От новаций в утечке до официальной легализации мониторинга

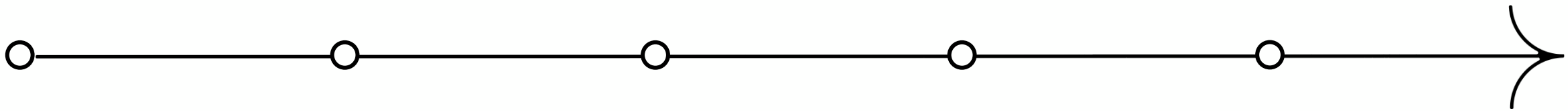
Анализ изменений в 2025-2026
и как адаптироваться

Ольга Попова

Главный юрист продуктовой группы Контур.
Эгида, эксперт по правовым вопросам
информационной безопасности

Контур Эгида × Контур staffcop

Таймлайн НПА в ИБ и КИ



1996-1997

– Введение УК РФ (незаконная деятельность в области защиты компьют. инф.

– Указ Президента 188 (Перечень КИ)

2004-2007

– 98-ФЗ о КТ

– 152-ФЗ о ПДН

– 149- ФЗ об информации

– Указ 646 –создание доктрины об ИБ страны

2007-2016

– Формирование и введение основных требований к защите ПДн

– 436- ФЗ о защите детей

– Указ 250 подключение компьют. сети к органам власти

2017-2018

– 187-ФЗ о безопасности КИИ

