КСБ-СОФТ альфа

КИИ и ПДн: автоматизация соответствия требованиям ИБ

Спикеры:

- **Шляпкин Максим –** руководитель отдела защиты объектов КИИ и АСУ ТП, КСБ-СОФТ
- **Скопинцева Вера –** руководитель службы экспертной поддержки экосистемы приложений «Альфа», НПЦ КСБ

Модератор:

- **Чирков Дмитрий –** руководитель регионального направления, КСБ-СОФТ

Обменивайтесь
сообщениями
во вкладке «Чат»

Запись вебинара
направим Всем
участникам на указанный
при регистрации e-mail

Задавайте вопросы
во вкладке «Вопросы»

План вебинара

- необходимость сочетания организационных мер и практической безопасности
- какие документы по ИБ необходимо разработать и как их поддерживать в актуальном состоянии
- взаимодействие с регуляторами по ИБ
- последние изменения требований НПА по ИБ КИИ и ПДн и ответственность за их несоблюдение
- демонстрация средства автоматизации для разработки организационной и технической документации по защите ПДн, объектов КИИ
- Ответы на дополнительные вопросы

Наградим авторов 3 лучших вопросов фирменным мерчем!

«КСБ-СОФТ»

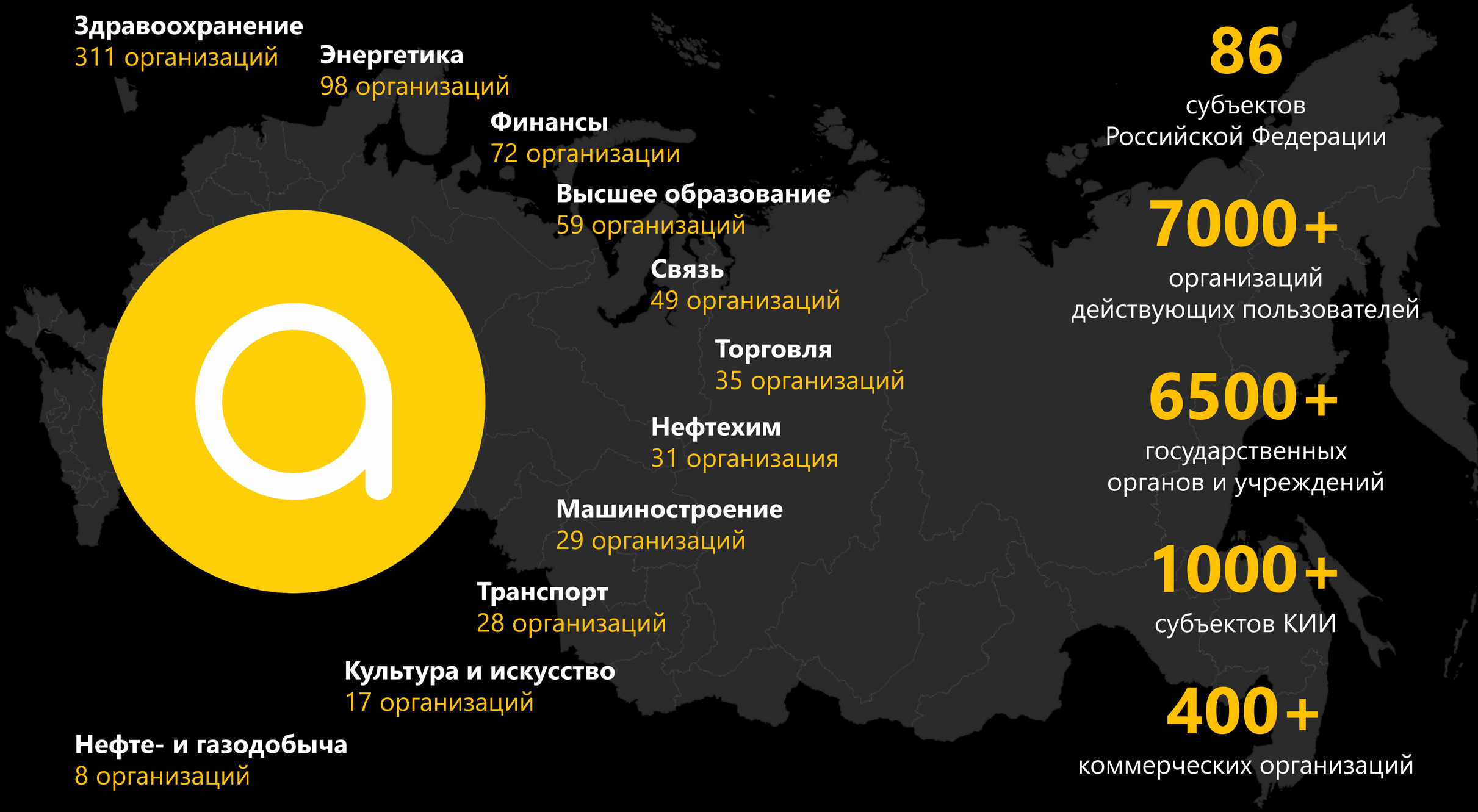
- Лицензиат ФСТЭК России
- Лицензиат ФСБ России

Системный интегратор в сфере информационной безопасности и импортозамещения информационных технологий

80+
регионов внедрения

4000+
реализованных проектов

Портфолио КСБ-СОФТ


Здравоохранение
311 организаций
Энергетика
98 организаций
Финансы
72 организации
Высшее образование
59 организаций
Связь
49 организаций
Торговля
35 организаций
Нефтехим
31 организация
Машиностроение
29 организаций
Транспорт
28 организаций
Культура и искусство
17 организаций
Нефте- и газодобыча
8 организаций
86
субъектов
Российской Федерации
7000+
организаций
действующих пользователей
6500+
государственных
органов и учреждений
1000+
субъектов КИИ
400+
коммерческих организаций

Способы защиты информации

Организационно-правовые

- Документация по установлению требований
- Организационно-распорядительная документация
- Проектная документация
- Рабочая, эксплуатационная документация

Инженерно-технические

- Аппаратные СЗИ
- Программные СЗИ
- СКЗИ
- Физические меры

Организационные меры. Разработка документации

Документация по установлению требований

- категорирование объектов КИИ
- моделирование угроз безопасности информации
- формирование требований к системе защиты информации (ТЗ)

Проектная документация

- определение субъектов и объектов доступа, политик управления доступом
- определение и обоснование орг. и тех. мер для ИБ ОКИИ, в том числе при взаимодействии с другими ОКИИ
- определение видов и типов СЗИ для реализации тех. мер
- выбор СЗИ с учетом категории значимости ОКИИ и совместимости с инфраструктурой
- разработка архитектуры системы защиты ОКИИ (места установки, взаимосвязи СЗИ)
- определение требований к параметрам настройки СЗИ, ПАК, ПО

Организационно-распорядительная документация

- назначение ответственных лиц, структурных подразделений, комиссий
- определение правил и процедур реализации мер по ИБ
- определение правил безопасной работы работников
- регламентация действий работников при возникновении нештатных ситуаций

Рабочая (эксплуатационная) документация

- описание архитектуры подсистемы безопасности ОКИИ;
- порядок и параметры настройки программных и программно-аппаратных средств, в том числе СЗИ;
- правила эксплуатации программных и программно-аппаратных средств, в том числе СЗИ (правила безопасной эксплуатации)

Организационные и технические меры

Ст.18.1 Федерального закона «О персональных данных»:

Меры, направленные на обеспечение выполнения оператором обязанностей, предусмотренных настоящим Федеральным законом

...**издание оператором**, являющимся юридическим лицом, **документов**, определяющих политику оператора в отношении обработки персональных данных, **локальных актов по вопросам обработки персональных данных**....

Ст.19 Федерального закона «О персональных данных»:

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...

