b_152

Матрица критичных данных: где они живут, кто имеет доступ и что будет при утечке

Матрица помогает определить, какие данные критичны для компании, где они находятся, кто имеет к ним доступ и какие действия с ними разрешены.

info@b-152.ru
+7 (499) 372-45-85

Как составить матрицу

1 Определите категории данных

Выберите удобный принцип классификации:

По правовому режиму и статусу:

- Персональные данные;
- Коммерческая тайна;
- Служебная информация (ДСП);
- Профессиональная тайна (например, врачебная);
- Иные виды охраняемой законом тайны.

По характеру и назначению:

- Операционные и технические данные;
- Кадровые данные;
- Клиентские и партнерские данные;
- Финансовая информация;
- Интеллектуальная собственность;
- Публичная информация.

ВАЖНО: одни сведения могут относиться к нескольким категориям. Например, зарплатная ведомость содержит ПДн сотрудников и конфиденциальную финансовую информацию.

2 Зафиксируйте места хранения и копии

- Собственные информационные системы, включая ИСПДн;
- Облачные сервисы и SaaS-платформы;
- Серверы баз данных;
- Резервные копии и архивы;
- Тестовые среды;
- Рабочие устройства и локальные выгрузки;
- Бумажные документы и другие материальные носители;
- Системы и инфраструктуру подрядчиков.

3 Укажите, кто имеет доступ

- Подразделения и конкретные роли;
- Администраторы;
- Сотрудники поддержки и разработчики;
- Подрядчики;
- Владельцы привилегированных и сервисных учетных записей.

4 Определите допустимые действия с данными

Для каждой категории зафиксируйте, кому и какие операции разрешены:

- Хранение на бумажных и цифровых носителях;
- Передача по электронной почте и другим каналам связи;
- Отправка почтой;
- Копирование, изменение и удаление;
- Распространение и передача третьим лицам.

Отдельно оцените последствия неправомерного доступа или утечки: штрафы и претензии, финансовые потери, нарушение договоров, развитие кибератаки и репутационный ущерб.

5 Определите приоритет защиты

Учитывайте:

- Чувствительность данных;
- Объем информации и количество субъектов ПДн;
- Количество пользователей с доступом;
- Наличие копий;
- Возможные последствия утечки.

Пример заполненной матрицы

Категория данных	Где находятся	Кто имеет доступ	Возможные последствия утечки	Приоритет риска
Персональные данные	CRM, HR-система, BI, архивы, бэкапы, облако подрядчика	HR, продажи, маркетинг, ИТ, подрядчики	Раскрытие ПДн, штрафы, претензии субъектов, репутационный ущерб	Высокий
Финансовая информация	ERP, файловое хранилище, резервные копии	Финансовый отдел, руководство, ИТ, аудиторы	Финансовые потери, мошенничество, нарушение договоров	Средний
Учетные данные и ключи доступа	Хранилище секретов, конфигурации, репозитории	DevOps, разработчики, администраторы	Несанкционированный доступ, развитие атаки, остановка сервисов	Высокий
Коммерческая информация	ERP, CRM, почта, локальные выгрузки	Руководство, финансы, продажи, подрядчики	Потеря конкурентных преимуществ, финансовый ущерб	Средний
Исходный код и проектная документация	Система контроля версий, рабочие устройства, бэкапы	Разработчики, DevOps, подрядчики	Утечка интеллектуальной собственности, компрометация продукта	Низкий

Приоритеты в примере условные. Фактический уровень риска определяется для конкретной организации.

В рабочую матрицу дополнительно внесите **допустимые действия с каждой категорией данных** и ответственных за их согласование.

Проверьте себя

- [ ] Все критичные категории данных определены.
- [ ] Указаны все места хранения, включая копии, бумажные носители и тестовые среды.
- [ ] Установлено, кто имеет доступ, включая подрядчиков и сервисные аккаунты.
- [ ] Определены допустимые действия с каждой категорией данных.
- [ ] Оценены возможные последствия утечки.
- [ ] Определен приоритет риска для каждой категории.
- [ ] Для всех критичных данных назначены владельцы.
- [ ] По результатам проверки определены необходимые меры защиты и ответственные за их выполнение.

ВАЖНО! Матрица не заменяет инвентаризацию ПДн и оценку рисков ИБ, но помогает связать их с реальной инфраструктурой компании и выявить неочевидные места хранения и доступа.