# Как принять DLP в работу

*Практическое руководство и рабочая тетрадь для аналитика и администратора*

Валерий Лагутин

Это пособие поможет разобраться в уже установленной DLP, определить её реальные границы и организовать свою работу. Оно подходит специалисту, который пришёл в новую организацию, принял систему у коллеги или впервые получил ответственность за её использование.

Вы пройдёте пять этапов. Сначала выясните задачи организации, затем сопоставите их с охватом системы, разберётесь в действующих настройках, договоритесь о порядке работы и составите план улучшений. По итогам у вас появится краткое описание DLP, список подтверждённых ограничений и понятный план на первый месяц.

Руководство рассчитано на разные DLP-системы. Названия экранов, состав модулей и доступные действия различаются. В тексте объясняется, какие сведения искать и какой вывод из них можно сделать. Точное расположение настроек уточняйте в документации вашей системы.

Подробные расследования отдельных нарушений остаются за рамками этого маршрута. Здесь вы готовите систему и рабочий процесс к повседневному использованию.

# Содержание

## Руководство

Как пользоваться книгой 3

1 Разобраться в задаче 4

2 Понять границы контроля 7

3 Разобраться в настройках 11

4 Организовать свою работу 15

5 Составить план улучшений 19

## Рабочая тетрадь

Работа с формами 23

Форма 1 Паспорт и задача 24

Форма 2 Границы контроля 25

Форма 3 Разбор действующей настройки 26

Форма 4 Повседневная работа 27

Форма 5 Задача на улучшение 28

## Заполненные примеры

Пример 1 Паспорт и задача 29

Пример 2 Границы контроля 30

Пример 3 Разбор действующей настройки 31

Пример 4 Повседневная работа 32

Пример 5 План первого месяца 33

## Как пользоваться книгой

Читайте разделы по порядку, если принимаете DLP впервые. Если часть работы уже выполнена, начните с соответствующего этапа и проверьте, есть ли результаты предыдущих. Например, осмысленно пересматривать исключения можно после того, как стали понятны разрешённые рабочие процессы.

Для каждого этапа предусмотрена одна форма в практической части этой книги «Рабочая тетрадь». Скопируйте нужную форму в свой рабочий документ или используйте её поля в действующей системе учёта. Если организация уже ведёт аналогичные сведения в системе заявок или внутренней базе знаний, используйте существующее место хранения. Переписывать данные ради заполнения тетради не требуется.

1. Разобраться в задаче. Результат — понятная цель работы и согласованные полномочия.
2. Понять границы контроля. Результат — описание того, что подтверждено, что ограничено и что пока неизвестно.
3. Разобраться в настройках. Результат — понятное назначение важных политик и решения по спорным настройкам.
4. Организовать свою работу. Результат — повседневный порядок действий и передачи задач.
5. Составить план улучшений. Результат — выполнимый план с ответственными и проверкой результата.

Не стремитесь заполнить все поля в первый день. Запись «не выяснено, уточнить у администратора почты до пятницы» полезнее предположения, которое позже будут принимать за факт.

**Как отмечать достоверность.** Используйте обычные слова: «подтверждено», «известно со слов», «не выяснено». Рядом записывайте дату, способ проверки и ограничения. Это рабочие пометки, а не отдельная система классификации.

**Если аналитик и администратор — разные люди.** Аналитик изучает доступные события, формулирует вопросы и оценивает пригодность данных. Администратор проверяет сбор, обработку и применение настроек в своей зоне ответственности. Кто меняет конфигурацию и кто разрешает изменение, нужно определить отдельно. Если обе задачи выполняете вы, сохраняйте это различие при согласовании решений.

**Если времени мало.** До подробного разбора выясните, кто принимает срочные сообщения, есть ли известный перерыв в контроле важного процесса и доступны ли ответственные сотрудники. Остальную работу запланируйте. Реальную проблему с продолжающимся ущербом передавайте по принятому порядку сразу, не дожидаясь завершения пособия.

### Сквозной пример компании Меридиан

«Меридиан» — вымышленная компания. Все приведённые сведения, сотрудники и результаты проверок придуманы для объяснения маршрута. Они не являются результатами проверки действующей DLP.

