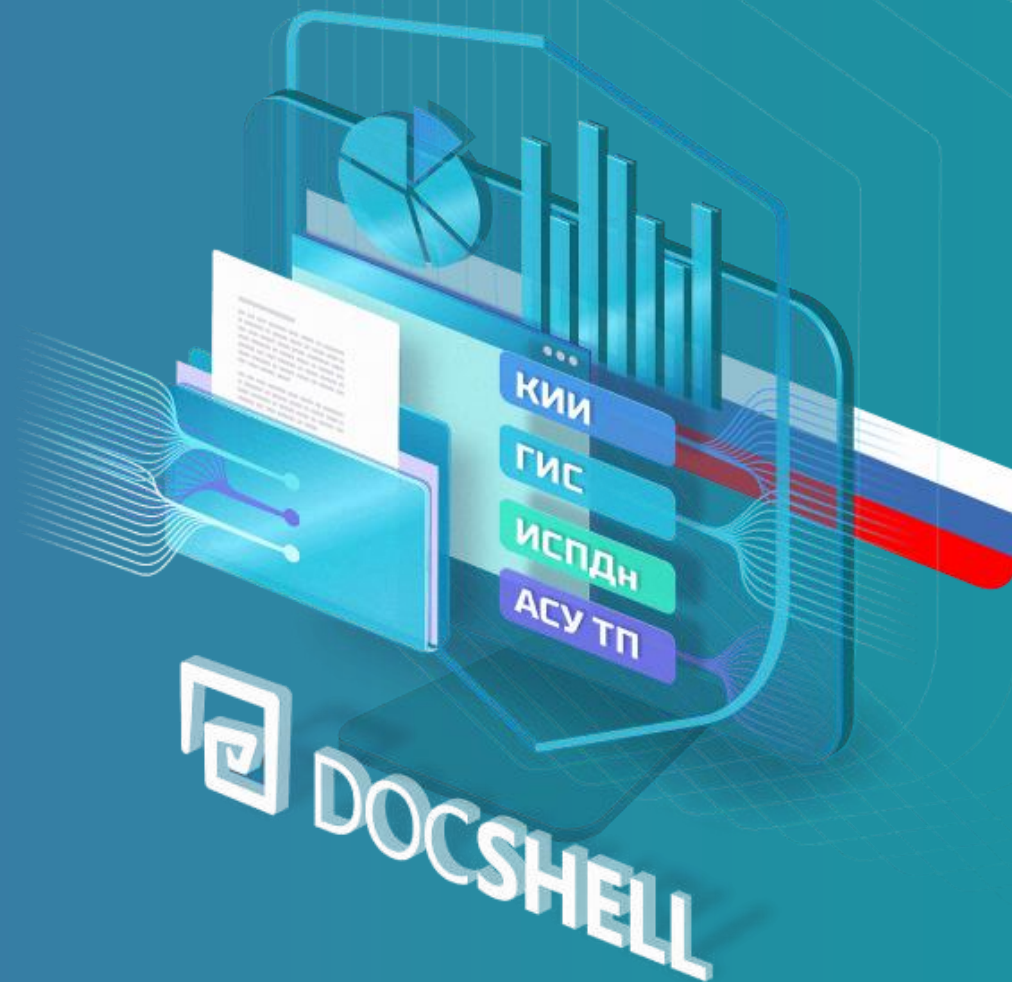


DOC SHELL 4.0 — система комплексного управления информационной безопасностью

Импортонезависимое решение, упрощающее обеспечение реализуемого комплекса мер по информационной безопасности с целью соблюдать требования, установленные федеральным законодательством (152-ФЗ, 187-ФЗ, 149-ФЗ) и иными нормативными актами



ФСБ РОССИИ



РОСКОМНАДЗОР



ФСТЭК РОССИИ



При возникновении вопросов, связанных с обработкой ПДн, эксплуатацией СКЗИ, КИИ, **необходимо тратить много времени** на поиск достоверной информации о решении либо обращаться за платными консультациями к экспертам

При изменениях в законодательстве важно понимать, что делать регулятору, какие изменения необходимы, какие шаги требуется выполнить

Большинство не соблюдения требований, приводящих к нарушениям законодательства, происходят из-за **низкой осведомленности сотрудников**