– УК РФ о неправомерном воздействии на КИИ

– Создание НКЦКИ

– Порядок представления информации в ГосСОПКА

2019-2024

– Ограничение
– Запрет
– Усиление
– Ужесточение
– Совершенствование

Основные направления

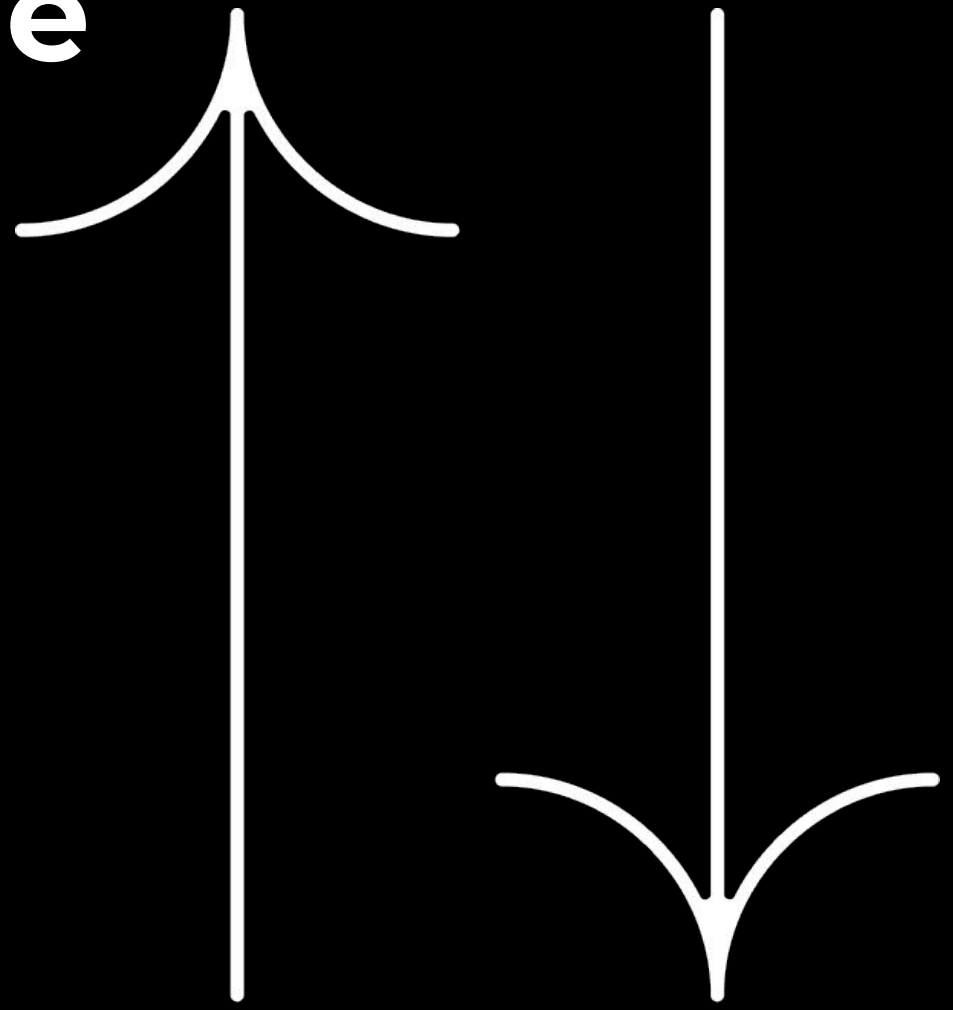
1 ПО, КИИ

2 Документы

3 ПДН, КИ

4 Регуляторы

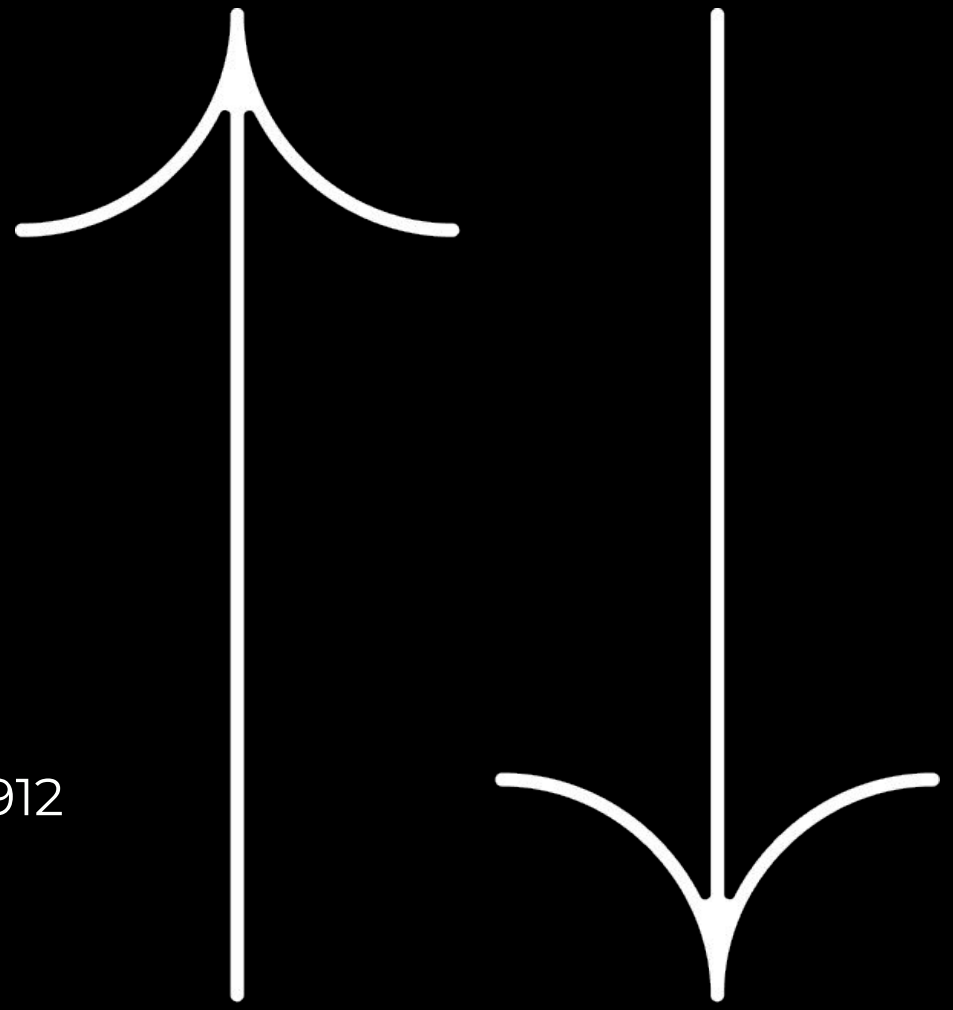
Ограничение на импортозамещение



Указ Президента РФ от 30.03.2022 N 166
(ред. от 07.04.2025) "О мерах по обеспечению технологической независимости и безопасности критической информационной инфраструктуры РФ"

с 31.03.2022 – согласование закупки
с 01.01.2025 – полный запрет закупки ИПО

Акцент по переходу на РПО



Постановление Правительства РФ от 14.11.2023 N 1912
с 01.01.2026 – ежегодный отчет о переходе
на российское ПО на КИИ до 01.03.

