альфа

Менеджмент защиты информации

Строим систему управления ИБ в соответствии с новыми требованиями законодательства

СИСТЕМА МЕНЕДЖМЕНТА ЗАЩИТЫ ИНФОРМАЦИИ

ИБ-процессы должны быть встроены в общую систему управления организацией по циклу

PDCA (Plan-Do-Check-Act)

ISO/IEC 27001

↓

ГОСТ Р ИСО/МЭК 27001-2021

↓

Приказ ФСТЭК России №117



ВЫПОЛНЕНИЕ ТРЕБОВАНИЙ ПРИКАЗА ФСТЭК РОССИИ № 117

Я – ОТВЕТСТВЕННЫЙ ЗА ЗАЩИТУ ИНФОРМАЦИИ

*«Требования о защите информации, содержащейся в государственных информационных системах, иных информационных системах государственных органов, **государственных унитарных предприятий**...»*

Государственное унитарное предприятие (ГУП) — это коммерческая организация, которая не владеет закреплённым за ней имуществом, а использует его по воле собственника — государства.

Сферы: ЖКХ и коммунальные услуги, транспорт, инфраструктура и т.д.

Мне нужно:

- ✓ Разбираться в требованиях и оперативно реагировать на изменения в них
- ✓ **Разработать документацию:**
  - *Политику защиты информации;*
  - *стандарт и регламенты защиты информации;*
  - *приказы и инструкции;*
  - *техническую документацию (МУ, ТЗ и Техпаспорт)*
  - *различные акты и т.д.*
- ✓ **Проводить оценку Кзи *(раз в 6 месяцев)* и Узи *(раз в 3 года)***
- ✓ Планировать мероприятия по ИБ
- ✓ Взаимодействовать с ГосСОПКА
- ✓ **Повышать уровень знаний сотрудников *(п.56 приказа)***
- ✓ Оценить свою готовность к проверке ФСТЭК России

- ✓ **Получать ответы на интересующие вопросы**

ИНФОРМАЦИОННОЕ СООБЩЕНИЕ ФСТЭК РОССИИ ОТ 12.03.2026

- **В первоочередном порядке необходимо разработать и утвердить:**
  - политику защиты информации
  - внутренние стандарты по защите информации
  - внутренние регламенты по защите информации
- **Рекомендуется разработать план перехода**, содержащий описание мероприятий и мер по защите информации, направленных на реализацию положений требований, утвержденных приказом ФСТЭК России № 117, **со сроками их реализации**

Информационное сообщение ФСТЭК России от 12 марта 2026 г. N 240/22/1492

ПРОКУРАТУРА, 04.09.2026

ПРОКУРАТУРА
Российской Федерации

[redacted]

04.09.2026 [redacted]

ПРЕДСТАВЛЕНИЕ
об устранении нарушений требований законодательства в сфере информационных технологий и защиты информации

Прокуратурой [redacted] по результатам анализа вскрыты недостатки в деятельности [redacted] при исполнении законодательства в сфере информационных технологий и защиты информации.

В соответствии с ч. 5 ст. 16 Федерального закона от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации» Требования о защите информации, содержащейся в государственных информационных системах, иных информационных системах государственных органов, государственных унитарных предприятий, государственных учреждений, а также при использовании технических средств и программ для электронных вычислительных машин и баз данных в соответствии с ч. 5.1 ст. 13 настоящего Федерального закона устанавливаются федеральным органом исполнительной власти в области обеспечения безопасности и федеральным органом исполнительной власти, уполномоченным в области противодействия техническим разведкам и технической защиты информации, в пределах их полномочий. При создании и эксплуатации государственных информационных систем, иных информационных систем государственных органов, государственных унитарных предприятий, государственных учреждений применяемые в целях защиты информации методы и способы ее защиты должны соответствовать указанным требованиям.