Организационные меры по защите ПДн

- Определение и назначение ответственных лиц
- Разработка политики в отношении обработки ПДн и иной документации
- Отправка Уведомлений в Роскомнадзор
- Разработка согласий на обработку ПДн и иных форм, требуемых НПА
- Ведение журналов
- Обучение сотрудников
- Осуществление контроля за принимаемыми мерами

Не существует конкретного перечня документов, который должен быть разработан у оператора ПДн

- Приказ об ответственном за организацию обработки персональных данных
- Приказ об ответственном за обеспечение безопасности персональных данных в информационных системах персональных данных
- Приказ об утверждении перечня информационных систем персональных данных
- Приказ об утверждении перечня персональных данных
- Приказ о сотрудниках, осуществляющих обработку персональных данных
- Приказ об обеспечении безопасности материальных носителей персональных данных
- Приказ об обеспечении безопасности помещений, в которых размещены ИСПДн
- Приказ о системе разграничения доступа в ИСПДн
- Приказ об оценке вреда, который может быть причинен субъектам персональных данных
- Политика в отношении обработки персональных данных
- Порядок хранения, использования и передачи персональных данных сотрудников
- Акт определения уровня защищенности персональных данных
- Модель угроз безопасности персональных данных

Полный перечень рекомендуемых к разработке документов

Этап 1. ОРД и документация по установлению требований

- Приказ о комиссии по категорированию ОКИИ
- Приказ об утверждении Положения о комиссии по категорированию ОКИИ
- Приказ о структурном подразделении, осуществляющем функции по обеспечению информационной безопасности
- Приказ об ответственном за обеспечение информационной безопасности
- Приказ о сотрудниках, ответственных за выявление инцидентов информационной безопасности и реагирование на них
- План мероприятий по реализации требований Федерального закона № 187-ФЗ
- План реагирования на компьютерные инциденты и принятия мер по ликвидации последствий компьютерных атак
- Положение о внешнем взаимодействии при обеспечении безопасности КИИ
- Акт категорирования ОКИИ
- Сведения о результатах присвоения ОКИИ одной из категорий значимости либо об отсутствии необходимости присвоения ему одной из таких категорий
- Модель угроз безопасности информации ОКИИ
- Частное техническое задание на создание подсистемы безопасности ОКИИ

Этап 2. Проектная документация

Том проектной документации в составе:

- ✓ Пояснительная записка в объеме:
  - пределение объектов защиты;
  - определение политики управления доступом;
  - определение организационных и технических мер защиты;
  - определение видов и типов средств защиты информации;
  - определение архитектуры подсистемы безопасности.
- ✓ Спецификация оборудования и ПО подсистемы ИБ.
- ✓ Ведомость объемов работ.
- ✓ Графическая часть:
  - схема комплекса технических средств ОКИИ с указанием средств защиты информации;
  - схема размещения оборудования;
  - схема электропитания.

Состав ПД определяется и согласовывается с Заказчиком на этапе разработки ТЗ на создание ОКИИ и (или) ТЗ на создание системы защиты

Этап 3. Рабочая (эксплуатационная) документация

Том рабочей документации в составе:

- ✓ Основной комплект рабочих чертежей в объеме:
  - Схема структурная комплекса технических средств подсистемы информационной безопасности ОКИИ;
  - План размещения шкафа ИБ;
  - Схема электропитания шкафа ИБ;
  - Схема интерфейсных соединений;.
  - Кабельный журнал;
  - Спецификация оборудования, изделий и материалов.
- ✓ Параметрирование СЗИ:
  - Настройка средств защиты информации.
  - Настройка системного ПО.
  - План распределения IP-адресов.
- ✓ Документация по испытанию подсистемы ИБ:
  - Программа и методика предварительных испытаний подсистемы информационной безопасности ОКИИ
  - Программа опытной эксплуатации подсистемы информационной безопасности ОКИИ
  - Программа и методика приемочных испытаний подсистемы информационной безопасности ОКИИ
- ✓ Задание заводу на изготовление шкафа ИБ: схема электрических соединений, перечень элементов, чертеж общего вида

Состав РД определяется и согласовывается с Заказчиком на этапе разработки ТЗ на создание ОКИИ и (или) ТЗ на создание системы защиты

Этап 4. Организационно-распорядительная документация

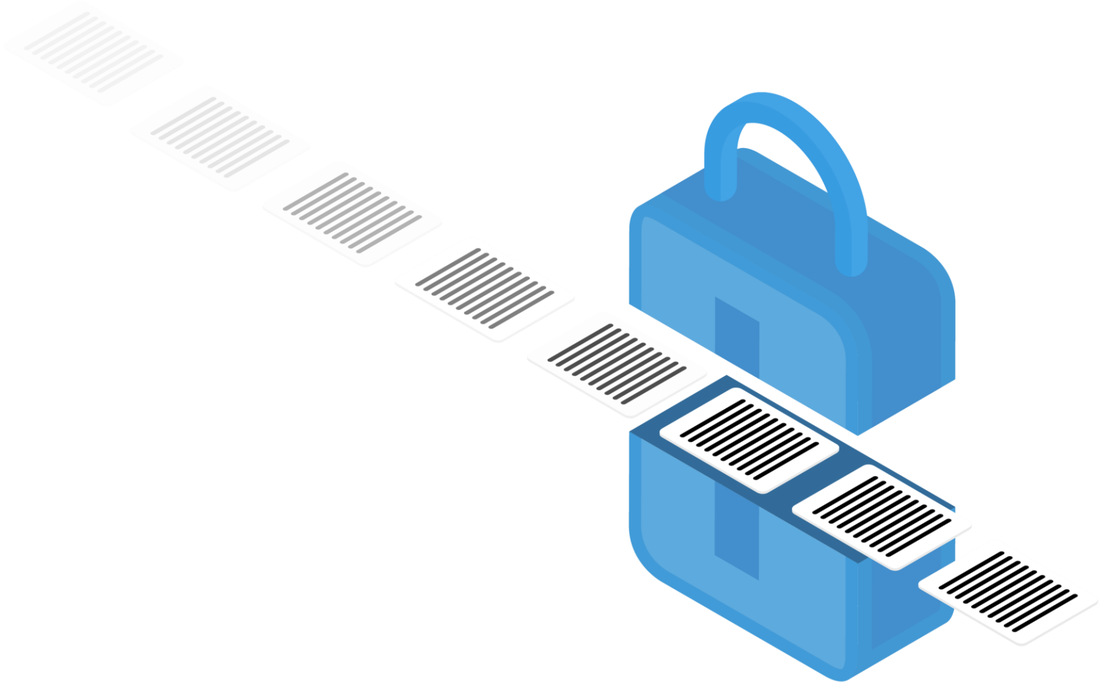
- Приказ об ответственном за обеспечение безопасности значимых объектов критической информационной инфраструктуры
- Приказ о сотрудниках, которым разрешены действия по внесению изменений в конфигурацию значимого объекта КИИ
- Приказ о силах обеспечения безопасности значимых объектов критической информационной инфраструктуры (при наличии значимых объектов КИИ)
- Приказ о назначении администратора безопасности объектов КИИ (при наличии значимых объектов КИИ)
- Приказ об ответственном за планирование и контроль мероприятий по обеспечению информационной безопасности (при наличии значимых объектов КИИ)
- Приказ об ответственном за управление (администрирование) подсистемой безопасности (при наличии значимых объектов КИИ)
- Приказ о контролируемых зонах

Этап 4. Организационно-распорядительная документация

- Регламент идентификации и аутентификации в объектах КИИ
- Регламент управления доступом в объектах КИИ
- Регламент ограничения программной среды в объектах КИИ
- Регламент защиты машинных носителей информации в объектах КИИ
- Регламент аудита безопасности объектов КИИ
- Регламент антивирусной защиты в объектах КИИ
- Регламент предотвращения вторжений (компьютерных атак) в объектах КИИ
- Регламент обеспечения целостности объектов КИИ
- Регламент обеспечения доступности объектов КИИ
- Регламент защиты технических средств и систем объектов КИИ
- Регламент защиты информационной (автоматизированной) системы и ее компонентов
- Регламент обновления программного обеспечения объектов КИИ
- Регламент действий сотрудников при возникновении нештатных ситуаций на объектах КИИ
- Регламент информирования и обучению персонала объектов КИИ

Что может дополнительно запросить регулятор у субъектов КИИ?

