РУБИКОН

Комплексные решения информационной безопасности

НАША РАБОТА — ВАША УВЕРЕННОСТЬ

WWW.RCNGROUP.RU

АУДИТ информационной безопасности

сформируем оптимальную и эффективную стратегию развития информационной безопасности компании

ПРИВЕДЕНИЕ В СООТВЕТСТВИЕ ТРЕБОВАНИЯМ РЕГУЛЯТОРОВ

187-ФЗ
Критическая информационная инфраструктура (КИИ)
152-ФЗ
Персональные данные (ПДн)
98-ФЗ
Коммерческая тайна (КТ)
Приказ ФСТЭК № 17
Подключение к государственным информационным системам (ГИС)

АНАЛИЗ УЯЗВИМОСТЕЙ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ

Положение Банка России № 757-П
анализ уязвимостей программного обеспечения и тестирование его на проникновение обязательны для кредитных организаций с 2021 года

ТЕСТИРОВАНИЕ НА ПРОНИКНОВЕНИЕ

Проведем тестирование

- внутренней сети и внешнего периметра на наличие уязвимостей
- приложений и сайтов на наличие уязвимостей
- сотрудников на устойчивость к социальной инженерии
- систем на устойчивость к DoS-атакам

ЗАЩИТА СИСТЕМ ОТ УТЕЧЕК ИНФОРМАЦИИ

Выполним

- блокирование утечек информации
- контроль коммуникаций сотрудников
- выявление признаков корпоративного мошенничества
- оценку рисков информационной безопасности
- расследование инцидентов информационной безопасности

187-ФЗ КИИ

критическая информационная инфраструктура

Каких сфер касается?

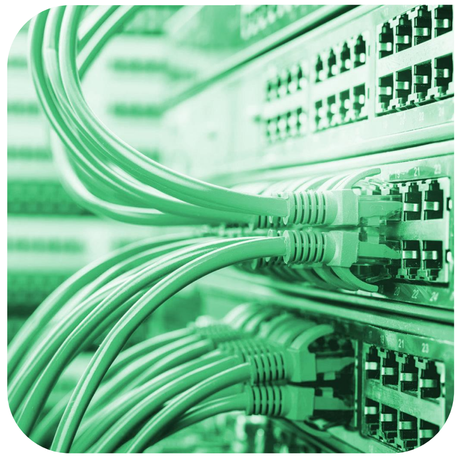
субъекты КИИ

- Здравоохранение
- Наука
- Транспорт
- Связь
- Энергетика
- Финансы
- ЮЛ и ИП, которые обеспечивают взаимодействие указанных систем и сетей
- Ракетно-космическая промышленность
- Горнодобывающая промышленность
- Металлургическая промышленность
- Химическая промышленность
- Топливно-энергетический комплекс
- Оборонная промышленность
- Область атомной энергии

Что нужно защищать?

объекты КИИ

Информационные системы



Информационно-телекоммуникационные сети

Автоматизированные системы управления технологическими процессами (АСУ ТП)

А если ничего не делать?

до 10 лет

лишения свободы

Невыполнение требований по безопасности, в случае наступления инцидента с тяжкими последствиями или их угрозой

до 6 лет

лишения свободы

Невыполнение требований по безопасности, нарушение правил эксплуатации

до 20 т.р.

штраф по КоАП

Невыполнение предписания регулятора об устранении нарушения законодательства

WWW.RCNGROUP.RU

187-ФЗ КИИ

критическая информационная инфраструктура

Что нужно сделать?

Чтобы выполнить требования 187-ФЗ, необходимо

- сформировать перечень объектов КИИ и провести их категорирование
- предоставить сведения об объектах КИИ в центральный аппарат ФСТЭК России
- реализовать организационные и технические меры по обеспечению безопасности объектов КИИ
- обеспечить подключение субъекта КИИ в ГосСОПКА

Что возьмем на себя?

1

ОПРЕДЕЛЕНИЕ ОБЪЕКТОВ КИИ

Обследуем объекты компании, выявим среди них потенциально значимые объекты КИИ

2

СОСТАВЛЕНИЕ МОДЕЛИ НАРУШИТЕЛЯ

Составим модели потенциального нарушителя безопасности КИИ и предскажем его возможности

3

ОПРЕДЕЛЕНИЕ КАНАЛОВ УТЕЧКИ

Определим каналы утечки конфиденциальной информации

4

ФОРМИРОВАНИЕ ПЛАНА РАБОТ

Сформируем плана работ по достижению соответствия требованиям 187-ФЗ

5

ВНЕДРЕНИЕ СИСТЕМЫ ЗАЩИТЫ

Подберём и поставим СЗИ для объектов КИИ в соответствии с нормативными требованиями

