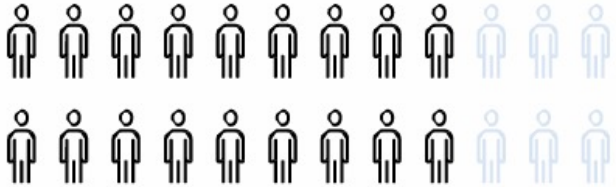
OVODOV
CyberSecurity

Особенности обеспечения информационной безопасности на промышленных предприятиях

Работаем с 2011 года

75% клиентов с нами более 5 лет

Потому что Ovodov Cyber Security настроены на интересы заказчика и объясняет сложное на доступном языке.

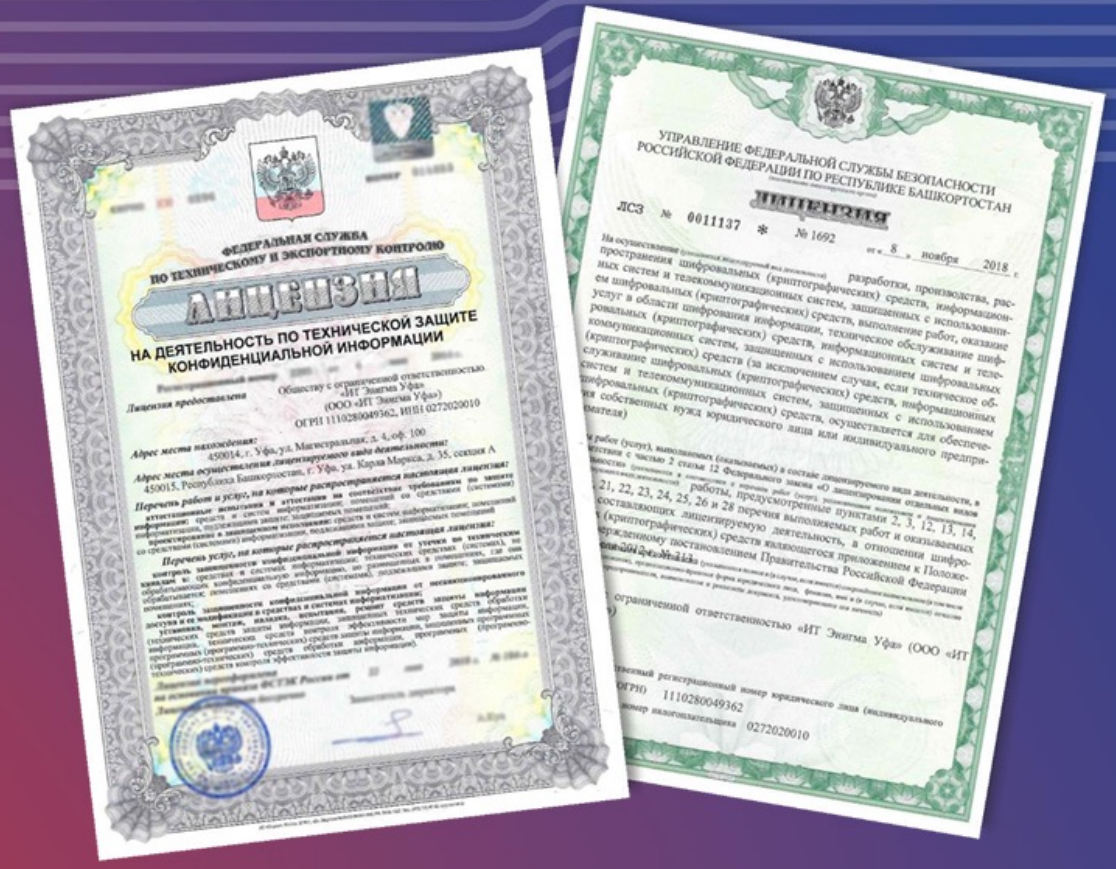


Защита информации на межрегиональном уровне

38 регионов присутствия

OVODOV CyberSecurity

Лицензии ФСБ и ФСТЭК



OVODOV
CyberSecurity

Сертификаты соответствия

СИСТЕМА ДОБРОВОЛЬНОЙ СЕРТИФИКАЦИИ СИСТЕМ МЕНЕДЖМЕНТА
«ФедРегистр»
РОСС RU.31184.04KHC5

Орган по сертификации
ООО «Федеральный Регистр»
(ОГРН 1147847035885)
191186, г. Санкт-Петербург, наб. канала Грибоедова, д. 5, лит. Е, пом. 23-Н, оф. 515, 516
Тел. (812) 913-01-92, FedRegister@com-1.ru