- ✓ Паспорт системы безопасности ЗО КИИ;
- ✓ Результаты оценки состояния технической защиты информации и обеспечения безопасности объектов информатизации:
  - Регламент оценки показателя КЗИ
  - Акт оценки показателя состояния технической защиты информации и обеспечения безопасности объектов информатизации
  - План реализации мероприятий по повышению уровня защищенности
- ✓ Приказ по утверждению Плана мероприятий по устранению уязвимостей
- ✓ Приказ по утверждению Регламента по анализу и установке обновлений безопасности
- ✓ Приказ по утверждению Регламента по выявлению, анализу и устранению критичных уязвимостей
- ✓ Результататы мероприятий по реагированию на компьютерный инцидент и принятию мер по ликвидации последствий компьютерных атак



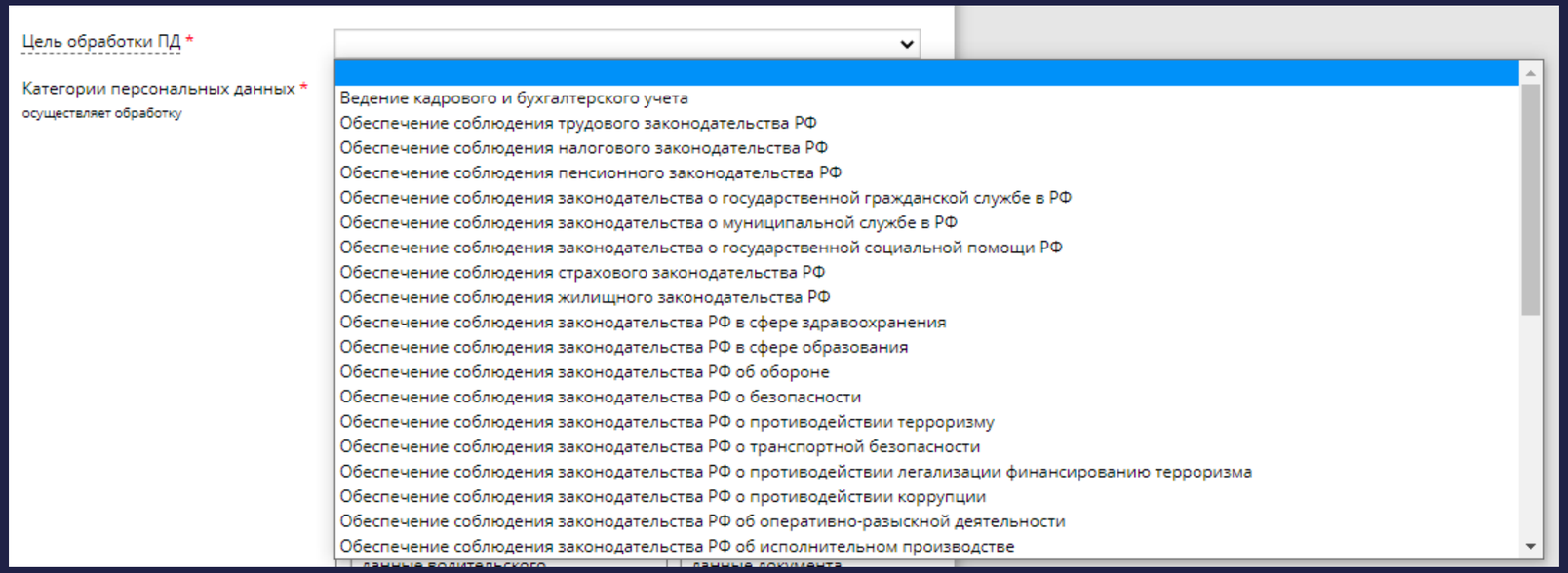
Уведомление в Роскомнадзор

- Об обработке ПДн
- Об изменении сведений, содержащихся в уведомлении о намерении осуществлять обработку ПДн
- О трансграничной передаче ПДн
- О факте неправомерной или случайной передачи ПДн, повлекшей нарушение прав субъектов ПДн
- О прекращении обработки ПДн

УВЕДОМЛЕНИЕ ОБ ОБРАБОТКЕ ПДН

Отменено большинство исключений, при котором можно было осуществлять обработку ПДн без соответствующего уведомления РКН (ч.2 ст.22 152-ФЗ)

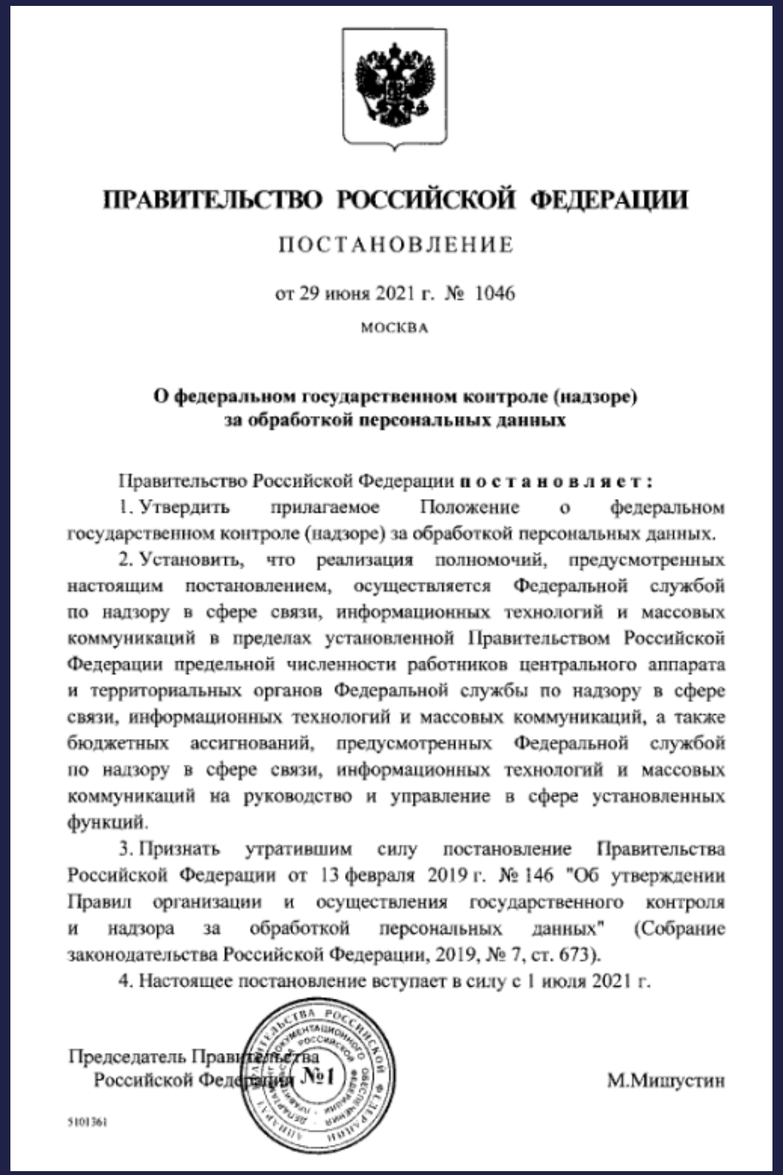
Ранее информация отправлялась в РКН в разрезе информационных систем организации, сейчас информация отправляется в разрезе конкретных и узких целей



Если организация подала уведомление об обработке ПДн по прежней форме до 26.12.2022 года, необходимо актуализировать сведения путем отправки в РКН уведомления о внесении изменений по ОБНОВЛЕННОЙ форме

МЕРОПРИЯТИЯ БЕЗ ВЗАИМОДЕЙСТВИЯ С КОНТРОЛИРУЕМЫМИ ЛИЦАМИ

- ✓ проводятся в рамках **ПП РФ от 29 июня 2021 г. № 1046** «О федеральном государственном контроле (надзоре) за обработкой персональных данных»
- ✓ включают в себя наблюдение:
  - за соблюдением требований при размещении информации **в сети «Интернет»**
  - за соблюдением требований посредством анализа **информации** о деятельности контролируемого лица, **которая представляется контролируемым лицом** (в том числе посредством использования федеральных государственных информационных систем) **в контролирующий орган** (территориальный орган)



ПРАВИТЕЛЬСТВО РОССИЙСКОЙ ФЕДЕРАЦИИ

ПОСТАНОВЛЕНИЕ

от 29 июня 2021 г. № 1046

МОСКВА

О федеральном государственном контроле (надзоре) за обработкой персональных данных

Правительство Российской Федерации **п о с т а н о в л я е т :**

1. Утвердить прилагаемое Положение о федеральном государственном контроле (надзоре) за обработкой персональных данных.

2. Установить, что реализация полномочий, предусмотренных настоящим постановлением, осуществляется Федеральной службой по надзору в сфере связи, информационных технологий и массовых коммуникаций в пределах установленной Правительством Российской Федерации предельной численности работников центрального аппарата и территориальных органов Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций, а также бюджетных ассигнований, предусмотренных Федеральной службой по надзору в сфере связи, информационных технологий и массовых коммуникаций на руководство и управление в сфере установленных функций.

3. Признать утратившим силу постановление Правительства Российской Федерации от 13 февраля 2019 г. № 146 "Об утверждении Правил организации и осуществления государственного контроля и надзора за обработкой персональных данных" (Собрание законодательства Российской Федерации, 2019, № 7, ст. 673).

4. Настоящее постановление вступает в силу с 1 июля 2021 г.

