SOLAR

SOLAR DOZOR

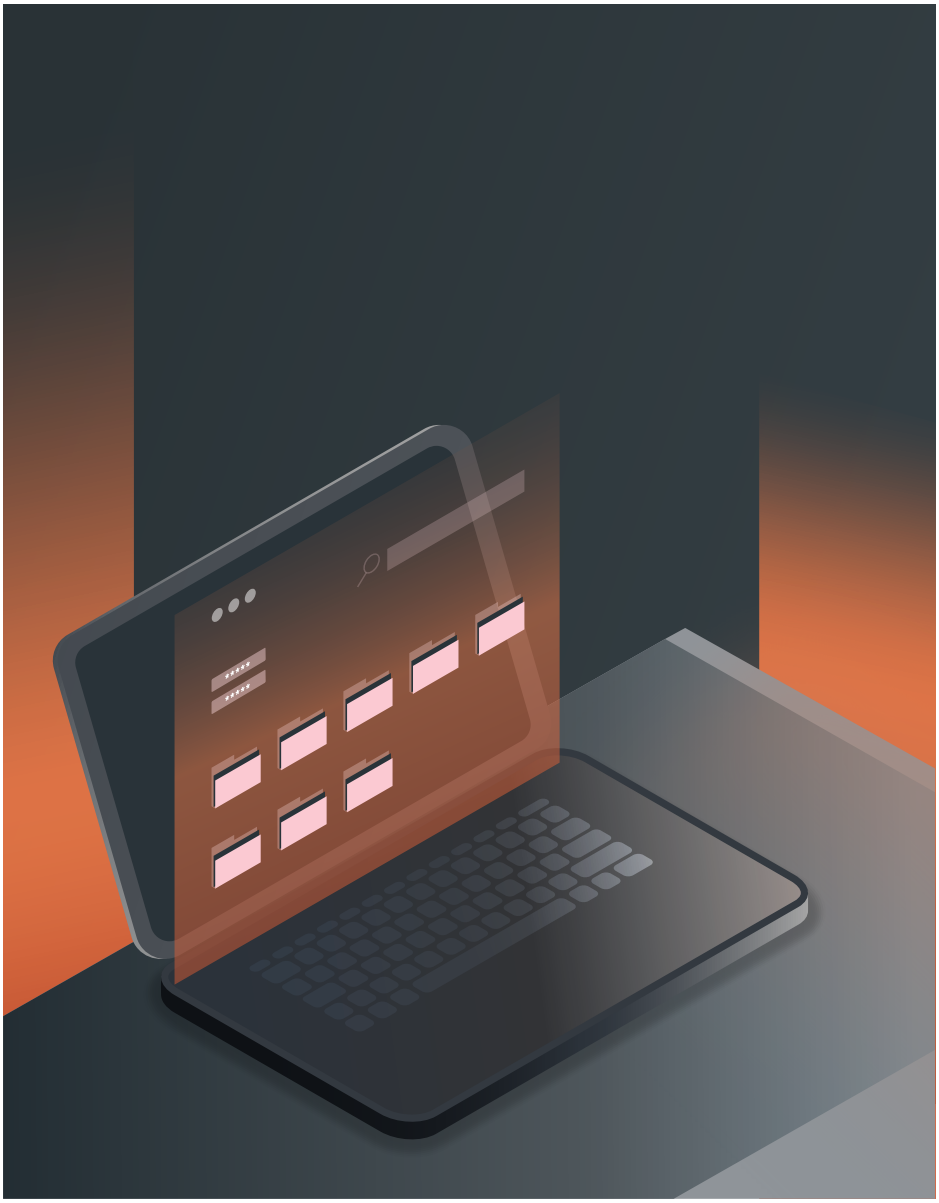
10 ШАГОВ К ПОСТРОЕНИЮ КОМПЛЕКСНОЙ СИСТЕМЫ ЗАЩИТЫ ДАННЫХ

Памятка

W: RT-SOLAR.RU

T: 8 (800) 302-85-23

Защита данных – казалось бы, такое простое и недвусмысленное понятие, но сам процесс на практике оказывается сложным и запутанным из-за широкого, если не сказать размытого, толкования этого термина. Каждая организация подразумевает под ним что-то свое и действует исходя из своих представлений.



Построение комплексной системы защиты данных в организации представляет собой многоэтапный процесс, состоящий из нескольких взаимосвязанных шагов. В этой памятке мы собрали 10 шагов, которые помогут вам в процессе построения или аудита системы защиты данных в вашей компании.