В ходе приведения рабочих мест сотрудников к соответствию требованиям законодательства необходимо собрать **большой объем различных данных**, которые разбросаны по многочисленным документам

В связи с **постоянными изменениями** разработанные пакеты документов теряют актуальность в процессе осуществления деятельности, а отслеживание документации, которую затронули изменения, требует большого количества времени и действий

Реагирование на утечки персональных данных и информирование Роскомнадзора об утечках ПДн

Отсутствие механизмов для отработки ИБ-инцидентов

Не готовы к экстренным ситуациям и ИБ-инцидентам, требующим реакции в сжатые сроки

Стресс при подготовке к **плановым проверкам** и авральным режим при внеплановых проверках

Причина возникновения

- **Отсутствие методологии** и процессного подхода в организации комплекса мер по информационной безопасности (ИБ)
- **Нехватка компетентных специалистов** на местах, чтобы нормализовать ситуацию и поддерживать в актуальном состоянии
- **Отсутствие инструментов** автоматизации на местах и обучения работе в данных инструментах
- **Смена ответственных** порождает утрату большей части наработанных данных



С чего начать?

01

Аудит процессов, документации и информационных систем

При возникновении вопросов, связанных с обработкой ПДн, эксплуатацией СКЗИ, КИИ, необходимо тратить много времени на поиск достоверной информации о решении либо обращаться за платными консультациями к экспертам.

02

Создание образа объекта

Оцениваем правовую основу договоров, на которых персональные данные передаются контрагентам, и выявляем возможные риски.

03

Подготовка пакета документов и рекомендаций

Готовим комплект документов по персональным данным и уведомление в Роскомнадзор. Выявляем факт соответствия или несоответствия бизнес-процессов федеральному закону №152-ФЗ "О персональных данных" и даем рекомендации, какие исправления необходимы.

04

Технические мероприятия по созданию системы защиты персональных данных

Проектирование и внедрение недостающих средств защиты информации, их интеграция в существующую инфраструктуру компании.

05

Консультации экспертов по №152-ФЗ

Поддержка по вопросам сбора, хранения и обработки персональных данных в организации по телефону и у вас в офисе, обновление документов в случае внутренних изменений в организации, а также в случае изменения законодательства, позиции Роскомнадзора и т.п.

06

Помощь в прохождении проверок

Проведение комплексного аудита процессов обработки персональных данных, документов и информационных систем персональных данных позволяет нам точно определить масштаб обработки персональных данных в организации не упустить ни одного риска для клиента.

С чего начать? (для КИИ)

Определить принадлежность организации к субъектам КИИ

Необходимо определить является ли Организация субъектом КИИ (т.е. узнать, попадают ли виды деятельности, прописанные в уставных документах организации, относятся к 14 отраслям КИИ)

Категорировать объектов КИИ

- Необходимо создать комиссию по категорированию объектов КИИ
- Определить перечень процессов и выявить критические процессы
- Разработать перечень объектов КИИ, подлежащих категорированию
- Определить угрозы безопасности для объектов КИИ
- Определить категории значимости для объектов КИИ
- Подготовить сведения о категорировании объектов КИИ (ЗОКИИ) и направить их регулятору (ФСТЭК РФ)

Разработать мероприятий по взаимодействию с ФСБ России

- Разработать регламент информирования ФСБ России
- Организовать взаимодействия с ФСБ России (НКЦКИ)



Обеспечить безопасность ЗОКИИ в ходе эксплуатации

- Планировать мероприятия по обеспечению безопасности ЗОКИИ
- Анализировать угрозы, администрировать систему безопасности
- Реагировать на инциденты и информировать персонал ЗОКИИ

Создать систему безопасности значимых объектов КИИ

- Установить требования к обеспечению безопасности значимых объектов КИИ (Тех. задание на систему безопасности ЗОКИИ (СБЗОКИИ))
- Разработать организационные и технические меры по обеспечению безопасности ЗОКИИ
 - Разработать модели угроз безопасности информации для ЗОКИИ
 - Выполнить проектирование СБЗОКИИ
 - Разработать рабочую (эксплуатационную) документацию на СБЗОКИИ
- Внедрить организационные и технические меры по обеспечению безопасности ЗОКИИ и ввод СБЗОКИИ в действие (установка СЗИ, анализ уязвимостей и приемочные испытания СБЗОКИИ)



Самостоятельно

изучать большой объем законодательных и нормативно-правовых актов, формировать шаблоны документов, отправлять в подведомственные организации, консолидировать, постоянно следить за изменениями законодательства, актуализировать шаблоны после каждого изменения.