Председатель Правительства Российской Федерации М.Мишустин

5101361

А ТЕПЕРЬ ПРОСТЫМ ЯЗЫКОМ

В рамках мероприятия без взаимодействия с контролируемыми лицами Роскомнадзор удаленно проверяет:

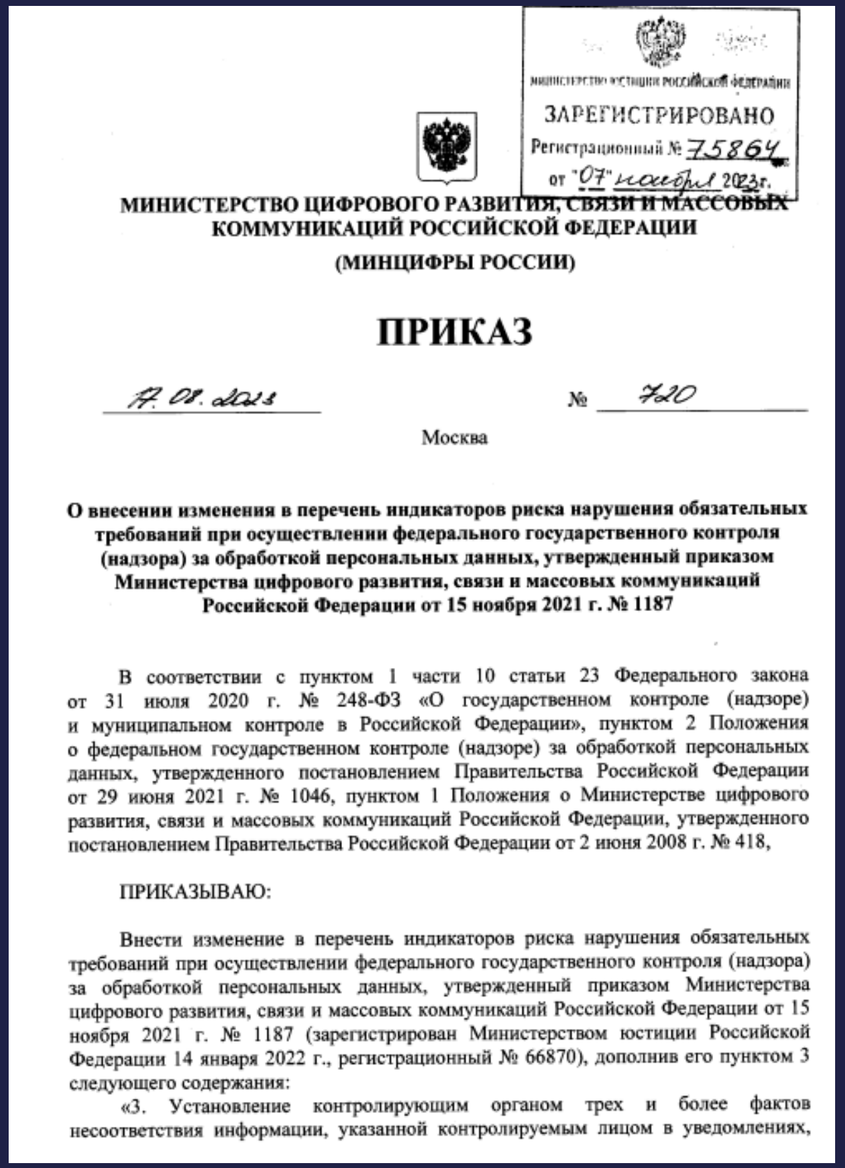
- сайт организации
- сведения, содержащиеся в реестре операторов, осуществляющих обработку ПДн

ТИПОВЫЕ НАРУШЕНИЯ, СВЯЗАННЫЕ С САЙТОМ ОРГАНИЗАЦИИ

- неопубликование на сайте документов, определяющих политику в отношении обработки ПДн, или опубликование некорректного документа
- использование на сайте электронных форм сбора ПДн в отсутствие механизма получения согласия на обработку ПДн
- отсутствие информирования пользователей об использовании файлов cookies
- распространение ПДн граждан в сети «Интернет» в отсутствие правовых оснований

ВНЕПЛАНОВАЯ ПРОВЕРКА?

С 18 ноября 2023 г. – установление Роскомнадзором **3 и более фактов несоответствия информации, указанной оператором в уведомлениях, политике обработки ПДн**, размещённой на сайте организации



Министерство юстиции Российской Федерации
ЗАРЕГИСТРИРОВАНО
Регистрационный № 75864
от "07" ноября 2023 г.

МИНИСТЕРСТВО ЦИФРОВОГО РАЗВИТИЯ, СВЯЗИ И МАССОВЫХ КОММУНИКАЦИЙ РОССИЙСКОЙ ФЕДЕРАЦИИ
(МИНЦИФРЫ РОССИИ)

ПРИКАЗ

07.09.2023 № 720

Москва

О внесении изменения в перечень индикаторов риска нарушения обязательных требований при осуществлении федерального государственного контроля (надзора) за обработкой персональных данных, утвержденный приказом Министерства цифрового развития, связи и массовых коммуникаций Российской Федерации от 15 ноября 2021 г. № 1187

В соответствии с пунктом 1 части 10 статьи 23 Федерального закона от 31 июля 2020 г. № 248-ФЗ «О государственном контроле (надзоре) и муниципальном контроле в Российской Федерации», пунктом 2 Положения о федеральном государственном контроле (надзоре) за обработкой персональных данных, утвержденного постановлением Правительства Российской Федерации от 29 июня 2021 г. № 1046, пунктом 1 Положения о Министерстве цифрового развития, связи и массовых коммуникаций Российской Федерации, утвержденного постановлением Правительства Российской Федерации от 2 июня 2008 г. № 418,

ПРИКАЗЫВАЮ:

Внести изменение в перечень индикаторов риска нарушения обязательных требований при осуществлении федерального государственного контроля (надзора) за обработкой персональных данных, утвержденный приказом Министерства цифрового развития, связи и массовых коммуникаций Российской Федерации от 15 ноября 2021 г. № 1187 (зарегистрирован Министерством юстиции Российской Федерации 14 января 2022 г., регистрационный № 66870), дополнив его пунктом 3 следующего содержания:

«3. Установление контролирующим органом трех и более фактов несоответствия информации, указанной контролируемым лицом в уведомлениях,

Взаимодействие с ФСТЭК России

Первичное:

- отправка регулятору сведений по форме приказа ФСТЭК России № 236;
- отправка регулятору модели угроз и технического задания (**в случае если ОКИИ является ГИС**)

Дальнейшее:

- согласование подключения ЗО КИИ к сети Интернет (**при необходимости**);
- отправка результатов категорирования новых ОКИИ;
- отправка регулятору актуализированных сведений по форме приказа ФСТЭК России № 236 **в случае изменений сведений об объекте КИИ, указанных в форме**;
- отправка регулятору актуализированных сведений по форме приказа ФСТЭК России № 236 **в случае изменения показателей критериев значимости или их значений**;
- отправка регулятору актуализированных сведений по форме приказа ФСТЭК России № 236 **не реже 1 раза в 5 лет;**
- подготовка ответов на запросы регулятора, осуществляемые в рамках мониторинга текущего состояния технической защиты информации и обеспечения безопасности значимых объектов критической информационной инфраструктуры;
- сопровождение регулятора при проведении выездной проверке соблюдения выполнения требований по ИБ

Взаимодействие с НКЦКИ и ФСБ России

Первичное:

- заключение соглашения с НКЦКИ об информационном взаимодействии;
- направление в НКЦКИ копии утвержденного Плана реагирования на компьютерные инциденты и принятия мер по ликвидации последствий компьютерных атак;
- отправка в ФСБ России модели угроз и технического задания (**в случае если ОКИИ является ГИС**)

Дальнейшее:

- взаимодействие в рамках мероприятий по реагированию на компьютерные инциденты и принятию мер по ликвидации последствий компьютерных атак

Проверки ФСТЭК России

Плановые:

- Проводятся по истечении 3 лет после внесения в реестр значимых объектов КИИ
- Проводятся по истечении 3 лет после проведения прошедшей проверки
- ФСТЭК России информирует субъектов КИИ, попавших в план проверок, до 1 января года проведения проверки

Внеплановые:

- Возникновение компьютерного инцидента
- Истечение срока выполнения предписания по результатам прошедшей проверки
- Поручение Президента РФ, Правительства РФ, требование прокурора

Изменения в законодательстве

- **Приказ Минцифры РФ от 17 августа 2023 г. N 720** «О внесении изменения в перечень индикаторов риска нарушения обязательных требований при осуществлении федерального государственного контроля (надзора) за обработкой персональных данных, утвержденный приказом Министерства цифрового развития, связи и массовых коммуникаций Российской Федерации от 15 ноября 2021 г. N 1187»
- Методика оценки показателя состояния технической защиты информации и обеспечения безопасности значимых объектов критической информационной инфраструктуры Российской Федерации (утв. ФСТЭК России 2 мая 2024 г.)

