Под прицелом регулятора.

Ответственность за

безответственность оператора.

Являюсь ли я оператором персональных данных?

Чтобы ответить на этот вопрос, необходимо понять:

Что такое персональные данные

Что такое обработка персональных данных

Кто такой оператор персональных данных

СПЕЦИАЛЬНЫЕ ВЫЧИСЛИТЕЛЬНЫЕ КОМПЛЕКСЫ

Научно-производственное предприятие

Персональные данные – любая информация, относящаяся к прямо или косвенно определенному или определяемому лицу (субъекту персональных данных).
Обработка персональных данных – любое действие или совокупность действий, совершаемых с использованием средств автоматизации или без использования таких средств с персональными данными, включая сбор, запись, систематизацию, накопление, хранение, уточнение, извлечение, использование, передачу, обезличивание, блокирование, удаление, уничтожение персональных данных.

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, совершаемые с персональными данными.
ч. 1 ст. 19 № 152-ФЗ Меры по обеспечению безопасности персональных данных при их обработке

Оператор при обработке персональных данных обязан принимать необходимые правовые, организационные и технические меры или обеспечивать их принятие для защиты персональных данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, предоставления, распространения персональных данных,
а также от иных неправомерных действий в отношении персональных данных.

Регуляторы в области защиты персональных данных:

Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзор) – уполномоченный орган по защите прав субъектов персональных данных.

Федеральная служба по техническому и экспортному контролю (ФСТЭК) – осуществляет контроль соблюдения установленных законодательством и ведомственными нормативно-правовыми актами в области технической защиты информационных систем персональных данных.

Федеральная служба безопасности (ФСБ) – осуществляет контроль соблюдения установленных законодательством и ведомственными нормативно-правовыми актами в области криптографических средств защиты информации.

Приоритетные направления и задачи Роскомнадзора:

2008 год – разработка и утверждение нормативно-правовых актов, регулирующих вопросы организации и проведения мероприятий по контролю (надзору) в отношении операторов, осуществляющих обработку персональных данных; активизация информационно – разъяснительной, профилактической работы.

2012 год – осуществление на постоянной основе мониторинга деятельности операторов, направленного на предупреждение, выявление и пресечение нарушений в области персональных данных.

Вывод: Период просвещения завершился, уже полным ходом идет эра контроля и надзора.

Плановые проверки Роскомнадзора:

- **проводятся на основании ежегодного плана проведения плановых проверок;**
- **проводятся как в отношении операторов, включенных в реестр операторов, так и в отношении операторов, не включенных в реестр, но осуществляющих обработку персональных данных;**
- **о проведении плановой проверки оператор уведомляется не позднее чем за три рабочих дня до начала ее проведения.**

СПЕЦИАЛЬНЫЕ ВЫЧИСЛИТЕЛЬНЫЕ КОМПЛЕКСЫ

Научно-производственное предприятие

В ходе плановой проверки проверяется:

- **назначение оператором ответственного за организацию обработки персональных данных;**
- **назначение оператором ответственного за обеспечение безопасности персональных данных;**
- **соответствие сведений, содержащихся в уведомлении об обработке персональных данных, фактически обрабатываемым оператором либо наличие законных оснований, подтверждающих отсутствие необходимости представления уведомления об обработке персональных данных;**
- **наличие изданных оператором организационно-распорядительных документов, определяющих политику оператора в отношении обработки персональных данных;**
- **наличие согласий субъектов на обработку персональных данных;**
- **договоры с третьими лицами, которым передаются персональные данные.**
- **Информационное оповещение о политике безопасности персональных данных на информационных ресурсах общего пользования (web ресурс), а также инструментарий обработки ПДн на общедоступных ресурсах.**
- **Наличие аттестатов соответствия ИСПДн требованиям безопасности информации , а также текущей деятельности учреждения по обеспечению безопасности обрабатываемых персональных данных.**

Основания для внеплановой проверки:

