такового</li> <li>• Принудительные работы на срок до 5 лет с ограничением свободы на срок до 2 лет или без такового либо лишением свободы на срок от 2 до 5 лет со штрафом в размере от 500 000 до 1 000 000 рублей или в размере заработной платы или иного дохода осужденного за период от 1 года до 3 лет</li> <li>• Принудительные работы на срок до 5 лет со штрафом в размере от 500 000 до 1 000 000 рублей или в размере заработной платы или иного дохода осужденного за период от 1 года до 3 лет и с ограничением свободы на срок до 2 лет или без такового либо лишением свободы на срок от 2 до 6 лет со штрафом в размере от 500 000 до 1 000 000 рублей или в размере заработной платы или иного дохода осужденного за период от 1 года до 3 лет.</li> <li>• Принудительные работы на срок до 5 лет с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до 3 лет или без такового либо лишением свободы на срок до 6 лет с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до 3 лет или без такового</li> </ul>
Уголовный Кодекс РФ, ст. 293.	Наступление последствий (аварий и чрезвычайных ситуаций), повлекших за собой ущерб.	<ul style="list-style-type: none"> <li>• Штраф в размере до 120 000 рублей или в размере заработной платы или иного дохода осужденного за период до 1 года, либо обязательные работы на срок до 360 часов, либо исправительные работы на срок до 1 года, либо арест на срок до 3 месяцев</li> <li>• Штраф в размере от 200 000 до 500 000 рублей или в размере заработной платы или иного дохода осужденного за период от 1 года до 3 лет с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до 3 лет или без такового, либо обязательными работами на срок до 480 часов, либо исправительными работами на срок до 2 лет, либо арест на срок до 6 месяцев.</li> <li>• Принудительные работы на срок до 5 лет с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до 3 лет или без такового либо лишением свободы на срок до 5 лет с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до 3 лет или без такового.</li> <li>• Принудительные работы на срок до 5 лет с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до 3 лет или без такового либо лишением свободы на срок до 7 лет с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до 3 лет или без такового.</li> </ul>