Согласно п. 14 Требований о защите информации, содержащейся в государственных информационных системах, иных информационных системах государственных органов, государственных унитарных предприятий, государственных учреждений, утвержденных приказом ФСТЭК России от 11.04.2025 № 117, организация деятельности по защите информации должна включать:

1) разработку и утверждение политики защиты информации, содержащей в том числе:

- область действия политики, включая перечень информации, информационных систем, компонентов информационно-телекоммуникационной инфраструктуры, подлежащих защите в соответствии с Требованиями;

- цели и задачи защиты информации;
- принципы защиты информации;
- перечни объектов защиты, включая программные, программно-аппаратные средства, информационные системы, сети и подсети, образующие информационно-телекоммуникационную инфраструктуру;
- категории лиц, участвующих в защите информации, их обязанности (функции) и полномочия;
- состав организационной системы управления деятельностью по защите информации и схему взаимодействия ее элементов;
- ответственность работников за нарушение требований о защите информации и установленных оператором (обладателем информации) правил обработки информации;

2) разработку и утверждение внутренних стандартов по защите информации, содержащих в том числе:

- требования к первичной идентификации лиц, обладающих правами доступа к информационным системам и (или) содержащейся в них информации и их использованию (далее - пользователи);
- требования к применяемым моделям доступа пользователей;
- перечень разрешенного и (или) запрещенного для использования программного обеспечения;
- требования к типовым конфигурациям и настройкам программных, программно-аппаратных средств;
- требования к конфигурациям и настройкам программных, программно-аппаратных средств, предназначенных для обеспечения доступа пользователей из информационных систем к информационно-телекоммуникационной сети «Интернет» (далее - сеть «Интернет»);
- требования к конфигурациям и настройкам программных, программно-аппаратных средств, предназначенных для обеспечения удаленного доступа пользователей к информационным системам и содержащейся в них информации, включая требования к обеспечению безопасной дистанционной работы;
- ограничения и запреты действий для пользователей при использовании и обеспечении эксплуатации ими информационных систем;
- требования к защите физических и виртуальных устройств информационных систем, имеющих доступ к сети «Интернет» (далее - конечные устройства);
- требования к защите мобильных устройств, планшетных, переносных компьютеров, применяемых пользователями для доступа к информационным системам (за исключением мобильных устройств, предназначенных для доступа к сайтам сети «Интернет» и иным публичным веб-ресурсам) (далее - мобильные устройства);
- требования к непрерывности функционирования информационных систем;
- требования к резервному копированию информации, программного обеспечения и его конфигураций;
- требования к сбору, регистрации и анализу событий, связанных с возможным нарушением безопасности информации, нарушением функционирования информационных систем, реализацией угроз безопасности информации (далее - события безопасности);

Вместе с тем, установлено, что в учреждении организация деятельности по защите информации проведена не в полном объеме: отсутствуют или находятся в неактуализированном в соответствии с приказом ФСТЭК России от 11.04.2025 № 117 состоянии необходимые внутренние локальные акты, что свидетельствует о необходимости разработки и утверждения политики защиты информации, внутренних стандартов и регламентов по защите информации.

Приведенные в представлении нарушения закона стали возможными вследствие ненадлежащего исполнения своих должностных обязанностей, ответственными за данное направление работы должностными лицами, что в соответствии со ст. 192 Трудового кодекса Российской Федерации, является основанием для привлечения к дисциплинарной ответственности.

На основании вышеизложенного в целях обеспечения верховенства закона, единообразного его применения, единства и укрепления законности, защиты прав и свобод человека и гражданина, а также охраняемых законом интересов общества и государства, руководствуясь ст. 24 Федерального закона «О прокуратуре Российской Федерации»,

ТРЕБУЮ:

1. Рассмотреть настоящее представление с обязательным участием представителя прокуратуры района. О дате и времени рассмотрения уведомить прокуратуру района заблаговременно.

2. Принять конкретные меры по устранению допущенных нарушений закона, причин и условий, им способствующих, и недопущению подобных нарушений впредь.

