КОНТУР
безопасность

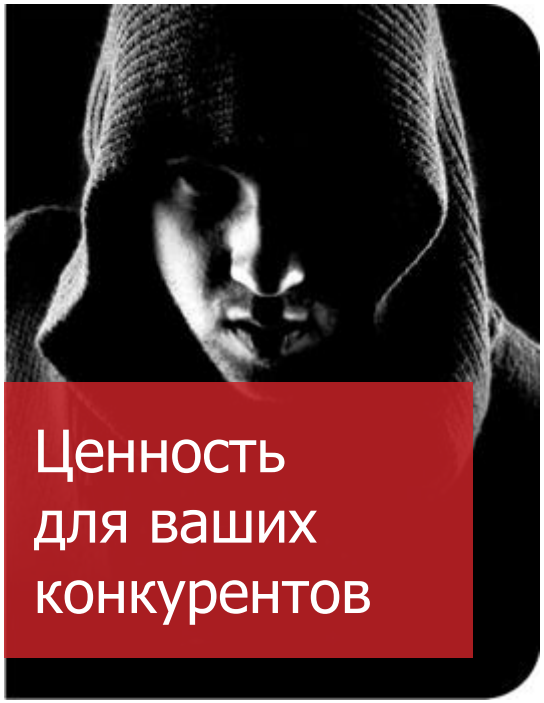
комплексная защита информации

Защита информации по вашим параметрам

Всё, что представляет ценность, необходимо защищать

КОНТУР безопасность

- Данные ваших сотрудников
- Информация о ваших клиентах
- Технологии вашего производства
- Специальные цены для партнеров
- Прочие коммерческие секреты



Последствия реализации угроз

КОНТУР безопасность

- Удар по бренду и репутации
- Потеря конкурентного преимущества
- Уменьшение акционерной стоимости
- Правовые и судебные иски от клиентов и партнеров
- Штрафы и санкции регуляторов
- Существенные затраты и усилия для извещения сторон

Финансовые потери

Риск банкротства

Сколько должна стоить защита информации

КОНТУР безопасность

Защита информации в соответствии с потребностями вашего бизнеса

КОНТУР безопасность

Точечная защита

- Высокая степень защиты от конкретных угроз
- Экономия вашего бюджета

Комплексная защита

- Гарантия защиты от различных угроз информационной безопасности

Комплекс услуг

КОНТУР безопасность

Аудит

информационной безопасности

Система

управления информационной безопасностью

Проектирование

и внедрение технических решений

Оценка

соответствия требованиям

Техническое сопровождение

систем информационной безопасности

Аудит информационной безопасности

КОНТУР безопасность

- **Анализ документации на соответствие нормами и требованиям, прописанным в законодательстве**
- **Анализ защищенности сети**

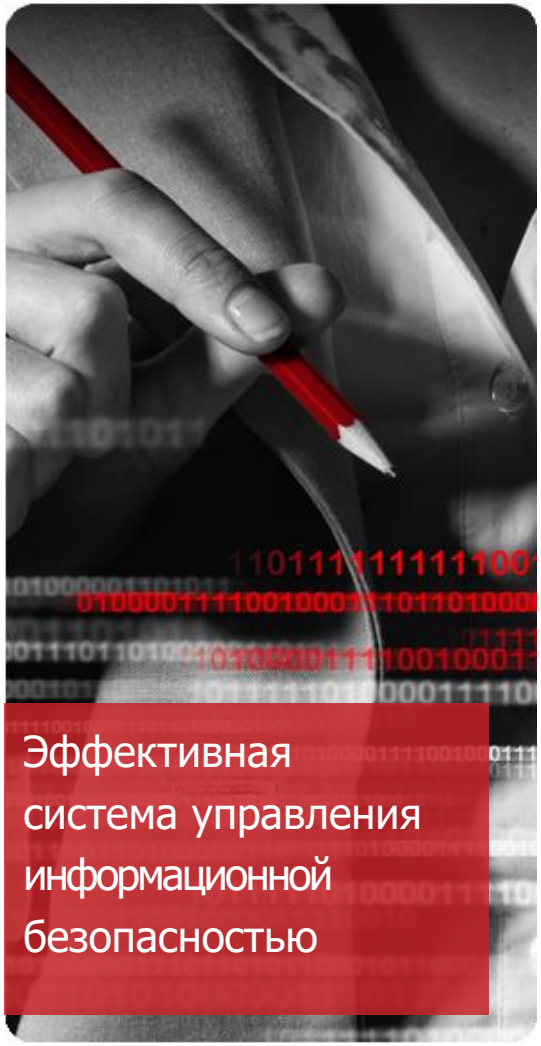
  Насколько текущие меры защиты корпоративной сети соответствуют требованиям лучших мировых практик в области информационной безопасности
- **Моделирование угроз**
  - определение угроз
  - описание каналов утечки информации
  - анализ поведения злоумышленника при взломе
  - тестирование защищенности сети
- **Рекомендации по предотвращению нарушений**