В компании передают клиентские реестры через корпоративную почту. Руководитель хочет получать сообщения о передаче таких сведений внешним получателям. У ИТ есть список из 60 действующих рабочих компьютеров. В консоли DLP отображается 65 записей об устройствах. В отделе продаж работают восемь сотрудников.

Новому специалисту передали доступ в консоль и сказали, что «всё уже настроено». В ходе работы он обнаруживает старые записи об устройствах и временное исключение для всего отдела продаж. Его задача — выяснить фактическое положение, согласовать решения и организовать дальнейшую работу. По мере чтения вы увидите, как меняются его записи.

# 1 Разобраться в задаче

Первый этап нужен, чтобы связать работу DLP с задачами организации. В первые дни легко потратить всё время на просмотр событий и настроек. Но без понимания того, что компания считает допустимым, даже корректное срабатывание трудно оценить.

Начните с короткого разговора с руководителем, который отвечает за использование DLP. Затем уточните рабочие процессы у людей, чьи подразделения создают и передают важные сведения. Разговоры лучше привязать к конкретным документам и операциям.

### Выясните ожидания руководителя

Вопрос «зачем у нас DLP» нередко вызывает общий ответ: «для защиты информации». Переведите его в рабочую задачу. Какие сведения сейчас важнее всего? Какая передача вызывает беспокойство? Кто должен получить сообщение? Какое действие он сможет принять после сообщения?

Например, «контролировать клиентские данные» можно уточнить так: «обращать внимание на передачу клиентских реестров внешним адресатам через корпоративную почту и передавать спорные случаи руководителю ИБ». Здесь уже понятны данные, операция, канал и получатель результата.

Попросите назвать одну или две задачи, с которых следует начать. Это не отменяет остальных обязанностей. Такая договорённость помогает распределить

внимание, пока вы ещё изучаете систему. Зафиксируйте также обязательные текущие задачи, которые нельзя приостановить на время приёма дел.

Если ожидание звучит как «предотвращать любые утечки», уточните его границы. Какие устройства принадлежат организации? Есть ли рабочие процессы в облаках? На каких участках система наблюдает за событиями, а на каких может влиять на передачу? Обещание полного контроля без проверки возможностей и охвата создаёт неверное ожидание у руководителя.

**Что записать.** В форме 1 сформулируйте цель двумя или тремя предложениями. Укажите, кто подтвердил задачу, и перечислите вопросы, по которым решения пока нет.

## Изучите разрешённые рабочие процессы

Попросите владельца процесса описать обычный рабочий день. Какие сведения сотрудник получает, что с ними делает и кому передаёт результат? Для начала достаточно одного важного процесса. Например, подготовка и отправка реестра партнёру или обмен документами с бухгалтерским подрядчиком.

Один и тот же документ может участвовать и в разрешённой, и в нежелательной передаче. Значение имеют получатель, цель, объём и способ передачи. Названия файла обычно недостаточно для вывода. Если допустимые варианты нигде не описаны, запишите вопрос владельцу процесса, а не вводите собственное правило от имени организации.

Для обсуждения удобно использовать обезличенный пример. Пусть сотрудник покажет, какие поля содержит документ, какой адресат получает его по работе и как подтверждается разрешение. Реальный клиентский реестр не нужно копировать в рабочую тетрадь. Достаточно описать состав и место хранения утверждённого примера.

Спросите о редких, но необходимых действиях. Ежеквартальная передача большого файла, работа замещающего сотрудника или обмен с новым подрядчиком могут отличаться от повседневного процесса. Если такие действия забыть, новая настройка позже начнёт мешать работе.

Зафиксируйте, кто имеет право подтвердить допустимость передачи. Сотрудник ИТ может объяснить технический маршрут документа, но разрешение на его передачу обычно относится к ответственности владельца данных или другого назначенного лица. Уточните принятую в организации модель, не назначая ответственных самостоятельно.

**Пример.** В «Меридиане» руководитель продаж объяснил, что часть клиентских сведений передают согласованному партнёру. Передача полного реестра на любой внешний адрес разрешённой работой не является. Специалист записал: «Проверять сообщения о внешней передаче; допустимость конкретной передачи

подтверждает руководитель продаж. Перечень согласованных адресатов требуется уточнить».