Изменения в законодательстве

Федеральный закон
от 14 июля 2022 № 266-ФЗ

«О внесении изменений в Федеральный закон «О персональных данных», отдельные законодательные акты Российской Федерации и признании утратившей силу части четырнадцатой статьи 30 Федерального закона «О банках и банковской деятельности»

Частично вступил в силу с 1 сентября 2022 г., вторая часть поправок – с 1 марта 2023 г.

Изменения касались:

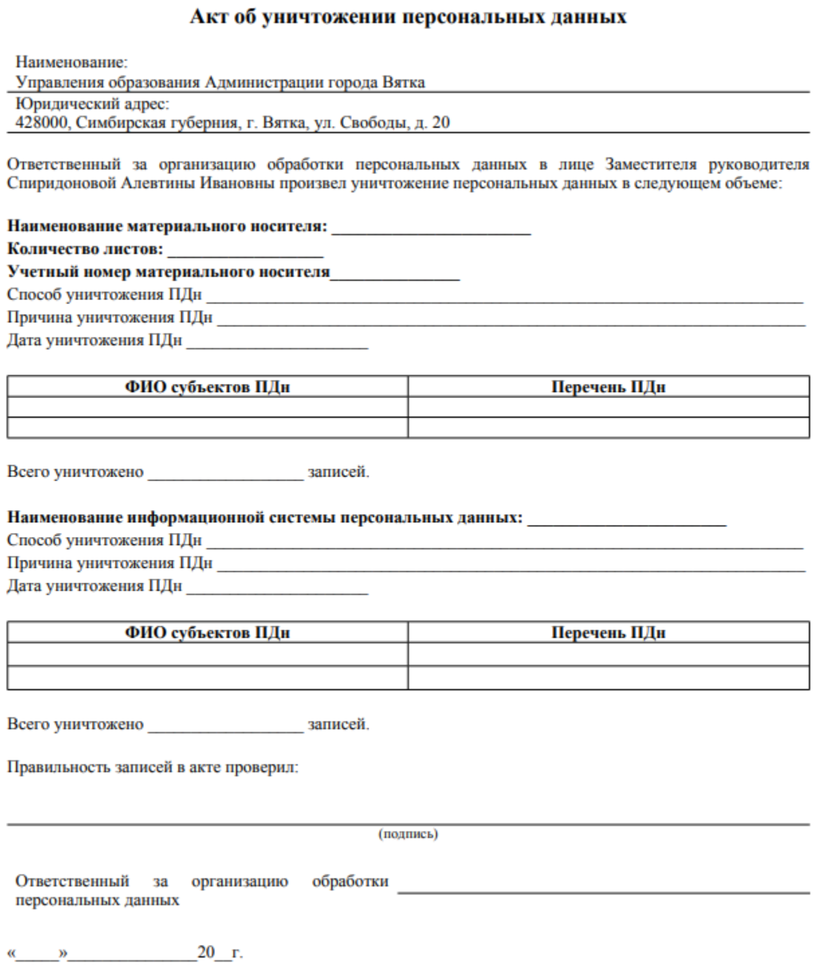
- порядка подтверждения уничтожения персональных данных
- оценки вреда, который может быть причинен субъектам персональных данных в случае нарушения закона о персональных данных
- трансграничной передачи данных
- уведомления Роскомнадзора об обработке персональных данных
- утечки персональных данных

Подтверждение уничтожения ПДн

С 1 марта 2023 года вступил в силу приказ Роскомнадзора № 179 «Об утверждении Требований к подтверждению уничтожения персональных данных»

Документы, подтверждающие уничтожение ПДн в зависимости от способа обработки данных:

- акт об уничтожении персональных данных
- выгрузка из журнала регистрации событий в информационной системе персональных данных



Акт об уничтожении персональных данных

Наименование:
Управления образования Администрации города Вятка
Юридический адрес:
428000, Симбирская губерния, г. Вятка, ул. Свободы, д. 20

Ответственный за организацию обработки персональных данных в лице Заместителя руководителя Спиридоновой Алевтины Ивановны произвел уничтожение персональных данных в следующем объеме:

Наименование материального носителя: _____
Количество листов: _____
Учетный номер материального носителя_____
Способ уничтожения ПДн _____
Причина уничтожения ПДн _____
Дата уничтожения ПДн _____

ФИО субъектов ПДн	Перечень ПДн

Всего уничтожено _____ записей.

Наименование информационной системы персональных данных: _____
Способ уничтожения ПДн _____
Причина уничтожения ПДн _____
Дата уничтожения ПДн _____

ФИО субъектов ПДн	Перечень ПДн

Всего уничтожено _____ записей.

Правильность записей в акте проверил:

_____
(подпись)

Ответственный за организацию обработки персональных данных _____

«_____»_____20__г.

Оценка вреда, который может быть причинен субъектам ПДн

С 1 марта 2023 года вступил в силу приказ Роскомнадзора № 178
«Об утверждении Требований к оценке вреда, который может быть причинен субъектам персональных данных в случае нарушения Федерального закона «О персональных данных»

Оператор определяет одну из степеней вреда в соответствии с требованиями:

- высокую
- среднюю
- низкую

Результаты оценки вреда оформляются соответствующим актом оценки вреда

Трансграничная передача ПДн

Ст.3 Федерального закона «О персональных данных»:

Трансграничная передача персональных данных - передача персональных данных на территорию иностранного государства органу власти иностранного государства, иностранному физическому лицу или иностранному юридическому лицу

С 1 марта операторы должны уведомлять Роскомнадзор о своем намерении осуществлять трансграничную передачу данных до начала осуществления этой деятельности.

Есть случаи, когда:

- можно осуществлять трансграничную передачу ПДн без уведомления
- Роскомнадзор вправе принять решение о запрете или ограничении трансграничной передачи

Обратите внимание:

Использование на сайте программы Google Analitics – будет расцениваться регулятором как трансграничная передача в адрес Google

Утечка ПДн

Приказ Роскомнадзора от 14 ноября 2022 г. № 187
«Об утверждении Порядка и условий взаимодействия Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций с операторами в рамках ведения реестра учета инцидентов в области персональных данных»

В РКН надо отправить 2 уведомления:

- первичное уведомление (в течение 24 часов) – информация о произошедшем инциденте
- дополнительное уведомление (в течение 72 часов) – информация о результатах внутреннего расследования выявленного инцидента

Уведомление направляется в виде документа на бумажном носителе или в форме электронного документа

Утечка ПДн

Приказ ФСБ России от 13 февраля 2023 г. № 77
«Об утверждении порядка взаимодействия операторов с государственной системой обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации, включая информирование ФСБ России о компьютерных инцидентах, повлекших неправомерную передачу (предоставление, распространение, доступ) персональных данных»

Операторы ПДн, которые не являются субъектами КИИ и у которых не организовано взаимодействие с ГосСОПКА, направляют информацию через сайт Роскомнадзора

Постановление Правительства Российской Федерации от 19.09.2024 № 1281 «О внесении изменений в постановление Правительства Российской Федерации от 8 февраля 2018 г. № 127»

5. Категорирование включает в себя:

а) определение процессов, указанных в пункте 3 настоящих Правил, в рамках выполнения функций (полномочий) или осуществления видов деятельности субъекта критической информационной инфраструктуры;

б) выявление управленческих, технологических, производственных, финансово-экономических и (или) иных процессов в рамках выполнения функций (полномочий) или осуществления видов деятельности субъектов критической информационной инфраструктуры, нарушение и (или) прекращение которых может привести к негативным социальным, политическим, экономическим, экологическим последствиям, последствиям для обеспечения обороны страны, безопасности государства и правопорядка (далее - критические процессы);

в) определение объектов критической информационной инфраструктуры, которые обрабатывают информацию, необходимую для обеспечения критических процессов, и (или) осуществляют управление, контроль или мониторинг критических процессов;

г) формирование перечня объектов критической информационной инфраструктуры, подлежащих категорированию (далее - перечень объектов);

д) оценку в соответствии с перечнем показателей критериев значимости масштаба возможных последствий в случае возникновения компьютерных инцидентов на объектах критической информационной инфраструктуры;

е) присвоение каждому из объектов критической информационной инфраструктуры одной из категорий значимости либо принятие решения об отсутствии необходимости присвоения им одной из категорий значимости.

Постановление Правительства Российской Федерации от 19.09.2024 № 1281 «О внесении изменений в постановление Правительства Российской Федерации от 8 февраля 2018 г. № 127»

15. Перечень объектов утверждается субъектом критической информационной инфраструктуры. Перечень объектов подлежит согласованию с государственным органом или российским юридическим лицом, выполняющим функции по разработке, проведению или реализации государственной политики и (или) нормативно-правовому регулированию в установленной сфере в части подведомственных им субъектов критической информационной инфраструктуры.