Оценка соответствия текущего уровня информационной безопасности на предприятии нормативным документам

Система управления информационной безопасностью

КОНТУР безопасность

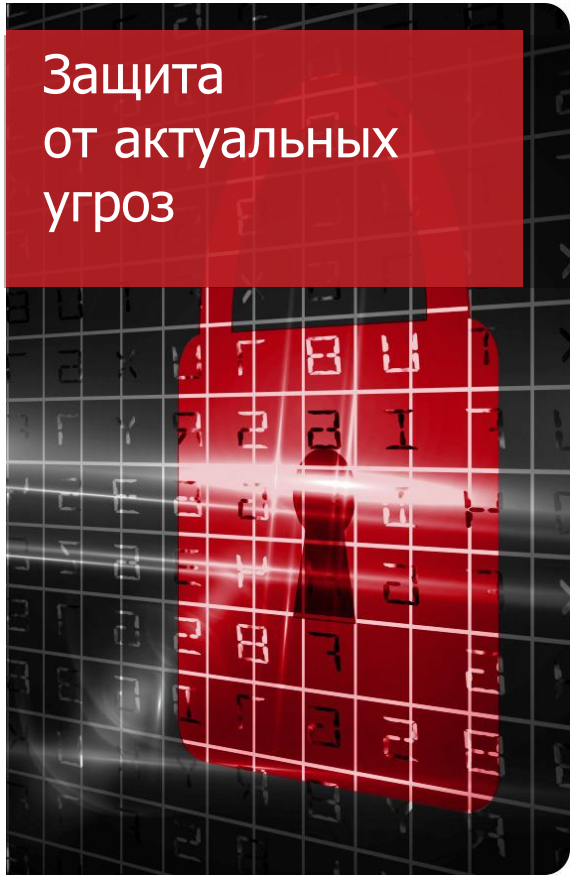
- Разработка организационной политики информационной безопасности
- Разработка политик информационной безопасности, ориентированных на задачи/системы
- Разработка инструкций и регламентов по информационной безопасности



Проектирование и внедрение технических решений

КОНТУР безопасность

- Антивирусная защита
- Идентификация и аутентификация
- Управление правами доступа к информации (IRM)
- Защита от несанкционированного доступа
- Межсетевое экранирование
- Обнаружение и предотвращение вторжений (IDS/IPS)
- Виртуальные частные сети VPN
- Инфраструктура открытых ключей PKI
- Обнаружение и предотвращение утечек информации DLP
- Криптографическая защита
- Резервное копирование и восстановление информации
- Автоматизированный анализ защищенности ИТ-инфраструктуры
- Защита информации от утечек по техническим каналам



Оценка соответствия требованиям

КОНТУР безопасность

Аттестация автоматизированных систем по требованиям безопасности информации

Оценка эффективности принимаемых мер по обеспечению безопасности ПДН в информационных системах персональных данных

Аттестация информационных систем персональных данных

Аттестация государственных/муниципальных информационных систем (ГИС/МИС)

Защищенное подключение к системам ФИС ГИА, ЕГИСМ, ФГИС Аккредитация

Техническое сопровождение систем информационной безопасности

КОНТУР безопасность

Периодический контроль состояния защиты информации на объектах информатизации

Техническое сопровождение систем защиты информации

Актуальность системы ИБ

Решения в области ИБ

КОНТУР безопасность

В портфеле компании множество готовых решений в области защиты данных.
Несмотря на отработанные методики, каждое решение будет уникальным.

Это зависит от многих факторов, которые выявляются при первом обследовании.

- Защита персональных данных
- Защита от внешних угроз при работе в интернете
- Защита от утечки данных
- Защита от утраты информации
- Защита информации при передаче по каналам связи
- Защита информации от несанкционированного изъятия
- Тест на проникновение

Защита персональных данных

КОНТУР безопасность

Проблема

Персональные данные обрабатывают почти все компании в РФ. Невыполнение требований 152-ФЗ грозит штрафами и другими мерами, вплоть до приостановки деятельности компании

Решение

Организационные мероприятия:

- оценка текущего состояния обработки ПДн, организационно-распорядительной документации и СЗИ на соответствие актуальным требованиям 152-ФЗ;
- моделирование угроз безопасности ПДн, проектирование эффективной работающей системы ИБ.