Заклучить договор с компанией-аутсорсером

на проведение работ, согласовывать бюджет, прибегать к услугам компании-аутсорсера на постоянной основе для актуализации документации в соответствии с изменениями как в самой организации, так и при изменении законодательства.



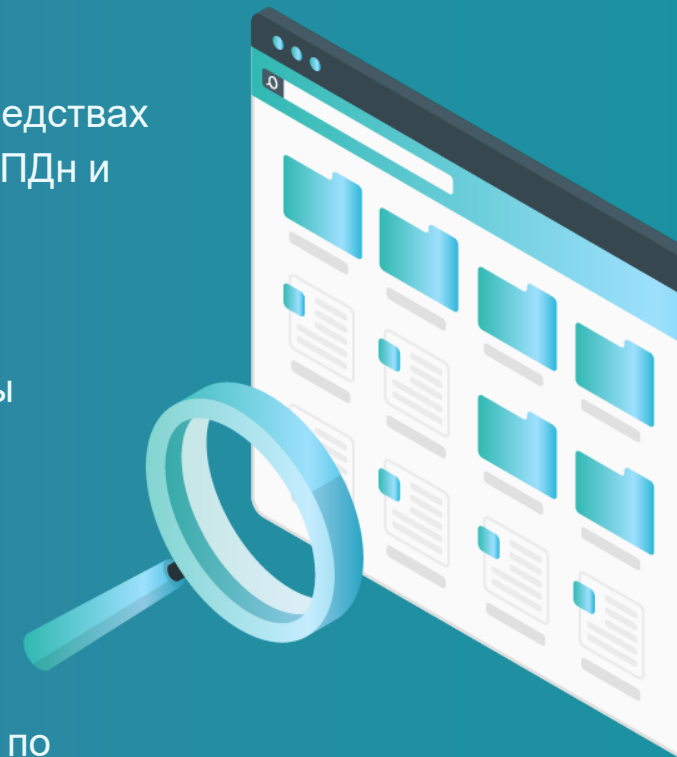
Воспользоваться сервисом DOCHELL 4.0

DOCHELL 4.0 – это простой и удобный способ управлять информационной безопасностью, организовать защиту критической инфраструктуры предприятия, а также обеспечить выполнение требований в области информационной безопасности, установленных федеральным законодательством (152-ФЗ, 187-ФЗ, 149-ФЗ) и иными нормативно-правовыми актами.

Обследование и внесение корректных данных в сервис

Полное обследование всей инфраструктуры для обеспечения сохранности данных и предотвращения их утечки, выполнения требований действующего законодательства, а также регуляторов в сфере обеспечения безопасности ПДн.:

- выявление всех процессов обработки ПДн, как в автоматизированном, так и в неавтоматизированном виде;
- выявление и определение всех информационных систем, в том числе ИСПДн и ГИС, в которых ведется обработка ПДн, с последующей классификацией и определением мер защиты;
- определение нюансов обработки ПДн в неавтоматизированном виде, происходящей без применения средств вычислительной техники;
- выявление нарушений требований законодательства;
- сбор сведений о технических средствах (ТС), участвующих в обработке ПДн и сетевой архитектуре;
- сбор сведений об имеющихся и применяемых средствах защиты информации.
- внесение всех необходимых данных в сервис DocShell 4.0.
- предоставление рекомендаций по устранению выявленных в процессе обследования нарушений и недочетов.



Результат:



Разработка актуального комплекта организационно-распорядительной документации, регламентирующего обработку ПДн, в т.ч. Модели угроз, Модели нарушителя и всё необходимое для отчетности перед Роскомнадзором.



Разработка отчета по результатам обследования, включающего в себя рекомендации и исходные данные для дальнейшего создания, разработки, проектирования и внедрение системы защиты объектов, участвующих в обработке ПДн.

В качестве выгоды вы получаете:

- ✓ знания о всех процессах обработки ПДн в организации, несоответствиях при обработке, оценку степени выполнения мер, рекомендации по приведению в соответствие.
- ✓ комплект ОРД, который необходим для выполнения требований по защите (комплаенс требования). Одно из требований - проводить периодический контроль выполнения мер!
- ✓ рекомендации по корректировке своих бизнес-процессов для более удобной организации ИБ.