По мере необходимости указанный перечень может быть изменен в порядке, предусмотренном для его разработки и утверждения.

Максимальный срок категорирования не должен превышать одного года со дня утверждения субъектом критической информационной инфраструктуры перечня объектов (внесения дополнений, изменений).

Перечень объектов в течение 10 рабочих дней после утверждения направляется в печатном и электронном виде в федеральный орган исполнительной власти, уполномоченный в области обеспечения безопасности критической информационной инфраструктуры.

В перечень объектов в том числе включаются объекты критической информационной инфраструктуры филиалов, представительств субъекта критической информационной инфраструктуры.

Постановление Правительства Российской Федерации от 19.09.2024 № 1281 «О внесении изменений в постановление Правительства Российской Федерации от 8 февраля 2018 г. № 127»

14. Комиссия по категорированию в ходе своей работы:

а) определяет процессы, указанные в пункте 3 настоящих Правил, в рамках выполнения функций (полномочий) или осуществления видов деятельности субъекта критической информационной инфраструктуры;

б) выявляет наличие критических процессов у субъекта критической информационной инфраструктуры;

в) выявляет объекты критической информационной инфраструктуры, которые обрабатывают информацию, необходимую для обеспечения выполнения критических процессов, и (или) осуществляют управление, контроль или мониторинг критических процессов, готовит предложения для включения в перечень объектов, а также оценивает необходимость категорирования вновь создаваемых информационных систем, автоматизированных систем управления, информационно-телекоммуникационных сетей;

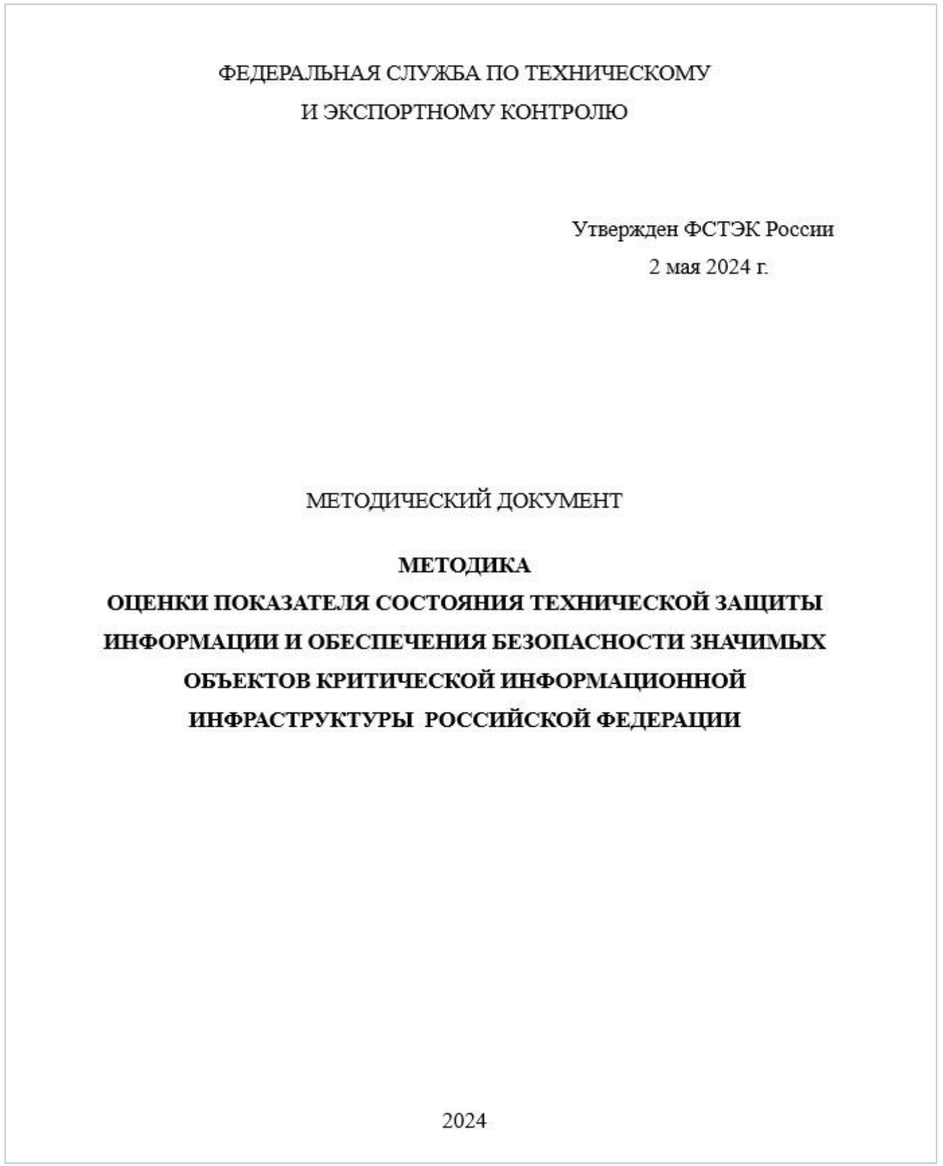
г) рассматривает возможные действия нарушителей в отношении объектов критической информационной инфраструктуры, а также иные источники угроз безопасности информации;

д) анализирует угрозы безопасности информации, которые могут привести к возникновению компьютерных инцидентов на объектах критической информационной инфраструктуры;

е) оценивает в соответствии с перечнем показателей критериев значимости масштаб возможных последствий в случае возникновения компьютерных инцидентов на объектах критической информационной инфраструктуры, определяет значения каждого из показателей критериев значимости или обосновывает их неприменимость;

ж) устанавливает каждому из объектов критической информационной инфраструктуры одну из категорий значимости либо принимает решение об отсутствии необходимости присвоения им категорий значимости.

Разбор изменений в Телеграм-канале «Мнение интегратора»



ФЕДЕРАЛЬНАЯ СЛУЖБА ПО ТЕХНИЧЕСКОМУ
И ЭКСПОРТНОМУ КОНТРОЛЮ

Утвержден ФСТЭК России
2 мая 2024 г.

МЕТОДИЧЕСКИЙ ДОКУМЕНТ

МЕТОДИКА
ОЦЕНКИ ПОКАЗАТЕЛЯ СОСТОЯНИЯ ТЕХНИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ И ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ЗНАЧИМЫХ ОБЪЕКТОВ КРИТИЧЕСКОЙ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ РОССИЙСКОЙ ФЕДЕРАЦИИ

2024

Предназначена для всех организаций (например, ОГВ, ОМСУ), которые в своих системах обрабатывают информацию, не составляющей государственную тайну (например, в ГИС, ИСПДн) и владельцев значимых объектов КИИ

Вышеупомянутые организации, применяя данную методику, могут:

- оценить текущее состояние защиты информации и (или) обеспечения безопасности объектов КИИ;
- разработать на основе такой оценки меры по повышению уровня защищенности;
- провести оценку эффективности деятельности заместителя руководителя организации, на которого возложены полномочия по обеспечению ИБ, и (или) структурного подразделения, осуществляющего функции по обеспечению ИБ организации.

Расчет показателя защищенности

$$К_{ЗИ}=(k_{11}+k_{12}+k_{13})R_1+(k_{21}+k_{22}+...+k_{2i})R_2+(k_{31}+k_{32}+...+k_{3i})R_3+(k_{41}+k_{42}+...+k_{4i})R_4,$$

Где: R_j **— весовой коэффициент**
j — й группы частных показателей безопасности

Значение $К_{ЗИ}$	Текущее состояние защиты информации (обеспечения безопасности объектов КИИ)
$К_{ЗИ}=1$	Обеспечивается минимальный уровень защиты от типовых актуальных угроз безопасности информации. Уровень состояния защищенности характеризуется как минимальный базовый («зеленый»)
$0,75<К_{ЗИ}<1$	Минимальный уровень защиты от актуальных угроз безопасности информации не обеспечивается, имеются предпосылки реализации актуальных угроз безопасности информации. Уровень состояния защищенности характеризуется как низкий («оранжевый»)
$К_{ЗИ}\leq0,75$	Минимальный уровень защиты от актуальных угроз безопасности информации не обеспечивается, имеется реальная возможность реализации актуальных угроз безопасности информации. Уровень состояния защищенности характеризуется как критический («красный»)

Ответственность за несоблюдение требований в сфере защиты КИИ (УК РФ)