3. О результатах рассмотрения настоящего представления и принятых мерах сообщить прокурору района безотлагательно после его рассмотрения.

Предлагаю рассмотреть вопрос о привлечении к дисциплинарной ответственности лиц, виновных в ненадлежащем осуществлении своих должностных обязанностей. В случае принятия решения о привлечении работников к дисциплинарной ответственности прошу предоставить копию соответствующего приказа.

[redacted]

ПЕРСОНАЛЬНЫЕ ДАННЫЕ

Я - ОТВЕТСТВЕННЫЙ ЗА ОРГАНИЗАЦИЮ ОБРАБОТКИ ПДН

Мне нужно:

- ✓ Разбираться в требованиях и оперативно реагировать на изменения в них
- ✓ Разработать документацию по обработке и защите ПДн:
  - *Политику в отношении обработки ПДн*
  - *приказы и инструкции*
  - *техническую документацию (МУ, ТЗ и Техпаспорт)*
  - *различные акты и т.д.*
- ✓ Отправить уведомление в РКН
- ✓ Наладить работу с согласиями
- ✓ Вести необходимые журналы
- ✓ Планировать мероприятия по внутреннему контролю
- ✓ **Привести в порядок сайт организации**
- ✓ Оценить свою готовность к проверке РКН

- ✓ **Получать ответы на интересующие вопросы**

РОСКОМНАДЗОР, 24.08.2026

РОСКОМНАДЗОР

УПРАВЛЕНИЕ ФЕДЕРАЛЬНОЙ СЛУЖБЫ ПО НАДЗОРУ В СФЕРЕ СВЯЗИ, ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ И МАССОВЫХ КОММУНИКАЦИЙ ПО ЦЕНТРАЛЬНОМУ ФЕДЕРАЛЬНОМУ ОКРУГУ
(Управление Роскомнадзора по Центральному федеральному округу)

117997, ГСП-7 , Москва г., ш. Старокаширское, д. 2, к. 10
Справочная: (495)587-44-85; факс (495)249-24-16
E-mail: rsockanc77@rkn.gov.ru

24.08.2026 №

На

О направлении требования

Управлением Роскомнадзора по Центральному федеральному округу (далее – Управление) в соответствии с пп. 58-60 Положения о федеральном государственном контроле (надзоре) за обработкой персональных данных, утвержденного постановлением Правительства от 29.06.2021 № 1046, на основании задания на проведение контрольного (надзорного) мероприятия по контролю без взаимодействия с контролируемым лицом, утвержденного заместителем руководителя Управления – начальник территориального отдела, от 13.08.2026 № в период с 17.08.2026 по 19.08.2026 проведено контрольное (надзорное) мероприятие без взаимодействия с контролируемым лицом в отношении (далее также – Оператор).

Управлением в целях предупреждения, выявления и пресечения нарушения обязательных требований, установленных законодательством Российской Федерации в области персональных данных, проведен анализ интернет-ресурса (далее – Сайт), по результатам которого установлено следующее.

На Сайте размещены формы сбора персональных данных (в том числе:

использованием которых собираются персональные данные пользователей Сайта (в том числе: Посетители сайта).

Сбор и последующая обработка персональных данных допускается в случаях, предусмотренных ч. 1 ст. 6 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных» (далее – Закон), в частности:

для исполнения договора, стороной которого либо выгодоприобретателем или поручителем, по которому является субъект персональных данных, а также для заключения договора по инициативе субъекта персональных данных или договора, по которому субъект персональных данных будет являться выгодоприобретателем или поручителем (п. 5 ч. 1 ст. 6 Закона);

для достижения целей, предусмотренных международным договором Российской Федерации или законом, для осуществления и выполнения возложенных законодательством Российской Федерации на оператора функций, полномочий и обязанностей (п. 2 ч. 1 ст. 6 Закона).

Вместе с тем при сборе персональных данных на Сайте выявлено отсутствие правовых оснований обработки персональных данных, предусмотренных ч. 1 ст. 6 Закона.