Возможности DocShell

DOC SHELL
8 800 200-79-32

Автоматическая разработка и Сопровождение документов

организационно-распорядительной документации, автоматическая корректировка при смене ответственных лиц, автоматическое отслеживании актуальности документов



Инвентаризация

информационных активов и ИТ-инфраструктуры, автоматическая инвентаризация имеющихся цифровых активов, отслеживание сроков лицензий и работоспособности систем




DOC SHELL



Управление инцидентами информационной безопасности

в целях оперативного реагирования на свершившиеся инциденты, нейтрализации последствий, а также последующего анализа и предотвращения угроз

Управление мероприятиями

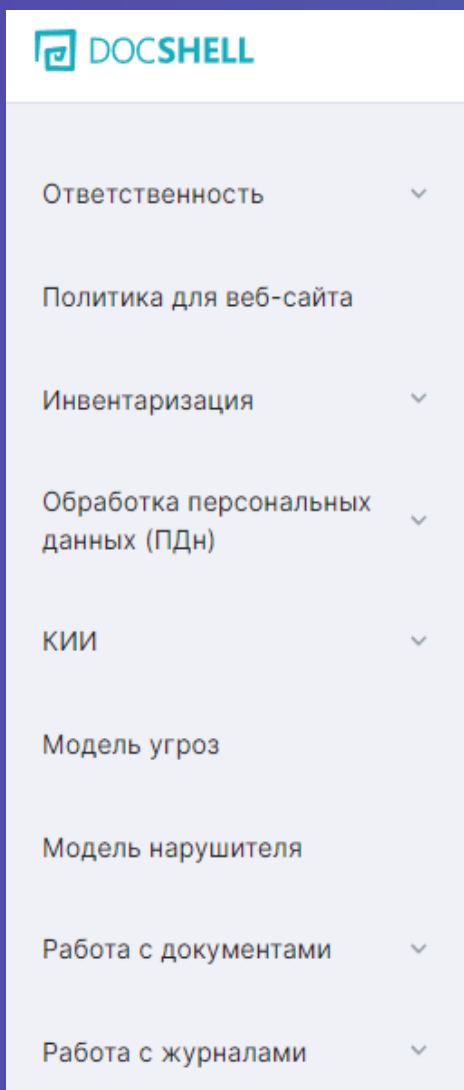
комплексное и согласованное управление мероприятиями информационной безопасности в центральном органе, во всех подразделениях и подведомственных учреждениях



Повышение осведомленности и контроль знаний сотрудников

Функции управления компетенциями помогут планировать и проводить инструктажи, обучение и тестирование знаний сотрудников