6

ПОДДЕРЖКА И СОПРОВОЖДЕНИЕ ПОСЛЕ ВНЕДРЕНИЯ

Окажем поддержу и помощь в развитии системы защиты КИИ на каждом из этапов внедрения

187-ФЗ КИИ

критическая информационная инфраструктура

Министерство здравоохранения Российской Федерации

Медицинская промышленность

- Фармацевтическая промышленность

Медицинские услуги

- Федеральные учреждения здравоохранения
- Государственные учреждения здравоохранения
- Муниципальные учреждения здравоохранения
- Частные учреждения здравоохранения

Система медицинского страхования

- Обязательное медицинское страхование
- Добровольное медицинское страхование

152-ФЗ ПДн

защита персональных данных

Каких сфер касается?

операторы персональных данных

Оператор персональных данных
любая организация или физическое лицо, организующие и (или) осуществляющие обработку персональных данных.

Персональные данные
любая информация, относящаяся к определенному или определяемому на основании такой информации физическому лицу, в том числе:

- ФИО
- дата рождения
- адрес
- семейное положение
- имущество
- образование
- место работы
- доходы и т.д.

Что нужно защищать?

места хранения персональных данных

в электронном виде

- Документы на компьютерах и серверах
- Документы в облачных хранилищах
- Система контроля доступом на проходной
- Учетные программы 1С
- Сайт компании, CRM и ERP-системы

в бумажном виде

- Отдел кадров
- Бухгалтерия
- Отдел продаж
- Служба безопасности
- Архив

это могут быть данные сотрудников, клиентов и посетителей

А если ничего не делать?

до 4 лет

лишения свободы

Незаконное собирание или распространение сведений о частной жизни лица без его согласия

до 300 т.р

штраф по УК

Незаконное собирание или распространение сведений о частной жизни лица без его согласия

до 75 т.р.

штраф по КоАП

Нарушение требований о защите информации

152-ФЗ ПДн

защита персональных данных

Что нужно сделать?

Чтобы выполнить требования 152-ФЗ, необходимо

1. Разъяснить необходимость сбора данных
2. Указать источник получения данных
3. Сообщить цель обработки данных
4. Хранить данные на серверах в РФ
5. Выполнить меры для защиты данных

! Для обработки общедоступных данных тоже нужно брать согласие человека и выполнять перечисленные обязанности

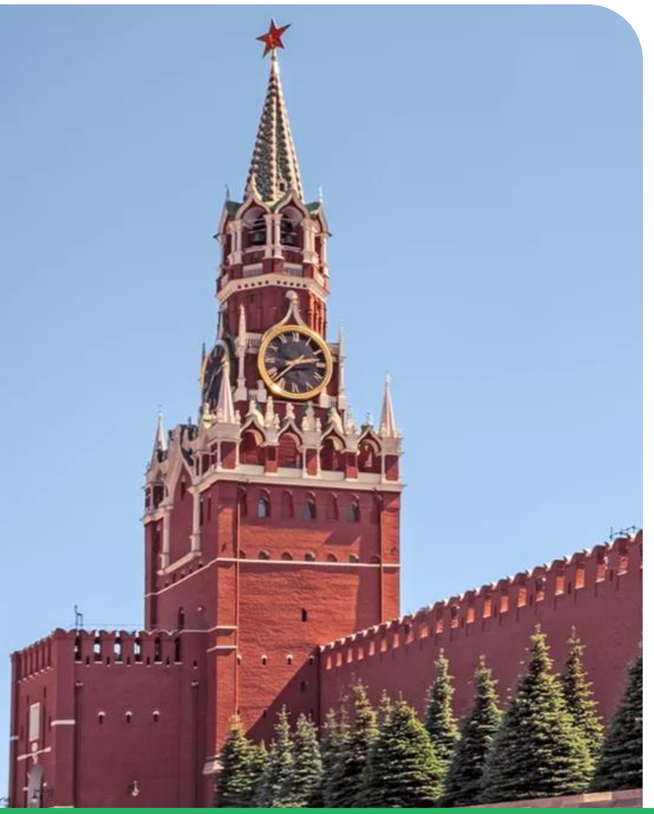
Что возьмем на себя?