## Договоритесь о полномочиях и взаимодействии

До самостоятельных действий выясните, что вы можете просматривать, выгружать, изменять и кому вправе передавать сведения. Доступ к консоли сам по себе не объясняет порядок работы. Организационные полномочия и технические права должны соответствовать порученным задачам.

Попросите показать действующий порядок работы, если он есть. Уточните, кто согласует изменение политики, кто разбирает технические неисправности и кто принимает решение по спорному событию. Отдельно выясните порядок обращения к сведениям о сотрудниках и передачи материалов другим подразделениям.

Для ежедневной работы достаточно короткого списка контактов с заменой на время отсутствия. Важнее знать, какое решение принимает человек, чем перечислить все должности компании. Формулировка «руководитель ИБ решает вопрос о срочном ограничении; при его отсутствии — назначенный заместитель» полезнее списка фамилий без полномочий.

Если часть нужных действий вам недоступна, согласуйте способ их выполнения через ответственного сотрудника. Например, аналитик может попросить администратора показать состояние обработки на сервере. Не обязательно выдавать аналитику расширенные права только ради разовой проверки.

Доступ нового специалиста лучше предоставлять на его личную учётную запись. Если дела передают через общую запись, выясните, как перейти к принятому в организации порядку доступа и сохранить возможность разобраться в предыдущих изменениях. Не меняйте и не удаляйте старые записи без согласования с ответственным за доступ.

## Запросите сведения для передачи дел

Попросите предыдущего специалиста или владельца системы показать основные рабочие места: консоль, состояние компонентов, действующие политики, журнал изменений и место хранения эксплуатационных записей. Цель такой встречи — понять, где искать ответы, а не запомнить все настройки сразу.

Сначала соберите уже существующие сведения: описание состава системы, действующие контакты поддержки, список известных неисправностей и незавершённых работ. Уточните, кто поддерживает серверы, интеграции и рабочие станции, а также где фиксируются обновления и обращения к поставщику.

Попросите отдельно рассказать об обходных решениях. Временные исключения, ручные перезапуски и периодические выгрузки часто остаются в памяти одного

человека. Запишите причину каждого такого действия и условие, при котором оно должно прекратиться.

Пароли, ключи и другие секреты не помещайте в паспорт DLP. Укажите, где они хранятся по принятому порядку и кто обеспечивает доступ. Сам паспорт может описывать устройство контроля, поэтому место его хранения и круг читателей также нужно определить.

Если предыдущего специалиста нет, не останавливайтесь. Собирайте сведения из конфигурации, заявок, внутренних документов и разговоров с ответственными. Отмечайте, какие ответы получены только со слов. Восстановление истории должно помогать текущей работе; отсутствие старого согласования не нужно компенсировать придуманной датой или подписью.

### Зафиксируйте исходное положение

Завершите этап коротким описанием: для чего используется DLP, кто за что отвечает, где находится информация и какие вопросы ещё открыты. Это начало паспорта системы, а не подробная техническая документация.

Сохраните дату исходного состояния. Если позже вы измените исключение или подключите новый источник, должно быть понятно, что существовало при приёме дел. Для важных настроек укажите место доступной выгрузки или согласованного снимка экрана. Копировать в паспорт все события и документы пользователей не требуется.

**Проверьте себя.** Можете ли вы своими словами объяснить первую рабочую задачу, назвать человека, который принимает решение по ней, и понять предел своих действий? Если ответы есть, переходите к границам контроля. Нерешённые вопросы сохраните с ответственным за уточнение.

**Результат в примере.** У специалиста «Меридиана» появилась согласованная задача по внешней передаче клиентских реестров. Руководитель продаж подтверждает допустимые рабочие передачи. ИТ отвечает за подключение устройств и почтовый источник. Изменения действующих настроек согласует руководитель ИБ. Старое исключение для продаж записано как вопрос, который предстоит изучить.

## 2 Понять границы контроля

Второй этап помогает отделить предполагаемый охват от подтверждённого. Наличие лицензии, агента или записи в консоли говорит о конкретном состоянии системы. Для рабочего вывода важно понять, какие действия вы действительно сможете увидеть и какие настройки на них распространяются.