- **истечение срока исполнения оператором ранее выданного предписания об устранении выявленного нарушения установленных требований законодательства РФ в области персональных данных;**
- **поступление обращений и заявлений граждан, юридических лиц, индивидуальных предпринимателей, информации от органов государственной власти, органов местного самоуправления, из средств массовой информации, в том числе о следующих фактах: возникновение угрозы причинения вреда жизни, здоровью граждан, причинение вреда жизни, здоровью граждан;**
- **приказ руководителя, изданный в соответствии с поручениями Президента РФ, Правительства РФ;**
- **нарушение прав и законных интересов граждан действиями (бездействием) операторов при обработке их персональных данных;**
- **нарушение операторами требований законодательства РФ в области персональных данных, а также несоответствие сведений, содержащихся в уведомлении об обработке персональных данных, фактической деятельности.**

Нарушение	Наказание
Непредставление в Роскомнадзор уведомления об обработке персональных данных.	Ст. 19.7 КоАП РФ
Нарушение ч.4 ст. 20 № 152-ФЗ, в соответствии с которой оператор в течении 30-ти дней после получения запроса обязан сообщить в Роскомнадзор необходимую информацию об обработке персональных данных	Ст. 19.7 КоАП РФ
Нарушение установленного законом порядка сбора, хранения, использования и распространения информации о гражданах.	Ст. 13.11 КоАП РФ
Нарушение требований конфиденциальности персональных данных.	Ст. 13.11 КоАП РФ
Незаконное собирание и распространение сведений о частной жизни лица, составляющих его личную или семейную тайну, без его согласия.	Ст. 137 УК РФ

Так что же может грозить компании за **нарушение Федерального Закона №152-ФЗ «О персональных данных»**:
статья 24 Закона № 152-ФЗ: «Лица, виновные в нарушении требований настоящего Федерального закона, несут гражданскую, уголовную, административную, дисциплинарную и иную предусмотренную законодательством Российской Федерации ответственность».

УГОЛОВНАЯ ОТВЕТСТВЕННОСТЬ (Уголовный Кодекс РФ (УК РФ)

«…УК РФ. *Статья 137. Нарушение неприкосновенности частной жизни*
1. 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 средствах массовой информации - наказываются штрафом, либо обязательными работами на срок от ста двадцати до ста восьмидесяти часов, либо исправительными работами на срок до одного года, либо арестом на срок до четырех месяцев...»

«…УК РФ. *Статья 140. Отказ в предоставлении гражданину информации*
Неправомерный отказ должностного лица в предоставлении собранных в установленном порядке документов и материалов, непосредственно затрагивающих права и свободы гражданина, либо предоставление гражданину неполной или заведомо ложной информации, если эти деяния причинили вред правам и законным интересам граждан, - наказываются штрафом, либо лишением права занимать определенные должности или заниматься определенной деятельностью на срок от двух до пяти лет...»

«…УК РФ. *Статья 272. Неправомерный доступ к компьютерной информации*
1. Неправомерный доступ к охраняемой законом компьютерной информации, то есть информации на машинном носителе, в электронно-вычислительной машине (ЭВМ), системе ЭВМ или их сети, если это деяние повлекло уничтожение, блокирование, модификацию либо копирование информации, нарушение работы ЭВМ, системы ЭВМ или их сети, - наказывается штрафом, либо исправительными работами на срок от шести месяцев до одного года, либо **лишением свободы на срок до двух лет**…»
В настоящее время в связи с принятием Федерального закона № 152 «О персональных данных» планируется внести изменения в некоторые законодательные акты РФ, в том числе в Кодекс об Административных Правонарушениях РФ и Уголовный кодекс РФ, что повлечет существенное увеличение размера наказания за нарушения в сфере обработки персональных данных.

Административная ответственность (Кодекс об Административных Правонарушениях РФ (КоАП РФ)
«…КоАП РФ. Статья 13.11. Нарушение установленного законом «О персональных данных» порядка сбора, хранения, использования или распространения информации о гражданах (персональных данных)
влечет предупреждение или наложение административного штрафа на граждан в размере от трехсот до пятисот рублей; на должностных лиц - от пятисот до одной тысячи рублей; на юридических лиц - от пяти тысяч до десяти тысяч рублей.