СВИДЕТЕЛЬСТВО № 1-804/22

ПОДТВЕРЖДЕНИЯ ДЕЙСТВИЯ СЕРТИФИКАТА СООТВЕТСТВИЯ
СИСТЕМЫ МЕНЕДЖМЕНТА

Орган по сертификации систем менеджмента ООО «Федеральный Регистр»
по результатам первого инспекционного контроля системы менеджмента
информационной безопасности

принял решение подтвердить действие сертификата соответствия сис
менеджмента № СДС.ФР.СМ.00804.22 от 28.01.2022г.
Общества с ограниченной ответственностью
«ИТ Эниgма Уфа»
на соответствие требованиям
ISO/IEC 27001:2013
при выполнении работ согласно Приложению № 1
к Сертификату № СДС.ФР.СМ.00804.22

Дата выдачи 12/12/2022г.

Руководитель органа по сертификации

СИСТЕМА ДОБРОВОЛЬНОЙ СЕРТИФИКАЦИИ СИСТЕМ МЕНЕДЖМЕНТА
«ФедРегистр»
РОСС RU.31184.04KHC5

Орган по сертификации
ООО «Федеральный Регистр»
(ОГРН 1147847035885)
191186, г. Санкт-Петербург, наб. канала Грибоедова, д. 5, лит. Е, пом. 23-Н, оф. 515, 516
Тел. (812) 913-01-92, FedRegister@com-1.ru

СВИДЕТЕЛЬСТВО № 1-803/22

ПОДТВЕРЖДЕНИЯ ДЕЙСТВИЯ СЕРТИФИКАТА СООТВЕТСТВИЯ
СИСТЕМЫ МЕНЕДЖМЕНТА

Орган по сертификации систем менеджмента ООО «Федеральный Регистр»
по результатам первого инспекционного контроля системы менеджмента качества

принял решение подтвердить действие сертификата соответствия системы
менеджмента № СДС.ФР.СМ.00803.22 от 28.01.2022г.
Общества с ограниченной ответственностью
«ИТ Эниgма Уфа»
на соответствие требованиям
ГОСТ Р ИСО 9001-2015 (ISO 9001:2015)
при выполнении работ согласно Приложению № 1
к Сертификату № СДС.ФР.СМ.00803.22

Дата выдачи 12/12/2022г.

Руководитель органа по сертификации /Рыбалкин С.С./
фамилия, инициалы

Соответствуем требованиям

ISO/IEC 27001:2013
ISO 9001:2015

OVODOV
CyberSecurity

Цифры говорят сами

40+

специалистов
в штате

100%

проверок пройдено
с нашей помощью

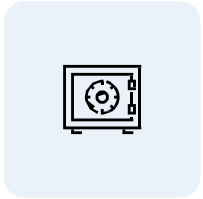
3000+

реализованных проектов
информационной
безопасности

OVODOV
CyberSecurity

Берем ответственность на себя

С OVODOV Cyber Security рабочие процессы и репутация компании надежно защищены, потому что охраняются на условиях договора.