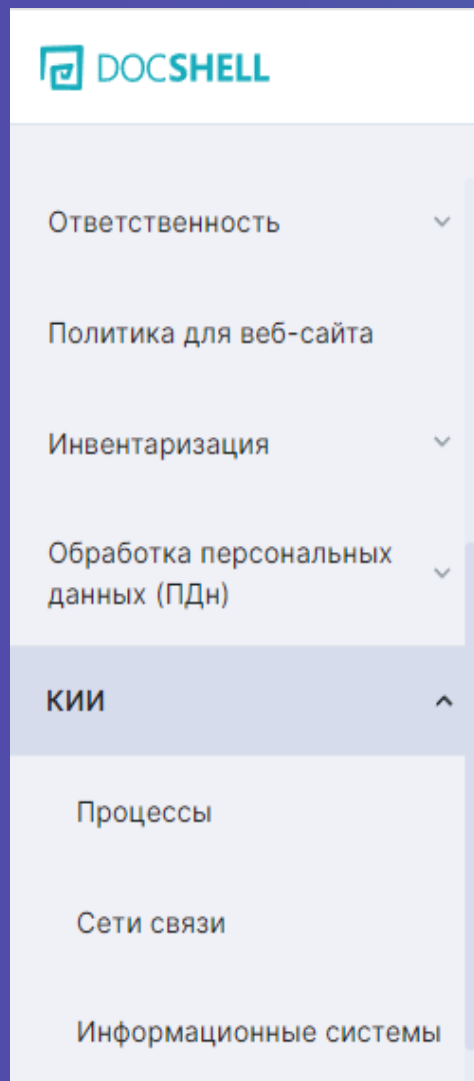
Оператору персональных данных



Фрагмент интерфейса программы

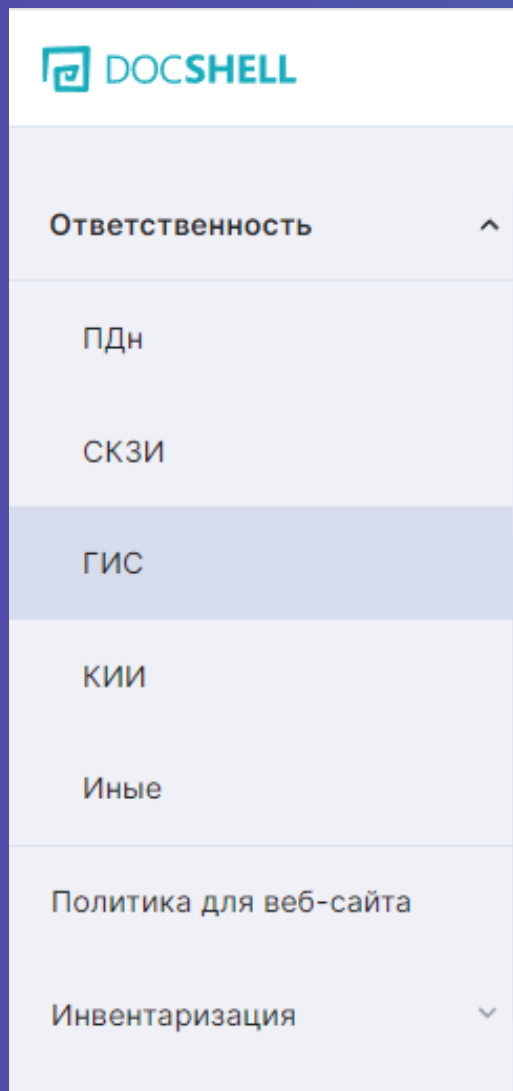
- ✓ **Помогает** определить процессы обработки ПДн, цели обработки ПДн, правовые основания случаев, когда возможна обработка данных – без согласия субъекта ПДн
- ✓ **Автоматизирует** процесс определения и утверждения сотрудников организации, допущенных к обработке ПДн в ИС, а также ответственных за хранение ПДн
- ✓ **Помогает классифицировать ИСПДн** и обеспечивать их безопасность в соответствии со значимостью системы в инфраструктуре предприятия
- ✓ **Помогает принимать** необходимые организационные и технические меры для защиты персональных данных от неправомерных действий
- ✓ **Помогает определять** контрагентов, которым оператор поручает обработку ПДн, перечень разрешенных им действий с ПДн и требования к защите ПДн
- ✓ **Регламентирует** предоставление субъектам ПДн сведений об обработке их персональных данных, в том числе готовит для публикации политику обработки ПДн
- ✓ **Автоматизирует** подготовку уведомления в уполномоченный орган по защите прав субъектов ПДн (Роскомнадзор) об изменении основных характеристик обработки ПДн

Владельцу объектов КИИ



- ✓ **Позволяет категорировать** объекты КИИ, которыми они владеют
- ✓ **Помогает незамедлительно** информировать о компьютерных инцидентах НКЦКИ ФСБ России (ГосСОПКА)
- ✓ **Регламентирует и планирует** обеспечение безопасности ОКИИ в соответствии с требованиями установленными ФСТЭК России и ФСБ России
- ✓ **Помогает установить** ответственность за мероприятия по обеспечению безопасности объектов КИИ
- ✓ **Автоматизирует** процесс определения уязвимостей, потенциальных нарушителей и актуальных угроз безопасности
- ✓ **Позволяет систематизировать** процесс управления информационной безопасностью ОКИИ