ШАГ 1

Аудит информационных активов

Рекомендуется проводить перед или параллельно с внедрением систем контроля и защиты данных.

Проводится в виде анкетирования работников. Если в компании отсутствует понимание о классификации информационных активов, они могут быть определены по рекомендации лиц, проводящих аудит.

В ходе аудита определяются:

- виды и типы информации
- критичность информации
- места ее хранения
- права доступа к информации и как они используются сотрудниками
- характер использования самой информации

Когда нужно проводить повторный аудит?

- Не реже одного раза в 2 года
- При существенном изменении организационной структуры, состава бизнес-активов (появление новых подразделений, филиалов и т. д.) и бизнес-процессов
- При изменениях в действующем законодательстве

ШАГ 2

Аудит процессов

Аудит процессов предполагает создание карты информационных потоков по основным бизнес-процессам организации.

Когда нужно проводить повторный аудит процессов?

- Не реже одного раза в 2 года
- При существенном изменении организационной структуры, состава бизнес-активов (появление новых подразделений, филиалов и т. д.) и бизнес-процессов.

ШАГ 3

Реестр информационных активов

Является результатом первых двух шагов – аудита информационных активов и аудита процессов.

Представляет собой систематизированное представление информационных активов со всеми характеристиками и ограничениями по передаче внутри периметра и за его пределы по каналам коммуникаций. Реестр используется для настройки системы контроля, а также разработки дискреционной модели доступа к внешним/внутренним ресурсам из внутреннего/внешнего периметра организации.

ШАГ 4

Аудит используемого ПО

Аудит используемого ПО проводится с целью формирования стандартов ПО, составления черных и белых списков. На этом этапе используются результаты аудита процессов и описание функциональных обязанностей сотрудников для профилирования универсального рабочего места (например, бухгалтера, дизайнера, HR-специалиста и т. п.), которое содержит, кроме прочего, перечень необходимого ПО.

Рекомендуем организовать внутренние репозитории ПО, системных и «золотых» образов, библиотек, обновлений и т. п., на уровне локальных нормативных актов (ЛНА) – описать процессы поддержания актуальности, контроля и использования ПО. Кроме того, необходимо описать порядок выдачи привилегированных прав (локальный, доменный администратор и т. п.) и их повышения для работников. Необходимо провести аудит прав доступа и выявить учетные записи с избыточным или критическим доступом. Аналогичные проверки прав проводятся и на этапе аудита инфраструктуры. Не забудьте предусмотреть проверку совместимости всех видов серверного и прикладного ПО.

Регулярность проведения инвентаризации ПО: раз в квартал.

ШАГ 5

Аудит инфраструктуры

Цель этого аудита – повышение видимости и прозрачности ландшафта инфраструктуры, выявление узких мест и отслеживание изменений ее компонентов. В рамках аудита выявляются учетные записи с избыточным/массовым доступом с привязкой к конкретной персоне, а также доступы к критическому оборудованию.

Результаты аудита инфраструктуры оформляются в виде отчетов и схемотехнических описаний с обозначением возможных проблем с инфраструктурой и зон риска.

Регулярность проведения аудита инфраструктуры: плановый аудит рекомендуем проводить раз в год, внеплановый – в случае кардинальных изменений инфраструктуры, состава бизнес-активов, действующего законодательства.

ШАГ 6

Архитектура комплексного решения

Выстраивание архитектуры комплексного решения с нуля (или ее пересмотр, актуализация) начинается с организации рабочих групп. Рекомендуем включить в их состав производителей программных продуктов и оборудования, планируемых к использованию. В рабочих группах прорабатываются варианты кросс-функциональных взаимодействий и требований к программному обеспечению и оборудованию, а также учитываются требования регуляторов и корпоративных стандартов.

Хорошей практикой считается агрегация данных со всех средств защиты и контроля с определением критически важных событий и инцидентов, методов реагирования и устранения.

Данный этап может проводиться в комплексе с аудитами инфраструктуры и ПО.

ШАГ 7

Аудит нормативной базы

Аудит внутренней нормативной документации проводится с целью проверки ее соответствия действующему законодательству, требованиям регуляторов, существующей организационной структуре и бизнес-процессам.

Регулярность проведения аудита нормативной базы: один раз в год, один раз в 2 года. При существенном изменении действующего законодательства и требований регуляторов проводится внеплановый аудит.

ШАГ 8

Анализ законодательной базы

Необходим регулярный мониторинг действующих и вновь принимаемых законных и подзаконных актов, а также требований и разъяснений профильных регуляторов, комитетов и органов.