- АУДИТ НА СООТВЕТСТВИЕ ТРЕБОВАНИЯМ 152-ФЗ
- РАЗРАБОТКА ТЕХНОРАБОЧЕГО ПРОЕКТА
- РАЗРАБОТКА МОДЕЛИ УГРОЗ И НАРУШИТЕЛЯ
- ВНЕДРЕНИЕ СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ
- РАЗРАБОТКА КОМПЛЕКТА ОРГАНИЗАЦИОННО-РАСПОРЯДИТЕЛЬНОЙ ДОКУМЕНТАЦИИ
- ПРОВЕДЕНИЕ АТТЕСТАЦИОННЫХ ИСПЫТАНИЙ
- РАЗРАБОТКА ТЕХЗАДАНИЯ НА СИСТЕМУ ЗАЩИТЫ ИНФОРМАЦИИ
- ПОДДЕРЖКА И СОПРОВОЖДЕНИЕ ВНЕДРЕННОЙ СИСТЕМЫ

WWW.RCNGROUP.RU

152-ФЗ ПДн

защита персональных данных



Несоблюдение закона о локализации приводит к штрафу и блокировке интернет-ресурсов компании

Локализация данных

на территории Российской Федерации

- Одна из обязанностей операторов ПДн — сбор, систематизация и хранение конфиденциальной информации в базах данных территории РФ.
- Трансграничная передача данных при определённых условиях не нарушает закон.
- Однако первоначально информация должна собираться в базах данных, размещённых в РФ.

Что возьмем на себя?

ВЫПОЛНИМ АУДИТ

информационных систем компании

РАЗРАБОТАЕМ ПРОЕКТ

по локализации данных и созданию системы защиты информации

ВЫПОЛНИМ РАБОТЫ

по переносу и настройке, сформируем необходимую документацию

ЗАЩИТА
от утечек информации

блокирование утечек, контроль коммуникаций, выявление мошенничества

Независимо от вида угрозы это всегда потеря денег

ХИЩЕНИЕ
конфиденциальной информации

НЕЦЕЛЕВОЕ ИСПОЛЬЗОВАНИЕ
сотрудниками рабочего времени

УТЕЧКИ ДАННЫХ
умышленные и непреднамеренные

WWW.RCNGROUP.RU

Что можно контролировать?

Микрофон компьютера	Файлы на компьютерах	Мессенджеры	Электронная почта
Запущенные приложения	Пересылаемые файлы	Внешние устройства	Почтовые серверы
Рабочий стол компьютера	Набираемый текст	Принтеры	Посещенные сайты
Время работы сотрудников	Сетевые диски	Буфер обмена	Социальные сети

ЗАЩИТА
от утечек информации

блокирование утечек, контроль коммуникаций, выявление мошенничества

Руководители

Информация о работе непосредственных подчиненных

Офицеры безопасности

Инциденты безопасности

HR

Информация о рабочем дне и рабочей активности

Особенности внедрения

- Установка и настройка из одной консоли
- Не требуются изменение инфраструктуры сети и покупка дополнительного оборудования
- Развертывание и запуск за несколько часов
- Сбор и анализ трафика сразу после установки

○ Информация компании защищена

○ Видимость только в пределах своей роли

ИМЕЮЩИЕСЯ ЛИЦЕНЗИИ

ЛИЦЕНЗИЯ ФСТЭК

на деятельность по технической защите конфиденциальной информации

ЛИЦЕНЗИЯ ФСБ

на осуществление деятельности по разработке, производству, распространению шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, выполнению работ, оказанию услуг в области шифрования информации, техническому обслуживанию шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств

СЕРТИФИКАТ СООТВЕТСТВИЯ

требованиям стандарта ГОСТ Р ИСО 9001-2015 (ISO 9001:20215)

СЛАБОТОЧНЫЕ СЕТИ

проектирование и внедрение

сформируем оптимальную и эффективную стратегию развития информационной безопасности компании

Пожарная сигнализация, системы оповещения и управления эвакуацией

- сохранить жизни сотрудников и имущество в случае пожара
- выполнить требования МЧС, чтобы избежать штрафов.

Структурированные кабельные системы

- объединить рабочие места сотрудников в единую локальную-вычислительную сеть
- объединить телефоны в единую телефонную сеть

Системы контроля и управления доступом

- обеспечить безопасность помещений компании
- учитывать время входа и выхода сотрудников

Системы охранного телевидения

- обеспечить безопасность зданий компании

Имеется лицензия МЧС России на осуществление деятельности по монтажу, техническому обслуживанию и ремонту средств обеспечения пожарной безопасности зданий и сооружений

РУБИКОН

100+

Исполненных контрактов, которые вы найдете на zakupki.gov.ru

5+

Лет на рынке информационной безопасности

10+

Средний стаж сотрудников в сфере информационной безопасности

10+

Наград и писем благодарности от заказчиков

WWW.RCNGROUP.RU

РУБИКОН

Наши контакты

поможем даже в самой сложной ситуации

ПОЛОВИНКО АРТЁМ
ДИРЕКТОР ПО ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Адрес г. Ростов-на-Дону, ул. Мясникова, 54 (оф. 405)

Телефон +7 (863) 273 34 24

E-mail info@rcngroup.ru

Сайт www.rcngroup.ru