«…КоАП РФ. *Статья 13.12. Нарушение правил защиты информации*
1. Нарушение условий, предусмотренных лицензией на осуществление деятельности в области защиты информации (за исключением информации, составляющей государственную тайну), -
влечет наложение административного штрафа на граждан в размере от трехсот до пятисот рублей; на должностных лиц - от пятисот до одной тысячи рублей; на юридических лиц - от пяти тысяч до десяти тысяч рублей.

2. Использование несертифицированных информационных систем, баз и банков данных, а также несертифицированных средств защиты информации, если они подлежат обязательной сертификации (за исключением средств защиты информации, составляющей государственную тайну), -влечет наложение административного штрафа на граждан в размере от пятисот до одной тысячи рублей с конфискацией несертифицированных средств защиты информации или без таковой; на должностных лиц - от одной тысячи до двух тысяч рублей; на юридических лиц - от десяти тысяч до двадцати тысяч рублей с конфискацией несертифицированных средств защиты информации или без таковой.

«…КоАП РФ. *Статья 13.14. Разглашение информации с ограниченным доступом*
Разглашение информации, доступ к которой ограничен федеральным законом «О персональных данных» (за исключением случаев, если разглашение такой информации влечет уголовную ответственность), лицом, получившим доступ к такой информации в связи с исполнением служебных или профессиональных обязанностей, за исключением случаев, предусмотренных частью 1 статьи 14.33 настоящего Кодекса, (ст.14.33-недобросовестная конкуренция) влечет наложение административного штрафа влечет наложение административного штрафа на
граждан в размере от пятисот до одной тысячи рублей; на должностных лиц - от четырех тысяч до пяти тысяч рублей...»

Дисциплинарная ответственность (Трудовой кодекс)
ТК *Статья 81* - Однократное грубое нарушение работником трудовых обязанностей - разглашение охраняемой законом тайны (государственной, коммерческой, служебной и иной), ставшей известной работнику в связи с исполнением им трудовых обязанностей, в том числе разглашение персональных данных другого работника - увольнение
ТК *Статья 90* - Нарушение норм, регулирующих получение, обработку и защиту персональных данных работника - увольнение

ВЫВОДЫ

По итогам проверки о соблюдении положений ФЗ -152 «О персональных данных» помимо наложения штрафов, может последовать уголовное преследование должностных лиц. Это конечно крайняя мера, но в России можно надолго оказаться в тюрьме и за ведро картошки.

Не стоит забывать и о возможности дисквалификации руководителя за несоблюдение требований закона, что повлечет невозможность занятия им соответствующих постов на длительное время.

Кроме того, штраф накладывается за зафиксированное нарушение. Но это не означает, что за это же нарушение нельзя оштрафовать снова. Это как будто Вы едите на автобусе без билета, и на каждой остановке заходит контролер и штрафует Вас за безбилетный проезд. Так и здесь, выдается предписание о немедленном устранении нарушений в течение 3 дней. И через этот срок проверка приходит снова и Вас снова штрафуют. Ведь за три дня нереально провести сертификацию своей информационной системы, и обеспечить выполнение всех **требований 152 федерального закона**.

Приведением бизнеса в соответствие с законом лучше озаботиться заранее, чтобы не нести дополнительных финансовых и моральных издержек.

Мероприятия по обеспечению безопасности ПДн при их обработке в МИС/ИСПДн включают в себя:

а) определение угроз безопасности ПДн при их обработке, формирование на их основе модели угроз;

б) разработку на основе модели угроз системы защиты персональных данных, обеспечивающей нейтрализацию предполагаемых угроз с использованием методов и способов защиты персональных данных, предусмотренных для соответствующего класса информационных систем;

в) проверку готовности средств защиты информации к использованию с составлением заключений о возможности их эксплуатации;

г) установку и ввод в эксплуатацию средств защиты информации в соответствии с эксплуатационной и технической документацией;

д) обучение лиц, использующих средства защиты информации, применяемые в информационных системах, правилам работы с ними;