75%

вина сотрудников

Ужесточение (УК РФ 421 ФЗ с 12.24)

ст. 272.1. Незаконные использование и (или) передача, сбор и (или) хранение компьютерной информации, содержащей ПДН, создание и (или) обеспечение функционирования информационных ресурсов, предназначенных для незаконного хранения и (или) распространения.
Штраф до 1 млн.р и срок лишения свободы до 10 лет.

1 Трансграничное перемещение КИ с ПДН (флешка, ноутбук)

2 Исключение ответственности, если виновник докажет, что данные использовались в личных целях (например, список д.р. родственников, размещенных на диске Яндекс)

3 Конкретизация действий с ПДН (Получено незаконным путем, без согласия, данные несовершеннолетних)

4 Отягчающие обстоятельства для CISO (специалист по ИБ несет повышенную ответственность)

Предложения 2025 по изменениям в УК РФ по ИИ

1 ИИ как отягчающие обстоятельство (изменения в ст. 63 УК РФ).

2 Незаконная передача с ИИ - ужесточение наказания до 4 лет, штраф до 500 тыс.р. штрафа. Если ДЛ до 8 лет, и до 2 млн штрафа (ст.272.1.УК РФ новая).

3 2х кратное увеличение штрафа по ст. 272, 273 и 274 УК РФ – неправомерный доступ к компьютерной информации.

4 массовые атаки, угрозы с вымогательством с ИИ - срок до 4 лет и штраф до 500 тыс.р. Группа лиц - до 7 лет и 1 млн р. штрафа.

(изменение в ст. 163.1)

Усиление ответственности (ПДН)

420- ФЗ с 30.05.2025. Уточнение составов правонарушений и увеличение штрафа по КоАП РФ (ст.13.11)).

Для ИП – штрафы по 3 категориям, два уведомления, обязательное уведомление до начала обработки

Было:

ЮЛ – от 60 до 100 т.р.
(Нарушение цели и объема обработки ПДн)

ЮЛ – от 60 до 100 т.р.
(повторно)

ЮЛ – **5 т.р.**
(не уведомление РКН об утечке ПДн)

Стало:

ЮЛ – от 100 до 300 т.р.
ФЛ – от 5 до 10 т.р., ДЛ **(ИП как ДИ) –** от 50 до 100 т.р.

ЮЛ **(ИП как ЮЛ) –** от 300 до 500 т.р.
ФЛ – от 15 до 30 т.р., ДЛ – от 100 до 200 т.р.

ЮЛ **(ИП как ЮЛ) –** от 1 до 3 млн. р
ФЛ – от 50 до 100 т.р., ДЛ – от 400 до 800 т.р.

Уточнение к локализации (ПДН)

с 01.07.2025 изменения в ч. 5 ст. 18 152 ФЗ.

Было:

При сборе ПДн, в т.ч. посредством информационно-телекоммуникационной сети "Интернет", оператор обязан обеспечить запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение ПДн граждан РФ с использованием БД на территории РФ, за искл. п. 2, 3, 4, 8 ч. 1 ст.6.

Стало:

При сборе ПДн, в т.ч. посредством информационно-телекоммуникационной сети "Интернет", запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение ПДн граждан РФ с использованием БД, находящихся за пределами территории РФ, не допускаются, за искл. п. 2, 3, 4, 8 ч. 1 ст.6.

Ужесточение к обработке

Изменения по ПДН с 01.09.2025

Согласие на обработку ПДн как отдельный документ (ст.6 152 ФЗ).

Нельзя включать в текст договора или иного документа на согласие.

Обязательные сведения в тексте формы Согласия:
– наименование оператора ;

– цель обработки персональных данных;

– перечень обрабатываемых данных и перечень действий с ними;

– способы обработки данных;

– срок действия согласия;

– подпись субъекта персональных данных.