Финансовые гарантии, компен-сация штрафов

Сопровождение на проверках, подключаемся при атаках

Решение ВСЕХ вопросов кибербезопасности

Персональный менеджер

OVODOV CyberSecurity

Направления информационной безопасности

Выполнение требований законодательства

- Государственные информационные системы (149-ФЗ)
- Критическая информационная инфраструктура (187-ФЗ)
- Персональные данные (152-ФЗ)
- Финансовый сектор (Требования Банка России)
- Автоматизированные системы управления (АСУ)

Защита от угроз безопасности информации

- Защита от компьютерных атак
- Выявление и предотвращение утечек информации
- Расследование компьютерных инцидентов
- Построение и эксплуатация систем управления и обеспечения информационной безопасности с учетом актуальных рисков

OVODOV CyberSecurity

Особенности промышленных компаний

- Основной бизнес-процесс - производство продукции имеет собственные системы автоматизации, не управляемые ИТ.
- 2 глобальных контура - корпоративный и производственный
- Системы электроснабжения, газоснабжения, вентиляции, кондиционирования, дымоудаления, контроля состояния окружающей среды влияют на возможность производить продукцию зачастую большую чем АСУ обеспечивающее сам процесс производства
- Четвертая промышленная революция - все системы онлайн и взаимодействуют со всем (подрядчики – компания – партнеры – заказчики)

Стоп-факторы построения СОИБ в промышленности

Организационные

Кто главный за информационную безопасность на производстве: директор по безопасности или директор по производству?

Кто отвечает за ИТ системы (MES, ТОИР и т.п.) на производстве: директор по ИТ или директор по производству?

Какую роль занимает подразделение АСУ? ИТ под АСУ, АСУ по ИТ, ИТ и АСУ это одно, АСУ под директором по производству

Кто определяет недопустимые события, оценивает риски и угрозы в целом и в части ИБ в частности для производственных и поддерживающих систем?

Кто пишет документы на СОИБ производственного контура и контролирует их соблюдение?

Стоп-факторы построения СОИБ в промышленности

Технические

- Много отдельных изолированных контуров:
  - проблемы с администрирование СрЗИ, анализом уязвимостей, ежедневным обновлением баз данных антивируса, отсутствие реагирования на признаки компьютерных атак и инциденты ИБ;
- Реализация только превентивных мер в промышленных системах (отсутствие мониторинга);
- Взаимодействие корпоративной сети с сегментами промышленной сети через ODBC сервера с двумя сетевыми картами

Решение через призму защиты бизнеса от потерь

I. Повышение значимости обеспечения ИБ

1) Определение недопустимых событий и событий несущих существенные потери для бизнеса, а также их реальной стоимости;

2) Оценка рисков реализации недопустимых событий.

Результаты:

- недопустимые события и риски определены и финансово оценены;
- предложены верхнеуровневые шаги по нейтрализации недопустимых событий и минимизации рисков;
- руководством компании верифицированы недопустимые события и риски и следующий шаг.

Решение через призму защиты бизнеса от потерь

II. Разработка мероприятий по минимизации рисков ИБ

1) Инвентаризация активов
2) Определение нарушителей
3) Реализация векторов атак по матрице MITRE/методике моделирования угроз ФСТЭК с оценкой времени их реализации нарушителями
4) Разработка комплекса мер необходимых мер для затруднения продвижения нарушителя к критичным активам и его своевременного обнаружения

Результат:

- Разработан и согласован с руководством план мероприятий по построению СОИБ на 3-5 лет по нейтрализации недопустимых событий и минимизации рисков до согласованного уровня

Основа для выработки мер

1) Результаты тестирований на проникновение, аудита процессов обеспечения ИБ и применяемых политик ИБ
2) Методологии разработанные Positive Technologies и соединенные с собственными наработками по результатам практического применения;
3) Нормативные акты и методические документы ФСТЭК и ФСБ по ЗОКИИ, ИСПДн и других видах защищаемых объектов
4) Матрицы MITRE Attack, Defense
5) CIS Controls, ISO/IEC 27000 СМИБ
6) CIS Benchmarks и другие
7) Пирамида зрелости ИБ

Стратегическое партнерство

uniteller

OVODOV CyberSecurity

Анлим

- Совокупная выручка – более 1,5 млрд рублей
- Прямой диалог с Минцифрой РФ, ФСТЭК и ФСБ
- Главные инженеры проектов - 2
- Руководители проектов - 3
- Пентестеры - 4
- Аналитики - 5
- Проектировщики - 3
- Инженеры – 12
- Сертифицированы по 1 и 2 линиям технической поддержки по СрЗИ, в т.ч. РТ

Присоединяйтесь повышать культуру информационной безопасности