Кроме того, на Сайте выявлен факт использования метрической программы (метрических программ) Яндекс Метрика, LiveInternet, функционал которой позволяет определить уникального посетителя Сайта, формировать сведения о его предпочтениях и поведении на Сайте, что является обработкой персональных данных и допускается в случаях, установленных ч. 1 ст. 6 Закона.

Вместе с этим в ходе осмотра Сайта выявлено отсутствие правовых оснований обработки персональных данных, собираемых посредством метрической программы (метрических программ) Яндекс Метрика, LiveInternet, в соответствии с ч. 1 ст. 6 Закона, а равно информирование при входе на Сайт об обработке персональных данных с использованием метрической программы (метрических программ) Яндекс Метрика, LiveInternet.

Ответ на указанный запрос с приложением подтверждающих документов можно по адресу электронной почты:

Одновременно разъясняем, в случае непредставления или несвоевременного представления в государственный орган сведений, представление которых предусмотрено законом и необходимо для осуществления этим органом его законной

деятельности, а равно представление в государственный орган таких сведений в неполном объеме или в искаженном виде, предусмотрена административная ответственность в соответствии со статьей 19.7 Кодекса Российской Федерации об административных правонарушениях (далее – КоАП РФ).

Одновременно разъясняем, что за нарушение требований законодательства Российской Федерации в области персональных данных предусмотрена административная ответственность по ст. 13.11 КоАП РФ.

Невыполнение оператором в сроки, установленные законодательством Российской Федерации в области персональных данных, требования уполномоченного органа по защите прав субъектов персональных данных образует состав административного правонарушения в соответствии с ч. 5 ст. 13.11 КоАП РФ.

Заместитель руководителя Управления – начальник территориального отдела

ТИПОВЫЕ НАРУШЕНИЯ, СВЯЗАННЫЕ С САЙТОМ ОРГАНИЗАЦИИ

Чек-лист по работе с сайтом

- **отсутствие политики** в отношении обработки ПДн, **или размещение некорректного документа**
- **отсутствие** на формах сбора ПДн **механизма получения согласия на обработку ПДн**
- **отсутствие информирования пользователей** о сборе метрических данных
- **распространение** ПДн в сети «Интернет» **без правовых оснований**
- трансграничная передача ПДн **(использование иностранных инструментов для сбора метрики, анкет, опросников и т.д.)**

КРИТИЧЕСКАЯ ИНФОРМАЦИОННАЯ ИНФРАСТРУКТУРА

Я – ОТВЕТСТВЕННЫЙ ПО ТЕМЕ КИИ

Мне нужно:

- ✓ Разбираться в требованиях и оперативно реагировать на изменения в них
- ✓ **Провести категорирование с учетом отраслевых особенностей**
- ✓ Разработать документы по защите ОКИИ
- ✓ **Проводить оценку Кзи *(раз в 6 месяцев)* и Узи *(раз в 3 года)***
- ✓ Планировать мероприятия обеспечению безопасности ОКИИ
- ✓ Взаимодействовать с ГосСОПКА
- ✓ Быть готовым к проверке регуляторов

- ✓ **Получать ответы на интересующие вопросы**

ФСТЭК

следующую информацию **строго по пунктам запроса:**

1) О системе безопасности значимых объектов КИИ, оператором которых является учреждение;

2) О принятых мерах по ограничению доступа третьих лиц к объектам КИИ, список сотрудников утверждения, имеющих доступ к объектам КИИ;

3) Приказ о создании постоянно действующей комиссии по категорирования объекта КИИ и документы о соответствии членов комиссии п. 11 Правил категорирования объектов КИИ РФ, утв. постановлением правительства РФ от 08.02.2018 № 127;

4) Перечень объектов КИИ, подлежащих катионированию, оператором которых является учреждение, акт категорирования на них;