Обезличивание ПДн

С 01.09.2025 (порядок, требования, методики)
методы- замена, изменение состава, смешивание или декомпозиция

Критерии

- ситуация
- деобезличивание
- цель
- особые требования

ПП 1154

- по требованию Минцифры
- невозможно
- для госнужд
- согласование с ФСБ, банком России для банков

Приказ 140

- для собственных нужд Оператора
- возможно
- для статистики добровольно
- общие для добровольного обезличивания

Рекомендуемые шаги по обезличиванию

- Политика по обезличиванию ПДн
- Определение объема ПДн для обезличивания
- Выбор метода обезличивание
- Способ хранения и защита
- внести изменения в общую политику с указанием анонимизации
- определить ответственных лиц
- раздельное хранение

Причины инцидентов утечки информации

53%

Программы – вымогатели и компрометация корпоративной почты

44%

Социальная инженерия и фишинг

12%

Облачные сервисы с плохой защитой

Изменения НПА в отношении СЗИ

1 ГОСТ Р 56939-2024 «Защита информации. Разработка безопасного ПО. Общие требования»

2 приказ ФСТЭК России № 230 «О внесении изменений в Порядок проведения сертификации процессов безопасной разработки средств защиты информации, действ. с июня 2025

3 ужесточение ответственности за несертифицированное СЗИ (ст.13.12. КОАП РФ), действ. с мая 2025

4 методика ФСТЭК России испытаний систем защиты информации ИС методами тестирования на проникновение, действ. с сентября 2025

2026. Новое в уголовной ответственности по КИИ

Законопроект № 1071997-8 (КОАП)
Ст. 13.2.2 «Нарушение правил эксплуатации объектов КИИ РФ».
нарушения по эксплуатации КИИ в отсутствии признаков преступления
Штраф 100-500 т.р. (ЮЛ) и 10-50 т.р. (ДЛ).

Законопроект № 1071966-8 (УК)
За неправомерное воздействие на КИИ РФ.
Ст. 274.1 УК РФ - освобождении от ответственности при участии в раскрытии, впервые. сохраняли следы преступления.

Новое в законопроекте
Понятие вреда
Освобождение
от ответственности
при содействии

Новое в законопроекте
Нет инцидента -есть ответственность

Рекомендации:
Всем КИИ необходимо провести аудит уязвимостей, включить в планы ИБ модернизацию или ввод в эксплуатацию ИБ-средств, выделить требуемые для этого ресурсы и отработать сценарии реагирования на инциденты.

Рекомендуемые шаги

- Централизованное зашифрованное хранение КИ
- Полноценное управление Доступом
- Журналирование всех операций по передаче КИ
- Ответственные за корпоративные секреты, «золотые списки»
- MFA для всех
- VPN для всех
- Регулярная чистка
- Регулярность обновлений ПО

2026 новое с ИС

ГИС Антифрод

- Сбор и обмен данными о кибермошеннических действиях;
- Выявление и учёт фишинговых сайтов и ресурсов
  Оперативное реагирование, уведомление всех участников
  создание баз подозрительных лиц.

Приказ 117

- Расширение области применения;
- Новые классы требования защиты к ИТ системе;
- Требования к подрядчикам;
- Периодичность контроля
- Выбор класса

НКЦИ

Расширение полномочий НКЦКИ:

- Сроки для значимых КИИ – 3 ч, остальные 24ч;
- Информирование о результатах 48 ч
  План реагирования 90 д с даты внесения в реестр значимых
- Субъекты КИИ обязаны реагировать о сообщениях НКЦИ о возможных атаках - 24 ч

2026 новое в 149 ФЗ

Изменения с 01.01.2026 в ст. 10.1. ч.1 : Организатор распространения информации в сети "Интернет" обязан хранить на территории Российской Федерации:

Было:

информацию о фактах приема, передачи, доставки и (или) обработки голосовой информации, письменного текста, изображений, звуков, видео- или иных электронных сообщений пользователей сети "Интернет" и информацию об этих пользователях в течение 1 ГОДА с момента окончания осуществления таких действий

Стало:

информацию о фактах приема, передачи, доставки и (или) обработки голосовой информации, письменного текста, изображений, звуков, видео- или иных электронных сообщений пользователей сети "Интернет" и информацию об этих пользователях в течение 3 ЛЕТ с момента окончания осуществления таких действий

2026 новое в 149 ФЗ

Изменения с 01.03.2026 добавить п.4.5.

Организатор сервиса обмена мгновенными сообщениями, являющийся российским ЮЛ или ФЛ РФ, обязан осуществлять взаимодействие с ГИС противодействия правонарушениям, совершаемым с использованием информационных и коммуникационных технологий, в случаях и порядке, которые устанавливаются Правительством РФ.

Цель:

требование направлено на усиление контроля за использованием мессенджеров в противоправных целях и повышение эффективности противодействия таким правонарушениям. Конкретные механизмы взаимодействия будут детализированы в нормативных актах, которые примет Правительство РФ.