ШАГ 9

Формирование комплекта организационно-распорядительной документации (ОРД)

При формировании комплекта ОРД вы можете опираться на перечень документов по легитимизации DLP-системы:

- Перечень информации, относящейся к коммерческой тайне (КТ) и персональным данным (ПДн)
- Положение о сведениях КТ и ПДн
- Приказ о введении режима защиты КТ и ПДн
- Листы ознакомления работников с Положением и Перечнем КТ и ПДн
- Политика допустимого использования корпоративных ресурсов
- Положение о контроле работников
- Соглашение о конфиденциальности с работником
- Уведомление работника о мониторинге и контроле
- Регламент мониторинга и контроля событий и инцидентов
- Регламент реагирования на выявленные инциденты ИБ
- Пакет шаблонов документов по оформлению разбора инцидента комиссией (приказ о назначении комиссии, запрос объяснения работника, объяснение работника, акт об отказе выдачи объяснения, протокол заседания комиссии)
- Приказ о введении в эксплуатацию систем защиты и контроля

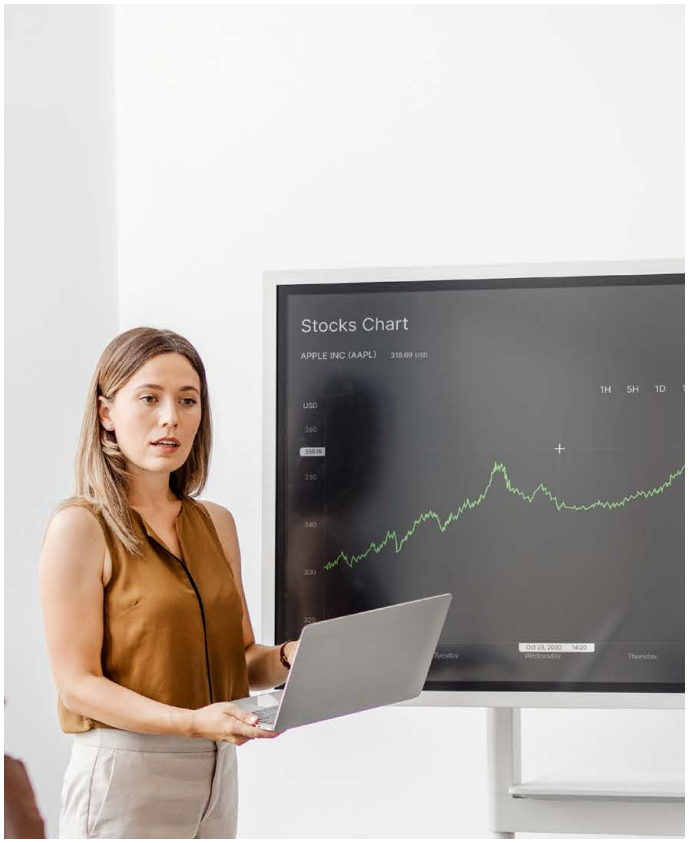
ШАГ 10

Юридическое сопровождение

Если анализ законодательной базы можно возложить на штатных юристов компании или выполнять самостоятельно, то для формирования комплекта ОРД и сопровождения судебных споров рекомендуем привлекать сторонних специалистов правового профиля.

О КОМПАНИИ

ГК «Солар» обеспечивает и гарантирует кибербезопасность в организациях от малого бизнеса до федеральных органов власти. Технологии компании и наличие распределенных по всей стране центров компетенций позволяют ей работать в режиме 24/7. Комплексный подход «Солар» включает в себя анализ угроз, предотвращение вторжений, построение и эксплуатацию систем кибербезопасности, что дает ей возможность нести ответственность за защиту от современных киберугроз. Ключевые направления деятельности компании – аутсорсинг ИБ, разработка собственных продуктов, комплексные проекты по кибербезопасности.



Линейка собственных продуктов включает DLP-решение Solar Dozor:

Solar Dozor – российская система предотвращения утечек конфиденциальной информации, выявления признаков корпоративного мошенничества. Отличается высокой производительностью, проработанным интуитивно понятным интерфейсом, полнофункциональным агентом под Linux и macOS, возможностью геораспределенной работы и технологичностью (нейронные сети, UBA, поддержка VDI).

ЧТО ДЕЛАТЬ ДАЛЬШЕ

Узнайте больше о DLP-системе Solar Dozor

Узнать подробнее

SOLAR

T +7 (499) 755-07-70
E info@rt-solar.ru

Центральный офис, 125009,
Москва, Никитский переулок, 7с1