5) Информацию о направлении учреждением в управление ФСТЭК России по ЦФО сведений о проведении объектам КИИ одной из категорий значимости;

6) Информацию о структурном подразделении учреждения ответственном за обеспечение безопасности значимых объектов КИИ, данные о сотрудниках, осуществляющих трудовую деятельность в указанном подразделении, их должностные инструкции - документы о соответствии работников структурного подразделения, ответственных за обеспечение безопасности значимых объектов КИИ, положениям п. 12 Требований к созданию системы безопасности значимых объектов КИИ, утв. Приказом ФСТЭК России от 21.12.2017 № 235;

7) Организационно-распорядительные документы, регулирующие порядок обеспечения подразделения, эксплуатирующего объекты КИИ безопасность значимых объектов, а также журналы ознакомления работников с указанными документами;

8) Документы о проведенных учреждением организационных мероприятиях, направленных на повышение уровня знаний работников, эксплуатирующих значимые объекты КИИ;

9) Схему сети (в части взаимодействия объектов КИИ с информационной инфраструктурой учреждения);

10 Информацию о созданных учреждением подсистемах безопасности объектов КИИ, а также документы по их создания (техническое задание, протоколы приемочных испытаний подсистем безопасности объектов КИИ и акты ввода в эксплуатацию);

10) Сведения и документы о средствах защиты информации, применяемых для обеспечения безопасности объектов КИИ, а также сертификаты соответствия, протоколы испытаний;

11) О принятых мерах по обеспечению безопасности объектов КИИ с использованием средств защиты информации, их параметры, характеристики, настройки, порядок их применения, в том числе в рамках планового и/или гарантийного обслуживания;

12) Организационно-распорядительные документы в сфере информационной безопасности, журналы ознакомления работников с ними;

13) План мероприятий по обеспечению безопасности объектов КИИ, результаты его реализации;

14) О проведенных учреждением мероприятиях по повышению защищенности информации инфраструктур от угроз безопасности информации, связанных с использованием электронной поты и иных ресурсов сети «Интернет».

Предлагаю обеспечить полноту и своевременность предоставления в прокуратуру запрашиваемых сведений и документов (их копий).

КОНТРОЛЬ КУРИРУЕМЫХ ОРГАНИЗАЦИЙ

Я – РУКОВОДИТЕЛЬ ОРГАНИЗАЦИИ/ЗАМЕСТИТЕЛЬ РУКОВОДИТЕЛЯ

Мне нужно:

- ✓ Знать, что происходит в курируемых организациях:
  - *кто ответственный?*
  - *в каком состоянии документы?*
  - *какие ОИ эксплуатируются?*
  - *что с СЗИ?*
- ✓ Помочь всем выполнить требования (в т.ч. разработать документы)
- ✓ **Оперативно** собирать информацию о состоянии ИБ в регионе/ ведомстве/ группе компаний:
  - *готовы ли к проверкам регуляторов?*
  - *какой уровень Кзи?*
- ✓ Раздавать поручения и контролировать их исполнение

альфа|док

SGRC-система, предназначенная для автоматизации и аналитической поддержки деятельности специалиста в области информационной безопасности

- Инвентаризация активов и документов, связанных с деятельностью по защите информации
- Определение классов защищенности ИС, уровней защищенности ИСПДн и категорирование объектов КИИ
- Разработка организационно-распорядительных и технических документов и поддержка их в актуальном состоянии
- Оценка показателей Кзи и Узи
- Взаимодействие с госрегуляторами
- Контроль курируемых организаций

п. 23 Требований, утвержденных 117 приказом



ON PREMISE

- Безопасность хранения информации
- Разработка документации по защите значимых объектов КИИ
- Интеграция с вашими системами
- Единая система для сети организаций

1 ЭТАП

АКТУАЛЬНАЯ ДОКУМЕНТАЦИЯ

АВТОМАТИЧЕСКОЕ ОБНОВЛЕНИЕ

СООТВЕТСТВИЕ ТРЕБОВАНИЯМ

Полный перечень организационно-распорядительных и технических документов, которые формируются в АльфаДок в зависимости от лицензии и приобретенных к ней модулей