е) учет применяемых средств защиты информации, эксплуатационной и технической документации к ним, носителей персональных данных;

ж) учет лиц, допущенных к работе с ПДн в информационной системе;

з) контроль за соблюдением условий использования средств защиты информации, предусмотренных эксплуатационной и технической документацией;

и) разбирательство и составление заключений по фактам несоблюдения условий хранения носителей персональных данных, использования средств защиты информации, которые могут привести к нарушению конфиденциальности персональных данных или другим нарушениям, приводящим к снижению уровня защищенности персональных данных, разработку и принятие мер по предотвращению возможных опасных последствий подобных нарушений;

к) описание системы защиты ПДн

Этапы приведения МИС/ИСПДн в соответствии с требованиями закона

Предпроектное обследование МИС/ИСПДн (Аудит)

Проектирование и реализация СЗ МИС/ИСПДн

Оценка соответствия МИС/ИСПДн

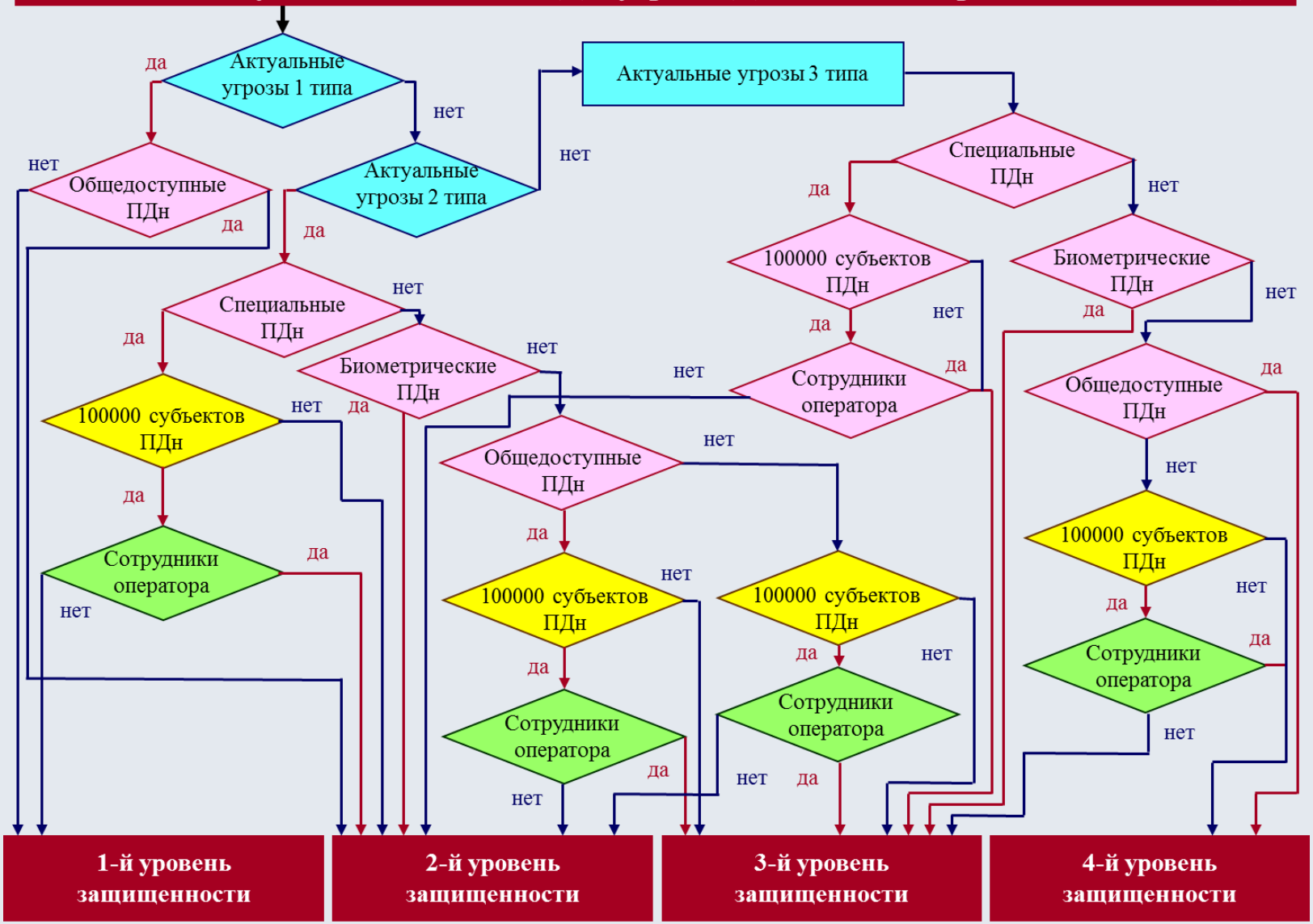
Порядок действий при организации защиты ПДн/ конфиденциальной информации в МИС/ИСПДн