Технические мероприятия по созданию системы защиты персональных данных в соответствии с классом:

- поставка и внедрение технических средств защиты информации (сертифицированные межсетевые экраны, антивирусы, средства защиты каналов связи VPN, системы обнаружения и предотвращения вторжений и т. д.);
- настройка средств и систем защиты информации в соответствии с требованиями.

Дополнительные мероприятия:

- аттестация информационной системы персональных данных;
- помощь в прохождении проверки контролирующих органов (Роскомнадзор, ФСТЭК, ФСБ).

Результат

Непрерывность бизнес-процессов; выполнение требований 152-ФЗ «О персональных данных», отсутствие штрафов и претензий регуляторов.

Защита от внешних угроз при работе в интернете

КОНТУР безопасность

Проблема

Сотрудникам любой современной компании необходим постоянный доступ в интернет, однако Сеть является источником большого числа угроз, таких как компьютерные вирусы, сетевые атаки и т. д.

Решение

Мини-обследование, в результате которого выявляются актуальные уязвимости.

Организационная часть:

- создание матрицы доступа пользователей интернета;
- введение регламента работы в интернете;
- периодическое обучение пользователей работе с информацией.

Техническая часть может представлять собой комплекс следующих решений:

- антивирусное ПО;
- межсетевое экранирование;
- системы предотвращения атак IDS\IPS;
- мониторинг доступа пользователей к интернет-ресурсам.

Результат

Минимизация рисков, связанных с угрозами, которые исходят из интернета.

Защита от утечки данных

КОНТУР безопасность

Проблема

Наличие в компании ценной информации, утечка которой может обернуться потерей бизнеса.
При этом доступ к информации имеют многие легальные пользователи системы.

Решение

Организационная часть:

- определение перечня сведений, составляющих коммерческую тайну;
- обследование бизнес-процессов с целью выявления факторов риска;
- введение режима коммерческой тайны.

Технические меры защиты информации, составляющей коммерческую тайну:

- управление данными, разграничение доступа к информации;
- контроль съемных носителей, контроль печати;
- контроль доступа в интернет, контроль мессенджеров;
- контроль движения информации внутри корпоративной сети (DLP);
- шифрование данных.

Результат

Сохранение критически важной для бизнеса информации внутри компании; возмещение убытков компании при попытке инсайдеров воспользоваться информацией, составляющей коммерческую тайну.

Отзывы наших клиентов

КОНТУР безопасность

Лапина Марина Николаевна, и. о. начальника БСА «ОАО РосНИТИ»:

— Нам требовалась помощь в выборе и внедрении DLP-системы. После уточнения наших потребностей и возможностей специалисты «Контур-Безопасности» предоставили для тестирования 3 системы, одну из которых мы впоследствии и выбрали. Со стороны «Контур-Безопасности» работали грамотные технические специалисты. Они оперативно привезли и установили серверы, провели внедрение, консультировали по всем вопросам и быстро реагировали на нестандартные ситуации.

Вячеслав Новоселов, руководитель программы развития ИТ-инфраструктуры ООО «ГЕН СтройУрал»:

— Специалисты «Контур-Безопасности» провели аудит информационной безопасности на нашем предприятии. По итогам обследования были описаны основные угрозы и рекомендованы конкретные действия по их устранению. Также нам был предоставлен технический проект системы защиты информации. В рамках реализации этого проекта специалисты «Контур-Безопасности» успешно внедрили систему резервного копирования, которая позволила нам быть спокойными за обеспечение непрерывности бизнеса.

Защита от уничтожения информации

КОНТУР безопасность

Проблема

Наличие в любой компании информации, утрата или блокирование которой может привести к убыткам.

Решение

Организационная часть:

- определение критических информационных активов, предполагаемых вариантов их потери/утраты/уничтожения;
- разработка регламента резервного копирования.

Технические меры защиты информации, составляющей коммерческую тайну:

- установка программных и аппаратных средств резервного копирования, хранения и восстановления информации;
- настройка системы в соответствии с разработанным регламентом резервного копирования.

Результат

Обеспечение непрерывности ведения бизнеса.

Защита информации при передаче по каналам связи

КОНТУР безопасность

Проблема

В каждой компании есть ценная информация, которая передается по корпоративной сети в удаленные подразделения компании (филиалы) или контрагентам. Такая информация может быть перехвачена злоумышленниками.