ДОКУМЕНТАЦИЯ

- Политики и Положения
- Приказы о назначении ответственных
- Акты
- Модели угроз безопасности информации
- Технические паспорта и Технические задания
- Регламенты

2 ЭТАП

ОТЧЕТНОСТЬ ПО ФОРМАМ ФСТЭК

ВЗАИМОДЕЙСТВИЕ С РКН

КОНТРОЛЬ, ЗАДАЧИ, ПЛАНИРОВАНИЕ

ДЕЯТЕЛЬНОСТЬ

- Цикличное обновление Модели угроз
- Актуализация уведомления для РКН
- Формирование планов контроля
- Автоматизация разработки согласий
- Учет инцидентов
- Планирование мероприятий
- Контроль курируемых организаций
- Взаимодействие с экспертной поддержкой

ОПЕРАЦИОННЫЕ КЕЙСЫ

ПРИМЕР 1. УВОЛЬНЕНИЯ СОТРУДНИКОВ

Как специалист по защите информации,
я хочу заблаговременно узнавать об увольняющихся сотрудниках,
чтобы своевременно изымать закрепленные за ними материально-технические средства (МТС).

Клиент:

Крупная энерго- и теплоснабжающая компания

Действия:

1. Внедрена платформа АльфаДок
2. Настроена интеграция с 1С Предприятие 8.3
3. Организовано ведение карточек сотрудников в АльфаДок

Результат для клиента:

- ✓ Ежедневные оповещения о предстоящих кадровых изменениях
- ✓ 100% возврата выданных МТС

ПРИМЕР 2. ПИСЬМА ФСТЭК РОССИИ

Как руководитель отдела по защите информации,
я хочу своевременно и качественно отработать запрос ФСТЭК России и предоставить им ответ,
чтобы избежать включения в план проверок и получения предписаний.

Клиент:

Региональная газоснабжающая организация

Действия:

1. Внедрена платформа АльфаДок
2. Организована работа в модуле «Управление задачами»

Результат для клиента:

- ✓ Прозрачный процесс для руководителя
- ✓ Консолидация доказательной базы проделанной работы в одном месте
- ✓ 100% ответов готовятся в срок

В РАЗРАБОТКЕ

альфадок

МОДУЛЬ «ВЗАИМОДЕЙСТВИЕ С РЕГУЛЯТОРАМИ»

Автоматизация работы организации с входящими письмами и требованиями госрегуляторов в области информационной безопасности, в частности ФСТЭК России:

- регистрация и обработка запросов регуляторов;
- создание задач по требованиям;
- формирование отчёта для ответа регулятору;
- распространение запросов на курируемые организации;
- формирование регламента взаимодействия с регуляторами;
- формирование отчётной документации по выполненным задачам

ФОРМИРОВАНИЕ ПЛАНА-ОТЧЕТА ОБ ИСПОЛЬЗОВАНИИ ДОВЕРЕННЫХ ПАК

Автоматизация подготовки отчёта по переходу на доверенные ПАК:

- ведение учета ПАК, применяемых на значимых объектах КИИ;
- интеграция с реестрами Минцифры и Минпромторга;
- формирование и актуализация плана перехода на доверенные ПАК;
- подготовка отчётности по форме, установленной ППП№ 1912



ПОДДЕРЖКА ПОЛЬЗОВАТЕЛЕЙ

- ✓ консультации по функциональным возможностям
- ✓ консультации по требованиям НПА
- ✓ консультации в рамках взаимодействия:
  - с Роскомнадзором
  - с органами прокуратуры
  - с ФСБ России
  - с ФСТЭК России