1. Назначить лицо, ответственное за проведение мероприятий по организации защиты ПДн в Организации.
2. При недостатке ресурсов для приведения МИС/ИСПДн к требованиям законодательства собственными силами -- найти специализированную компанию (имеющую лицензии ФСТЭК, ФСБ России)
3. Провести обследование ИС с целью оценки текущего состояния ИБ и сбора необходимых исходных данных для создания СЗПДн (определение кол-ва защищаемых объектов, их назначение, технические характеристики, схема взаимодействия между собой).
4. Урегулировать правовые вопросы обработки ПДн (согласие с субъектов, обязательство о неразглашении, уведомление в Роскомнадзор)
5. Определить угрозы безопасности ПДн в каждой МИС/ИСПДн.
6. Определить перечень обрабатываемых ПДн и провести классификацию МИС/ИСПДн.
7. Определить требования к системе защиты ПДн на основании модели угроз и класса МИС/ИСПДн (написание Технического задания на создание СЗПДн).
8. Спроектировать систему защиты персональных данных (СЗПДн): подобрать необходимые средства защиты информации (СЗИ).
9. Разработать организационно-распорядительную и регламентную документацию по обеспечению безопасности ПДн в МИС/ИСПДн.
10. Закупить, настроить, внедрить СЗИ в соответствии с разработанной документацией.
11. Провести обучение ответственных лиц и сотрудников правилам работы с СЗИ.
12. Распределить ответственность между сотрудниками Организации допущенными к работе с ПДн: назначить пользователей, администраторов безопасности, ответственных за эксплуатацию МИС/ИСПДн, а также ответственного за обработку ПДн в Организации – для каждой группы допущенных к ПДн разработать Инструкции.
13. Провести оценку соответствия МИС/ИСПДн требованиям по безопасности информации (с привлечением специализированной организации – лицензиата ФСТЭК России).
14. На основании положительных результатов оценки соответствия ввести МИС/ИСПДн в опытную эксплуатацию.
15. Организовать контроль соблюдения использования СЗИ и обеспечить управление обеспечением безопасности ПДн в динамике изменения обстановки и контроля эффективности защиты, включая учет применяемых СЗИ и носителей ПДн, а также учет лиц, допущенных к работе с ПДн.

СПЕЦИАЛЬНЫЕ ВЫЧИСЛИТЕЛЬНЫЕ КОМПЛЕКСЫ

Научно-производственное предприятие

Анализ совокупности типов ИСПДн, угроз ПДн и объема обрабатываемых ПДн



Класс защищенности информационной системы определяется в соответствии с приказом ФСТЭК России № 17 от 11.02.2013:

Уровень значимости информации	Масштаб информационной системы		
	Федеральный	Региональный	Объектовый
УЗ 1	К1	К1	К1
УЗ 2	К1	К2	К2
УЗ 3	К2	К3	К3
УЗ 4	К3	К3	К4

Политика информационной безопасности как основа системы защиты персональных данных учреждений. Рекомендации по построению политики информационной безопасности.