Решение

Организационная часть:

- определение схем потоков информации, передающейся между удаленными подразделениями или контрагентам по каналам связи;
- формирование правил передачи информации между удаленными подразделениями компании или контрагентам.

Выбор оптимального технического решения:

шифрование пакетов передаваемых данных (VPN).

Результат

Защищенная передача данных и сохранение конфиденциальности информации, которая циркулирует между офисами и филиалами.

Защита информации от несанкционированного изъятия

КОНТУР безопасность

Проблема

В любой организации есть информация, доступная ограниченному кругу сотрудников (финансовые документы, данные о VIP-клиентах и т. п.), которая ни в коем случае не должна попасть в руки третьих лиц при изъятии или утере носителей.

Решение

Организационная часть:

- изучение бизнес-процессов путем обследования (для средних и крупных компаний) или в рамках простого опроса (небольшие предприятия), выявление критически важных данных, способов их хранения;
- формирование регламентов работы для сотрудников по обращению с информацией.

Техническая часть:

системы шифрования (SecretDisk) с возможностью уничтожения ключа для расшифровки информации при возникновении внештатной ситуации.

Результат

Возможность превратить информацию в бессмысленный набор символов при попытке ее изъятия.

Тест на проникновение (Penetration testing)

КОНТУР безопасность

Проблема

После создания ИТ-инфраструктуры важно проверить на практике, как она защищена от злоумышленников, т. к. даже верно подобранные технические средства защиты могут быть некорректно сконфигурированы.

Решение

Поиск максимально возможного числа уязвимостей и векторов атак за ограниченный промежуток времени.

Исследование ИТ-инфраструктуры (внутренняя сеть или внешний периметр):
в рамках заданного срока и модели нарушителя определяются все возможные известные уязвимости ПО, недостатки парольной политики, недостатки и тонкости настроек конфигурации, особенности архитектуры и т. д.

Исследование приложения и его окружения:
в рамках заданного срока и модели нарушителя проводится глубокий анализ приложения, определяются неизвестные уязвимости (архитектурные, некорректные настройки), а также проверяется окружение (ОС, базы данных, веб-сервер) на наличие известных уязвимостей, логики, парольной политики, тонких настроек и т. п.

Результат

Детальная проработка реальных уязвимостей и возможных векторов атак, а также рекомендации по их устранению.

Тест на проникновение (Penetration testing)

КОНТУР безопасность

Кейс

Крупная федеральная компания, пожелавшая остаться неизвестной, предоставляет востребованный веб-сервис для организаций по всей России.

Со слов представителей организации, выполнено всё, чтобы информация, обрабатываемая в сервисе, была защищена.
Однако решено было привлечь для независимой оценки людей, которые ничего не знают о том, как построена система защиты сервиса.

Уже на первом этапе тестирования (сканирование автосканерами) выяснилось, что серверы функционируют под управлением устаревшего ПО, имеющего большое количество уязвимостей.

Ручное тестирование выявило ряд еще более серьезных уязвимостей, которые позволяли получать доступ к ресурсам организации.

По итогам пен-теста был проведен общий аудит ИБ. Впоследствии скорректированы ключевые моменты в организации ИБ.

Преимущества работы с нами:

КОНТУР безопасность

«Контур-Безопасность» — проект компании СКБ Контур, который оказывает комплексные услуги по обеспечению информационной безопасности с 2009 года.

- Комплексный подход к информационной безопасности
- Оптимальное решение проблем клиентов за счет максимального использования возможностей каждого СЗИ
- Глубокое знание рынка технических средств
- Разработка проектов ИБ с учетом отраслевой специфики
- Богатая практика в различных отраслях экономики

О компании СКБ Контур

СКБ Контур

- Компания СКБ Контур основана в 1988 году и специализируется на разработке решений для электронного документооборота, программ для автоматизации бухгалтерского и кадрового учета, создании специализированных веб-сервисов
- Входит в пятерку крупнейших разработчиков программного обеспечения в России (рейтинг «Коммерсант Деньги», 2013 г.)
- Входит в ТОП-50 крупнейших ИТ-компаний России (по данным РИА-Аналитика и Cnews Analytics)
- Является лидером среди поставщиков SaaS-решений по объемам выручки от реализации облачных продуктов за 2013 год (Cnews, 2013)
- Клиентская база компании насчитывает более 1 миллиона абонентов

Преимущества работы с федеральной компанией:

СКБ Контур

- Многолетний опыт защиты информационных и автоматизированных систем
- Высокие стандарты работы
- Реализация проекта в любой точке России
- Рекомендации от крупных российских компаний
- Все необходимые лицензии

Наши клиенты

КОНТУР безопасность