2026 новое в 149 ФЗ

Изменения с 01.03.2026 добавить п.4.1. В СТ. 10.2-1. Особенности регулирования деятельности провайдера хостинга

Провайдер хостинга обязан осуществлять взаимодействие с государственной информационной системой противодействия правонарушениям, совершаемым с использованием информационных и коммуникационных технологий, в случаях и порядке, которые устанавливаются Правительством РФ.

Цель:

часть комплексной стратегии по усилению государственного контроля в сфере информационных технологий и повышению уровня кибербезопасности в России.

2026 новое в 149 ФЗ

Изменения с 01.03.2026 в ст.12.1. Особенности государственного регулирования в сфере использования российских программ для электронных вычислительных машин и баз данных

1.Правительство РФ по представлению Минцифры России определяет некоммерческую организацию, которая будет осуществлять функции оператора реестра российского программного обеспечения
2.Федеральный орган исполнительной власти утверждает классификатор программ РПО
3.Правообладатель РПО считается контролируемым российскими лицами, если они прямо или косвенно распоряжаются более чем 50% голосов на общем собрании организации-правообладателя.
4.Исключена доля участие иностранной организации.

Цель:

совершенствование механизмов регулирования ИТ-отрасли, повышение прозрачности и контроля за происхождением ПО, а также поддержка импортозамещения.
Новый подход позволит точнее выявлять лиц, способных влиять на правообладателя ПО, и учитывать сложные корпоративные структуры.

2026 новое в КоАП РФ

Изменения с 01.03.2026, новая ст.13.54.

Осуществление деятельности по предоставлению вычислительной мощности для размещения информации в информационной системе, постоянно подключенной к информационно-телекоммуникационной сети "Интернет", провайдером хостинга, сведения о котором не включены в реестр провайдеров хостинга

– штрафа на граждан от 50 т.р. до 100 т.р.

– ДЛ - от 200 до 500 т.р.

– ЮЛ - от 600 до 1000 т.р. и т.д.

Цель:

создание более строгого правового поля для регулирования хостинговой деятельности, обеспечение контроля за использованием вычислительной мощности и защиту интересов государства в сфере информационной безопасности.