Документы, регламентирующие политику безопасности информации в организации:

1.Приказ (распоряжение) об организации работ по обеспечению безопасности ПДн при их обработке в Учреждении:
2. Перечень лиц, имеющих доступ к ИСПДн:
3. Инструкция по режимным мерам и допуску.
4. Акт определения уровня защищенности персональных данных, обрабатываемых в МИС/класса защищенности государственной информационной системы
5. Инструкция пользователя в части обеспечения безопасности информации.
6. Разрешительная система доступа пользователей к информационным ресурсам МИС/ИСПДн.
7. Политика в отношении обработки персональных данных (на сайт).
8. Технический паспорт на МИС/ИСПДн.
9. Приказ об установлении границ контролируемой зоны.
10. Инструкция администратора информационной безопасности.
11. Инструкция по организации парольной защиты в МИС|ИСПДн.
12. Инструкция по проведению антивирусного контроля.
13. Инструкция по резервному копированию и восстановлению данных.
14. Инструкция по работе с инцидентами информационной безопасности.
15. Частная модель угроз безопасности информации.
16. Приказ об организации криптографической защиты информации.

Документ, определяющий политику информационной безопасности для сайта (или ознакомления другим способом)

ч.2 ст.18.1 № 152-ФЗ

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.

Документ, определяющий политику информационной безопасности для сайта (или ознакомления другим способом)

СОДЕРЖАНИЕ

1. Правовые основания, цели и способы обработки персональных данных.
2. Наименование и место нахождения оператора, сведения о лицах, которые имеют доступ к персональным данным. Система допуска и круг лиц, допущенных к обработке персональных данных.
3. Обрабатываемые персональные данные, относящиеся к соответствующему субъекту персональных данных.
4. Сроки и правила хранения персональных данных.
5. Меры по обеспечению безопасности персональных данных при их обработке.
6. Порядок осуществления субъектом персональных данных прав. Порядок реагирования на запросы субъектов ПДн. Лица, ответственные за организацию обработки персональных данных.

Перечень ПДн, обрабатываемых в ИСПДн.

ИСПДн	Категория субъекта ПДн	Набор ПДн	Основания для обработки ПДн	Срок хранения, условия прекращения обработки
Зарплата и Кадры	Сотрудники	ФИО; Дата рождения; ИНН; СНИЛС; Образование; Доходы.	ст.85-90 Трудового кодекса Российской Федерации	До достижения заявленных целей обработки
Клиенты	Контрагенты	ФИО; Паспортные данные.	В целях исполнения договора (с.6 № 152-ФЗ)	

Перечень лиц, имеющих доступ к ИСПДн

ПП РФ № 1119 п. 13в) (для обеспечения всех УЗ):

- *утверждение руководителем оператора документа, определяющего перечень лиц, доступ которых к ПДн, обрабатываемых в информационной системе, необходим для выполнения ими служебных (трудовых) обязанностей.*

Наименование ИСПДн	ФИО	Должность
Зарплата и Кадры	Иванова Людмила Степановна	Начальник отдела кадров
	Щеглова Валентина Федоровна	Бухгалтер
Клиенты	Сидоров Александр Сергеевич	Менеджер
…		

СПЕЦИАЛЬНЫЕ ВЫЧИСЛИТЕЛЬНЫЕ КОМПЛЕКСЫ

Научно-производственное предприятие

ООО «НПП «СВК»» осуществляет весь спектр работ по защите информации:

- Аудит организаций и информационных систем
- Разработка локальных документов для выполнения требований ФЗ №152, Приказов ФСТЭК России и ФСБ России
- Разработка технических проектов систем защиты информации
- Моделирование угроз безопасности
- Настройка и внедрение средств защиты информации
- Аттестация информационных систем с конфиденциальной информацией
- Аутсорсинг и полное сопровождение подсистем безопасности информации организаций

Наши контакты:

Дорохин Александр Николаевич –Директор Югорского филиала ООО «НПП «СВК»

Щетинина Юлия Александровна – заместитель директора по коммерции и развитию бизнеса Югорского филиала ООО «НПП «СВК»

Белов Алексей Николаевич – заместитель директора по технической защите информации Югорского филиала ООО «НПП «СВК»

Тел.: 8 (3467) 318274, 318291
Email: JSch@h-lan.ru , ban@h-lan.ru