При приобретении соответствующего пакета поддержки

ИНТЕГРАЦИИ

ГОТОВЫЕ РЕШЕНИЯ

Кадровые системы

- ✓ 1С Предприятие 8.3. ЗУП
- ✓ Bitrix24

Системы сетевой инвентаризации

- ✓ Kaspersky Security Center (KSC)
- ✓ АРМ Сканер
- ✓ MaxPatrol SIEM

Системы авторизации

- ✓ Active Directory
- ✓ Альфа-ID*
  (**сертифицированное решение*)

1С

По организации	По подразделению	По должностям	По сотрудникам
Наименование	Является филиалом организации	Полное наименование	ФИО полностью
Краткое наименование	Полное наименование	Наименование	Должность
Полное наименование	Наименование	Дата создания	Должность (в документах)
ИНН	КПП	Дата расформирования	СНИЛС
КПП	Дата создания		Табельный номер
ОГРН	Дата расформирования		Email
Тип			Домашний телефон
Юридический адрес			Телефон
Фактический адрес			Рабочий телефон
Почтовый адрес			Дополнительная контактная информация
Email			
Контактный телефон			

ТЕХНИЧЕСКАЯ ИНВЕНТАРИЗАЦИЯ

Наименование	АРМ-Сканер	MaxPatrol SIEM	Kaspersky Security Center
Сетевое имя	+	+	+
Домен	+	+	+
IP адрес	+	+	+
MAC адрес	+	+	+
Процессор	+	+	+
Материнская плата	+	+	+
Системная память	+	+	+
Видеоадаптер	+		
Дисковые устройства	+		
Приводы CD/DVD	+		
Монитор	+		
Клавиатура	+		
Мышь	+		
Наименование ОС	+	+	
Версия ОС	+	+	
Микропрограммное обеспечение	+		
Версия микропрограммного обеспечения	+		

«АЛЬФА»: РЕГУЛЯРНЫЕ ПРОЦЕССЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

АльфаИнциденты

Единый центр обработки событий ИБ:

- инцидент-менеджмент и оповещение о событиях
- пошаговые сценарии реагирования на типовые инциденты кибербезопасности
- автоматизированное реагирование на инциденты с помощью агентов
- интеграция с ГосСОПКА
- интеграция с SIEM-системами

АльфаИнтенсив

Решение для повышения уровня киберграмотности сотрудников организации и подготовки кадров в области информационной безопасности:

- собственная образовательная платформа
- готовые курсы по защите информации
- платформа для имитации фишинговых атак

АльфаКрипто

Приложение, которое помогает вести учет СКЗИ, отслеживать их жизненный цикл, оформлять все необходимые документы и организовывать процесс выдачи криптосредств:

- для пользователей криптосредств
- для органов криптозащиты

АльфаКоннект

Система, которая организует процесс подачи и обработки заявок на доступ к информационным системам, контролирует выполнение требований безопасности и ведет учет всех подключенных пользователей и организаций:

- заключение соглашений
- прием и регистрация заявок
- техническая проверка соответствия требованиям
- контроль сроков действия СрЗИ

Комплексные проекты по организации и управлению ИБ:

в 28 регионах

На базе региональных Минцифр

в 16 регионах

На базе региональных МИАЦ

B2B-организации из сфер:

57
организаций
Промышленное производство

41
организация
Энергетика

32
организации
ИТ

30
организаций
Транспорт

25
организаций
Водоснабжение

24
организации
Коммерческая медицина

19
организаций
Наука

16
организаций
Добыча полезных ископаемых

ОСТАЛИСЬ ВОПРОСЫ?

info@npc-ksb.ru

8 800 500 52 33

ПРОТЕСТИРУЙТЕ БЕСПЛАТНО

НА ALFA-DOC.RU

ЗАКАЖИТЕ ПИЛОТНЫЙ ПРОЕКТ

НА ВАШИХ МОЩНОСТЯХ

Наш канал в MAX

- Экспертные материалы
- Разборы законодательства
- Новостные дайджесты
- Обзоры обновлений
- Развлекательный контент