Ст. 23 Конституции РФ

Нарушение личных границ

Ст. 137 УК РФ

Ответственность

Любая компания это

1 **Работодатель**

ст. 15, 22,56 ТК РФ

2 **Собственник**

ч.2 ст.209 ГК РФ

3 **Обладатель информации**

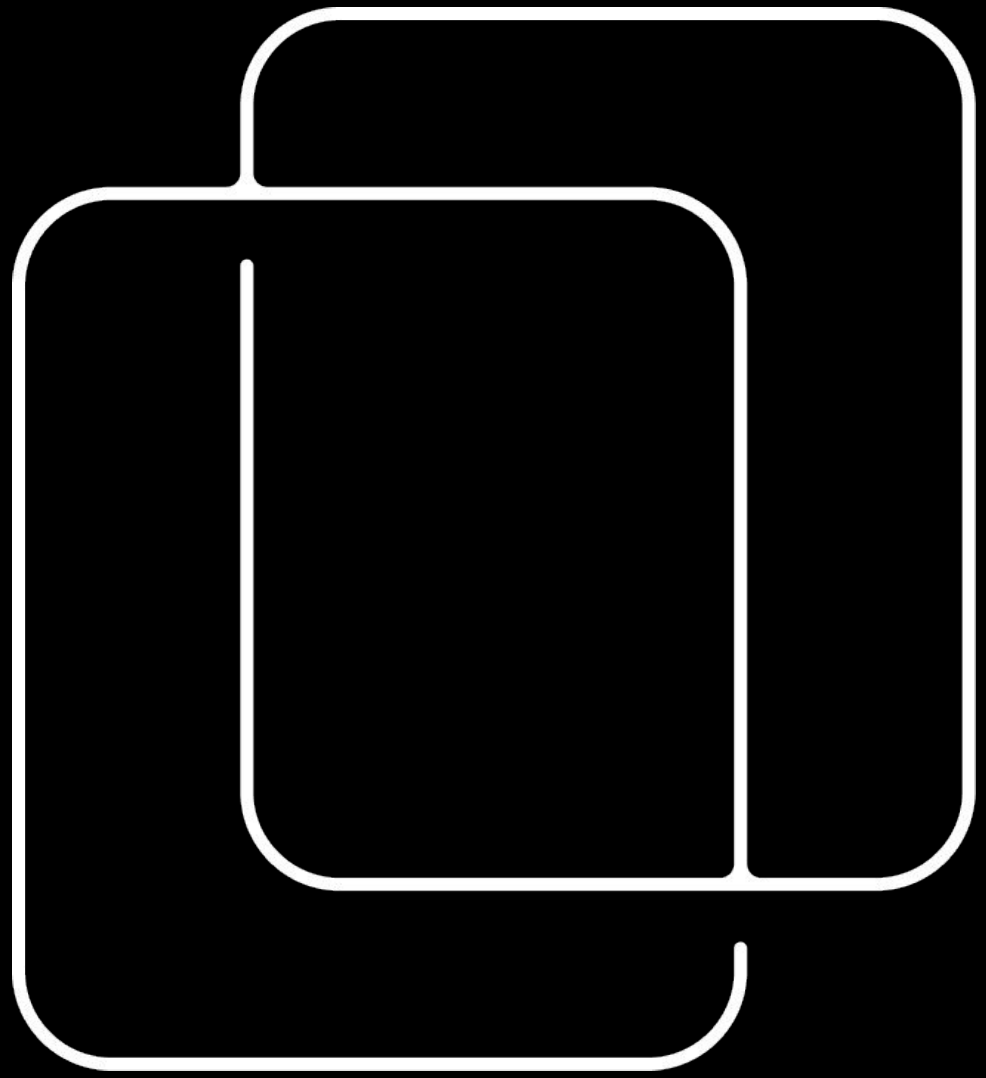
п.4 ст. 3 , ст.6.1. 98-ФЗ

4 **Оператор ПДн**

ст. 3, ст.19 152 - ФЗ

Проект национального стандарта (ГОСТ ФСТЭК России)

«Защита информации. Защита информации от неправомерной передачи или распространения из информационных и автоматизированных систем. Общие положения»



Конкретизация понятий

Утечка заменена на неправомерную передачу и распространение.

Легализация мониторинга

В целях защиты КИ применяется мониторинг , о чем уведомляется при приеме на работу или в процессе ввода в эксплуатацию новой информационной (автоматизированной) системы.

Конкретизация функций ответственных лиц

- ИТ-служба внедряет СЗИ и корректирует работу ИТ систему в случае инцидентов
- ИБ-специалисты отвечают за ЛНА об обращении с защищаемой информацией и вводе ПО по ее защите в эксплуатацию, анализирует информационные ресурсы в поисках КИ, потенциальных угроз ее безопасности и каналов ее утечки, настраивает политики ИБ, выявляет и реагирует на инциденты ИБ
- HR и ЮРО помогают ИБ в разработке ЛНА уведомляют сотрудников о мерах ответственности за нарушения правил работы с КИ, сообщают регуляторам об инцидентах и результатах расследования.

От приема до архива: алгоритм работы с бумагой

- Беспризорный документ
- Шредер «ваше» все
- Регламент для «посыльных»
- Помни о журнале
- Выделенная территория

Контур.Эгида × Staffcop

- Экспертность в организации ИБ в компаниях любого размера и профиля
- Простое внедрение и использование, удобный и понятный интерфейс
- Интеграции с продуктами Контура и другими IT-решениями
- Прозрачные ценообразование и стоимость владения

Как продукты Контура решают проблемы в сфере ИБ

Контур.Эгида

- Безопасность корпоративных учетных записей сотрудников
- Контроль привилегированных пользователей
- Безопасное удаленное подключение
- Аудит и организация комплексных мер защиты ИБ

Staffcop

- Расследование инцидентов
- Контроль и анализ действий персонала
- Учет рабочего времени
- Выявление утечек и мошеннических действий
- Предотвращение неправомерных действий

Как продукты Контура решают проблемы в сфере ИБ

ID

Сервис двухфакторной аутентификации

PAM

Система контроляпривилегированных пользователей

Безопасность

Услуги информационной безопасности

Коннект

Защищенный доступ к корпоративной сети

Контур staffcop

Расследование инцидентов внутренней ИБ

Контур.Эгида × Staffcop — это комплексный подход к формированию культуры информационной безопасности в компании

Мы изучим ваши потребности и поможем найти подходящее решение для ваших задач

Мы вас не контролируем, а защищаем

staffcop.ru

kontur.ru/aegis

Ольга Попова

Главный юрист продуктовой группы Контур.
Эгида, эксперт по правовым вопросам
информационной безопасности

Контур Эгида × Контур staffcop