Уголовная ответственность			
УК РФ	274.1 (ч.1)	Создание, распространение и (или) использование компьютерных программ либо иной компьютерной информации, заведомо предназначенных для неправомерного воздействия на КИИ РФ, в том числе для уничтожения, блокирования, модификации, копирования информации, содержащейся в ней, или нейтрализации средств защиты указанной информации.	• принудительные работы до 5 лет с ограничением свободы до 2 лет или без такового; • лишение свободы 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.
	274.1 (ч.2)	Неправомерный доступ к охраняемой компьютерной информации, содержащейся в КИИ РФ, в том числе с использованием компьютерных программ либо иной компьютерной информации, которые заведомо предназначены для неправомерного воздействия на КИИ РФ, или иных вредоносных компьютерных программ, если он повлек причинение вреда КИИ РФ	• 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; • лишение 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
	274.1 (ч.3)	Нарушение правил эксплуатации средств хранения, обработки или передачи охраняемой компьютерной информации, содержащейся в КИИ РФ, или ИС, ИТС, АСУ, сетей электросвязи, относящихся к КИИ РФ, либо правил доступа к указанным информации, ИС, ИТС, АСУ, сетям электросвязи, если оно повлекло причинение вреда КИИ РФ	• принудительные работы до 5 лет с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до 3 лет или без такового; • лишение свободы на срок до 6 лет с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до 3 лет или без такового.
	274.1 (ч.4)	Деяния, предусмотренные частями 1-3 статьи 274.1, совершенные группой лиц по предварительному сговору или организованной группой, или лицом с использованием своего служебного положения	лишение свободы на срок от 3 до 8 лет с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до 3 лет или без такового.
	274.1 (ч.5)	Деяния, предусмотренные частями 1-4 статьи 274.1, если они повлекли тяжкие последствия	лишение свободы на срок от 5 до 10 лет с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до 5 лет или без такового.

Статистика применения ст.274.1 УК РФ: https://valerykomarov.blogspot.com/p/2741.html

Ответственность за несоблюдение требований в сфере защиты КИИ (КоАП РФ)

НПА	Статья	Тип нарушения	Наказание
		Административная ответственность	
КоАП РФ	13.12.1 (ч.1)	Нарушение требований к созданию систем безопасности значимых объектов КИИ РФ и обеспечению их функционирования либо требований по обеспечению безопасности значимых объектов КИИ РФ, установленных федеральными законами и принятыми в соответствии с ними иными нормативными правовыми актами РФ, если такие действия (бездействие) не содержат уголовно наказуемого деяния	• для должностных лиц – штраф от 10 000 до 50 000 рублей; • для юридических лиц – штраф от 50 000 до 100 000 рублей.
	13.12.1 (ч.2)	Нарушение порядка информирования о компьютерных инцидентах, реагирования на них, принятия мер по ликвидации последствий компьютерных атак, проведенных в отношении значимых объектов КИИ РФ, установленного федеральными законами и принятыми в соответствии с ними иными нормативными правовыми актами РФ	• для должностных лиц – штраф от 10 000 до 50 000 рублей; • для юридических лиц – штраф от 100 000 до 500 000 рублей.
	13.12.1 (ч.3)	Нарушение порядка обмена информацией о компьютерных инцидентах между субъектами КИИ РФ, между субъектами КИИ РФ и уполномоченными органами иностранных государств, международными организациями, международными неправительственными и иностранными организациями, осуществляющими деятельность в области реагирования на компьютерные инциденты	• для должностных лиц – штраф от 20 000 до 50 000 рублей; • для юридических лиц – штраф от 100 000 до 500 000 рублей.
	19.7.15 (ч.1)	Непредставление или нарушение сроков представления в федеральный орган исполнительной власти, уполномоченный в области обеспечения безопасности КИИ РФ, сведений о результатах присвоения объекту КИИ РФ одной из категорий значимости, предусмотренных законодательством в области обеспечения безопасности КИИ РФ, либо об отсутствии необходимости присвоения ему одной из таких категорий либо представление недостоверных сведений	• для должностных лиц – штраф от 10 000 до 50 000 рублей; • за повторное нарушение – штраф от 10 000 до 50 000 рублей (ч.3 ст. 19.7.15); • для юридических лиц – штраф от 50 000 до 100 000 рублей; • за повторное нарушение – штраф от 100 000 до 200 000 рублей (ч.3 ст. 19.7.15).
	19.7.15 (ч.2)	Непредставление или нарушение порядка либо сроков представления в государственную систему обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы РФ информации, предусмотренной законодательством в области обеспечения безопасности КИИ РФ, за исключением случаев, предусмотренных частью 2 статьи 13.12.1 КоАП	• для должностных лиц – штраф от 10 000 до 50 000 рублей; • для юридических лиц – штраф от 100 000 до 500 000 рублей.

Ответственность за несоблюдение требований законодательства в сфере защиты ПДн

Лица, виновные в нарушении требований Федерального закона «О персональных данных», несут предусмотренную законодательством РФ, а именно: гражданско-правовую, уголовную, административную, дисциплинарную и иную ответственность (ст.24 Федерального закона «О персональных данных»)

Полная информация о штрафах

Ответственность за несоблюдение требований в области ПДн (КоАП РФ)

НПА	Статья	Тип нарушения	Наказание (штраф)
Административная ответственность			
КоАП РФ	13.11 (ч.1)	Обработка данных в случаях, не предусмотренных законодательством	• для граждан –от 2 000 до 6 000 рублей; • за повторное нарушение – от 4 000 до 12 000 рублей; • для должностных лиц – от 10 000 до 20 000 рублей; • за повторное нарушение – 20 000 до 50 000 рублей; • для ИП за повторное нарушение –от 50 000 до 100 000 рублей; • для юридических лиц – от 60 000 до 100 000 рублей. • за повторное нарушение – от 100 000 до 300 000 рублей.
	13.11 (ч.2)	Обработка ПДн без письменного согласия субъекта	• для граждан – от 10 000 до 15 000 рублей; • за повторное нарушение – от 15 000 до 30 000 рублей; • для должностных лиц – от 100 000 до 300 000 рублей; • за повторное нарушение – от 300 000 до 500 000 рублей; • для ИП за повторное нарушение – от 500 000 до 1 000 000 рублей; • для юридических лиц – от 300 000 до 700 000 рублей; • за повторное нарушение – от 1 000 000 до 1 500 000 рублей.
	13.11 (ч.3)	Невыполнение обязанности по опубликованию или обеспечению иным образом неограниченного доступа к документу, определяющему политику оператора в отношении обработки ПДн, или сведениям о реализуемых требованиях к защите ПДн	• для граждан – от 1 500 до 3 000 рублей; • для должностных лиц – от 6 000 до 12 000 рублей; • для ИП – от 10 000 до 20 000 рублей; • для юридических лиц – от 30 000 до 60 000 рублей.
	13.11 (ч.4)	Невыполнение обязанности по предоставлению субъекту ПДн информации, касающейся обработки его ПДн	• для граждан –от 2 000 до 4 000 рублей; • для должностных лиц – от 8 000 до 12 000 рублей; • для ИП – от 20 000 до 30 000 рублей; • для юридических лиц – от 40 000 до 80 000 рублей.

Ответственность за несоблюдение требований в области ПДн (КоАП РФ)

НПА	Статья	Тип нарушения	Наказание (штраф)
Административная ответственность			
КоАП РФ	13.11 (ч.5)	Невыполнение оператором в сроки, установленные законодательством, требования об уточнении ПДн, их блокировании или уничтожении.	• для граждан – от 2 000 до 4 000 рублей; • за повторное нарушение – от 20 000 до 30 000 рублей; • для должностных лиц – от 8 000 до 20 000 рублей; • за повторное нарушение – от 30 000 до 50 000 рублей; • для ИП – от 20 000 до 40 000 рублей; • за повторное нарушение – от 50 000 до 100 000 рублей; • для юридических лиц – от 50 000 до 90 000 рублей; • за повторное нарушение – от 300 000 до 500 000 рублей.
	13.11 (ч.6)	Невыполнение при обработке ПДн без использования средств автоматизации обязанности по соблюдению условий, обеспечивающих сохранность ПДн при хранении материальных носителей ПДн и исключающих несанкционированны к ним доступ.	• для граждан – от 1 500 до 4 000 рублей; • для должностных лиц – от 8 000 до 20 000 рублей; • для ИП – от 20 000 до 40 000 рублей; • для юридических лиц –от 50 000 до 100 000 рублей.
	13.11 (ч.7)	Невыполнение оператором, являющимся государственным или муниципальным органом, обязанности по обезличиванию ПДн либо несоблюдение установленных требований или методов по обезличиванию ПДн.	• для должностных лиц – от 6 000 до 12 000 рублей.
	13.11 (ч.8)	Невыполнение оператором при сборе ПДн, в том числе посредством информационно-телекоммуникационной сети «Интернет», предусмотренной законодательством РФ в области ПДн обязанности по обеспечению записи, систематизации, накопления, хранения, уточнения (обновления, изменения) или извлечения ПДн граждан РФ с использованием баз данных, находящихся на территории РФ.	• для граждан – от 30 000 до 50 000 рублей; • за повторное нарушение – от 50 000 до 100 000 рублей; • для должностных лиц – от 100 000 до 200 000 рублей; • за повторное нарушение – от 500 000 до 800 000 рублей; • для ИП и юридических лиц – от 1 000 000 до 6 000 000 рублей.