Владельцу ГИС



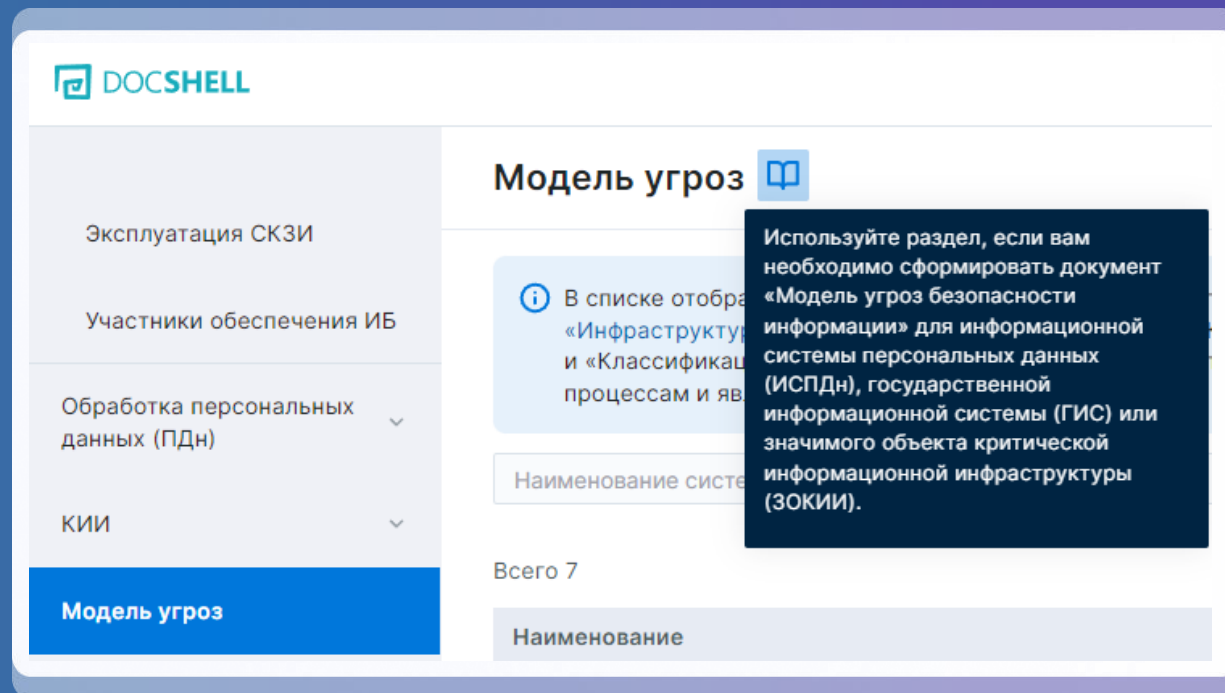
- ✓ **Помогает выполнить** все требования законодательства при создании и классификации информационных систем
- ✓ **Доводит до пользователей ГИС** требования по защите информации, которые необходимо выполнить до момента их подключения к системе
- ✓ **Позволяет пользователям** подготовить документы, принять организационные меры
- ✓ **Поможет организовать** контроль выполнения пользователями ГИС требований по защите информации, в том числе отобразит свидетельства (приказы, отчеты, акты, аттестаты и иную информацию)
- ✓ **Поможет владельцу обеспечить** проведение классификации ГИС, моделирование угроз, принятие организационных мер

■ Модель угроз

Модель угроз определяет угрозы безопасности информации (УБИ), которые могут возникнуть в:

- информационных системах,
- автоматизированных системах управления,
- информационно-телекоммуникационных сетях,
- информационно-телекоммуникационных инфраструктурах центров обработки данных
- облачных инфраструктурах.

Модель угроз безопасности информации содержит описание системы и её структурно-функциональных характеристик, а также описание УБИ, включающее описание возможностей нарушителей, возможных уязвимостей системы, способов реализации УБИ и последствий от нарушения свойств безопасности информации.



При разработке и корректировке моделей угроз обеспечиваются:

- описание методик определения актуальности угроз безопасности
- описание возможностей нарушителя
- описание уровня и класса защищённости информационной системы, категорирование ЗОКИИ
- учёт угроз, представленных в Банке данных угроз ФСТЭК России

Модель нарушителя безопасности информации содержит:

- общее описание информационной системы и её структурно-функциональных характеристик
- описание защитных мер
- свойств и возможностей нарушителей
- определение обобщенной возможности и требуемого класса защиты средства криптографической защиты информации

DocShell 4.0 поможет сформировать «Модель нарушителя»

DOC SHELL

Модель нарушителя

Используйте раздел, если вам необходимо сформировать документ «Модель нарушителя безопасности информации» для информационной системы персональных данных (ИСПДн) или государственной информационной системы (ГИС) с обработкой персональных данных