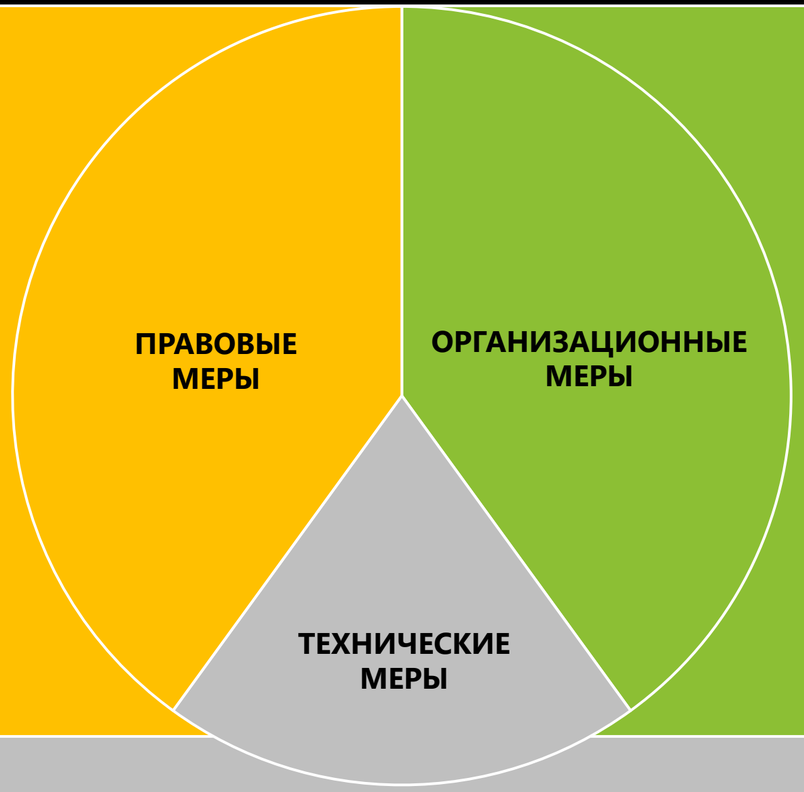
Ответственность за несоблюдение требований в области ПДн (КоАП РФ)

НПА	Статья	Тип нарушения	Наказание (штраф)
	13.11.2	Незаконное использование в случаях, предусмотренных ч. 8 ст. 10 Федерального закона от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации», принадлежащих иностранным юридическим лицам и (или) иностранным гражданам информационных систем и (или) программ для электронных вычислительных машин, которые предназначены и (или) используются для обмена электронными сообщениями исключительно между пользователями этих информационных систем и (или) программ для электронных вычислительных машин, при котором отправитель электронного сообщения определяет получателя или получателей электронного сообщения и не предусматривается размещение пользователями сети «Интернет» общедоступной информации в сети «Интернет» либо подключение к этим информационным системам и (или) программам для электронных вычислительных машин иных информационных систем в случаях, предусмотренных законодательством Российской Федерации об информации, информационных технологиях и о защите информации	• для должностных лиц – от 30 000 до 50 000 рублей; • для юридических лиц – от 100 000 до 700 000 рублей.
	13.11.3	Размещение и обновление банками, многофункциональными центрами предоставления государственных и муниципальных услуг, иными организациями в случаях, определенных федеральными законами, биометрических персональных данных субъекта персональных данных в государственной информационной системе "Единая система идентификации и аутентификации физических лиц с использованием биометрических персональных данных" с нарушением установленных законодательством Российской Федерации требований	• для должностных лиц – от 100 000 до 300 000 рублей; • для юридических лиц – от 500 000 до 1 000 000 рублей.

ПРОБЛЕМЫ РЕАЛИЗАЦИИ МЕР ПО ЗАЩИТЕ ИНФОРМАЦИИ

Законодательство Российской Федерации характеризуется:

- Большим количеством действующих НПА
- Частыми изменениями
- Сложным юридическим и, одновременно, техническим изложением правовых норм
- Малой степенью конкретизации
- Различным трактованием государственными регуляторами



Организационно-распорядительная документация организации должна:

- Актуализироваться каждый раз при любых штатных или инфраструктурных изменениях
- Не зависеть от компетенций или загруженности сотрудника, который её разрабатывает
- Не просто лежать на полке, а способствовать повышению осведомленности и ответственности сотрудников организации
- Быть единой и распространяться на все подконтрольные организации

Технические средства защиты информации

альфа|реестр

- Учет информационных систем
- Автоматизированное формирование единого реестра ГИС/ИС
- Создание портала для публикации сведений об информационных системах
- Формирование графического ИТ-ландшафта

альфа|док

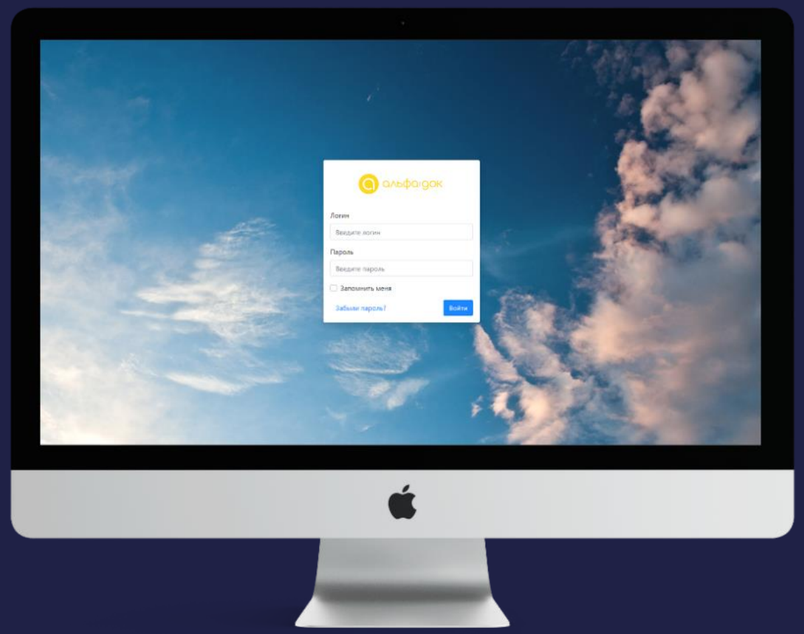
- Реализация организационных мер по обработке и защите ПДн, КИИ, ГИС, включая разработку и актуализацию документации
- Контроль корректности и достаточности применения СЗИ
- Управление процессом по защите информации в курируемых организациях

альфа|крипто

- Электронный учет СКЗИ в соответствии с требованиями ФСБ России
- Автоматизация процесса выдачи СКЗИ, включая электронную очередь
- Контроль сроков действия лицензий и сертификатов

альфа|коннект

- Цифровизация регламентов подачи и обработки заявок на подключение пользователей к ИС
- Контроль выполнения требований по подключению пользователей к ИС
- Ведение реестра пользователей



альфа-док

Демонстрация программного комплекса

Спецпредложение для участников вебинара:

При покупке платформенного решения в этом году –

скидка 10%

При запросе ценового предложения в этом году для бюджетирования на следующий –

скидка 5%

на платформенные решения

ПРОТЕСТИРУЙТЕ БЕСПЛАТНО

НА ALFA-DOC.RU

ЗАКАЖИТЕ ПИЛОТНЫЙ ПРОЕКТ

НА ВАШИХ МОЩНОСТЯХ

- 8 800 3333-872
- info@ksb-soft.ru
- ksb-soft.ru

Телеграм
Экосистема Альфа

Компания КСБ-СОФТ оказывает полный комплекс услуг по защите объектов КИИ

Безопасность объектов КИИ

Оценка показателя состояния технической защиты информации и обеспечения безопасности значимых объектов критической информационной инфраструктуры

Импортозамещение

SOCRAT - центр мониторинга и реагирования на инциденты информационной безопасности

Телеграм-канал «Мнение интегратора»