В списке отображаются системы «Инфраструктура ИТ», «Классификация ГИС» и «Обработка персональных данных»

Наименование системы (сети)

Всего 6

Наименование
Пользовательский сегмент ГИС EMCЭД Дело

Эксплуатация СКЗИ

Участники обеспечения ИБ

Обработка персональных данных (ПДн)

КИИ

Модель угроз

Модель нарушителя

Важно помнить: в случае с ГИС, Модель нарушителя необходимо отправить на согласование регулятору (ФСБ России)



SaaS (облачная версия)

- Система находится на облачном сервере.
- Мы берем все работы по установке, актуализации и технической поддержке системы на себя.

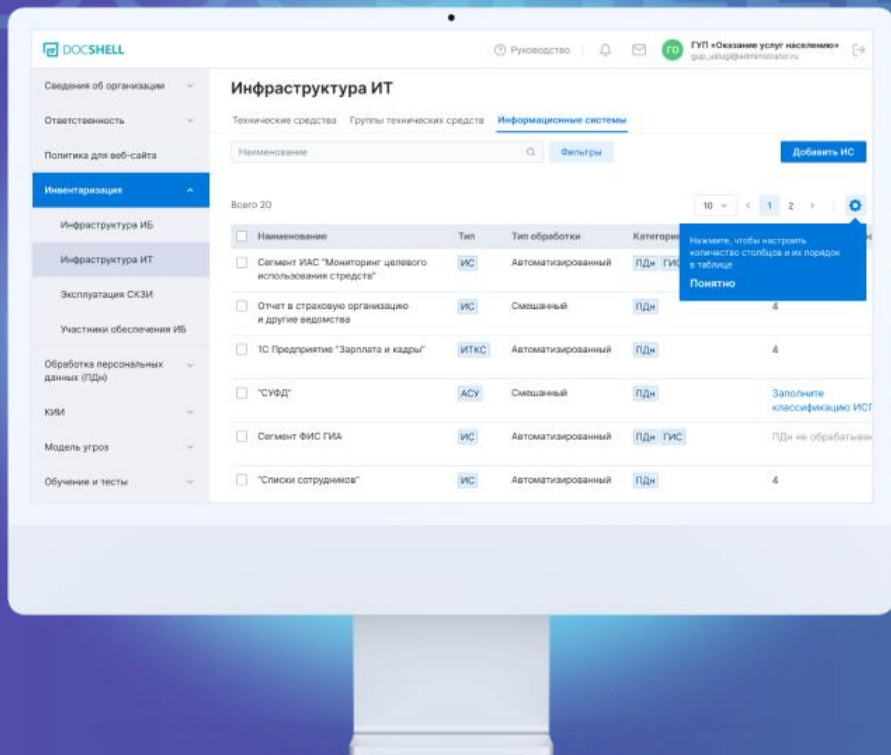
Варианты лицензирования (размещения)



On-Premise (серверная версия)

- Установка системы на сервере клиента.
- Обслуживание клиента в рамках технической поддержки.

Какой результат получаете при использовании



СТОРОННЯЯ ЭКСПЕРТИЗА

Вам и Вашим ответственным сотрудникам не надо тратить большое количество времени на поиск и чтение рекомендаций регуляторов, Федеральных законов и нормативно-правовых актов. Наши эксперты разработали шаблоны документов, которые учитывают все нюансы, Вам остается только внести свои данные и выгрузить готовые документы.



ЭКОНОМИЯ ВРЕМЕНИ

Автоматизируем формирование документов, шаблоны актуализируются при обновлении. DocShell 4.0 сокращает время на подготовку и периодическую актуализацию документов втрое. А умная система подсказок поможет успешно работать в сервисе на любом этапе.



ЭКОНОМИЯ СРЕДСТВ

Кратное снижение рисков штрафных санкций и невыполнения требований законодательства. Экономия до 70% на ИБ-обеспечение и потребности в высокооплачиваемых специалистах.



ГАРАНТИЯ СПОКОЙСТВИЯ

Полный контроль ситуации по ИБ, в том числе и в подведомственных организациях. Повышение эффективности мер по ИБ-обеспечению за счет автоматизации контура управления.

■ Контактная информация

DOCHELL

ООО «АйТи Новация»

 8 800 511 47 85

 office@docshell.ru