УДК 004.021

Паутова Л.Д.,
студент магистратуры,
Национальный исследовательский Нижегородский государственный университет им. Н.И. Лобачевского,
г. Нижний Новгород

ИДЕНТИФИКАЦИЯ ИНФОРМАЦИОННЫХ АКТИВОВ НА ОСНОВЕ DFD-МОДЕЛЕЙ: МЕТОДИЧЕСКИЙ ПОДХОД ДЛЯ МАЛЫХ IT-КОМПАНИЙ

Аннотация: *В статье представлен методический подход к идентификации информационных активов в малых IT-компаниях, основанный на построении DFD (диаграмм потоков данных). Подход ограничен двумя ключевыми шагами: 1) выбор ключевых бизнес-процессов для анализа, 2) построение DFD-моделей этих процессов с последующей инвентаризацией активов. Описаны критерии отбора процессов, правила построения DFD первого уровня, а также техника выявления «скрытых» активов и маркировки точек риска. Применимость подхода апробирована на стандартном процессе малой IT-компании (разработка программных продуктов).*

Ключевые слова: *DFD, идентификация активов, малый IT-бизнес, выбор бизнес-процессов, реестр активов, анализ рисков ИБ.*

Annotation: *The article presents a methodological approach to the identification of information assets in small IT companies based on the construction of DFD (data flow diagrams). The approach is limited to two key steps: 1) selecting key business processes for analysis, 2) building DFD models of these processes followed by asset inventory. The criteria for selecting processes, the rules for building a first-level DFD, as well as the technique for identifying "hidden" assets*

and marking risk points are described. The applicability of the approach has been tested on the standard process of a small IT company (software product development).

Key words: *DFD, asset identification, small IT business, business process selection, asset registry, information security risk analysis.*

Введение

С каждым годом возрастают внешние и внутренние угрозы информационной среды, такие как кибератаки, утечки данных или несанкционированный доступ. Для любой сферы деятельности, связанной с информационными технологиями, критически важно обеспечить защиту информационной инфраструктуры и данных. Особенно уязвимы небольшие IT-компании, не располагающие значительным бюджетом для обеспечения ИБ. Исходя из правового поля РФ, методический подход идентификации активов нацелен на компании, число сотрудников которых не превышает 100 человек [1] и предельный размер годовой выручки не превосходит 800 млн. рублей [2].

Первым этапом любого анализа рисков информационной безопасности является идентификация информационных активов [3, с. 8]. Однако практика показывает, что в малых IT-компаниях реестр активов либо отсутствует, либо неполон. При этом во время мозгового штурма по составлению реестра активов могут быть упущены «теневые» активы (например, неформальные файлы конфигураций, локальные копии ПДн). Это приводит к тому, что реальные уязвимости остаются вне поля процесса анализа.

Информационные потоки являются ключевой системой IT-компании и основным объектом защиты. Метод их моделирования должен наглядно отображать движение критичных данных (конфиденциальная информация, персональные данные, ключи доступа) по бизнес-процессам, точки их обработки, хранения и передачи, а также границы доверенных зон.

Методология DFD (Data Flow Diagrams) предназначена для описания бизнес-процессов предприятия с точки зрения ввода, обработки и хранения информации. Отличительной особенностью ее является наличие хранилищ данных и внешних сущностей – источников и приемников данных, находящихся за пределами рассматриваемой системы. Потоки данных используются для моделирования передачи информации из одной части системы в другую и на диаграммах изображаются именованными стрелками, ориентация которых указывает направление движения информации. Кроме того, методология включает функции (процессы, преобразующие потоки данных), а также хранилища – внутренние накопители информации (базы данных, файлы, физические хранилища) [4, с. 43]. Преимущества DFD для анализа рисков ИБ заключаются в следующем: элемент «хранилище» позволяет инвентаризировать все точки накопления информации (базы данных, удаленные файловые серверы, облачные диски), которые можно выделить как критичные активы; визуализация потоков между процессами и сущностями наглядно показывает, как данные перемещаются между внутренними процессами и внешними субъектами, что позволяет идентифицировать каналы передачи данных, оценить их защищенность и выявить избыточные маршруты; анализируя DFD, можно проверить, имеет ли каждый процесс доступ только к тем хранилищам и внешним сущностям, которые необходимы для его функции, и выявить нарушения принципа минимизации привилегий.

Методический подход к идентификации активов на основе DFD

Предлагаемый методический подход к идентификации информационных активов для малых IT-компаний состоит из двух ключевых шагов.

Первый шаг – выбор приоритетных бизнес-процессов для анализа. При согласовании с руководителем организации достаточно выбрать 1–3 процесса, которые несут основные риски. Критериями отбора могут выступать

критичность для выручки и репутации, обработка чувствительных активов (персональные данные, коммерческая тайна, исходный код), высокая частота информационных обменов, наличие предпосылок инцидентов.

Второй шаг – построение DFD-модели выбранного процесса и идентификация активов. Для выбранного процесса строится DFD-диаграмма первого уровня. На диаграмме отражаются внешние сущности, основные процессы, хранилища данных (система управления задачами, Git-репозиторий, тестовая база данных и т.д.) и потоки данных между ними. Каждый поток и каждое хранилище анализируются на предмет того, какие информационные активы в них содержатся. Полученные активы заносятся в реестр. Дополнительно для каждого актива фиксируется отсутствующая базовая мера защиты (например, отсутствие шифрования, двухфакторной аутентификации, обезличивания, логирования). Эти «болевые точки» маркируются на DFD красным цветом для наглядности. Под болевой точкой подразумевается место на DFD диаграмме в виде хранилища либо потока, где не внедрена хотя бы одна базовая мера защиты. Для определенности в таблице 1 представлены примеры проверки базовых мер защиты.

Таблица 1.

Примеры проверки базовых мер защиты

Мера защиты	Список обследования
Наличие шифрования при хранении	Изучение конфигурацию серверов, облачных хранилищ и баз данных
Правило разграничения доступа	Проверка права в репозитории и базах данных
Логирование в части доступа и обновления данных	Проверка наличия логов на сроки, необходимые для выявления нежелаемых изменений
Резервное копирование с проверкой целостности	Уточнение у администраторов системы или изучение регламентов (если существуют)

Практическая апробация: процесс разработки ERP-решения

Ниже представлена сформированная DFD-диаграмма процесса разработки и тестирование нового функционала ERP-решения для малой IT-компании, специализирующейся на внедрении ERP-решений для малого

бизнеса. Границы процесса начинаются от получения технического задания и заканчиваются в момент передачи готовой доработки в репозиторий и развертывание ее на тестовой среде.

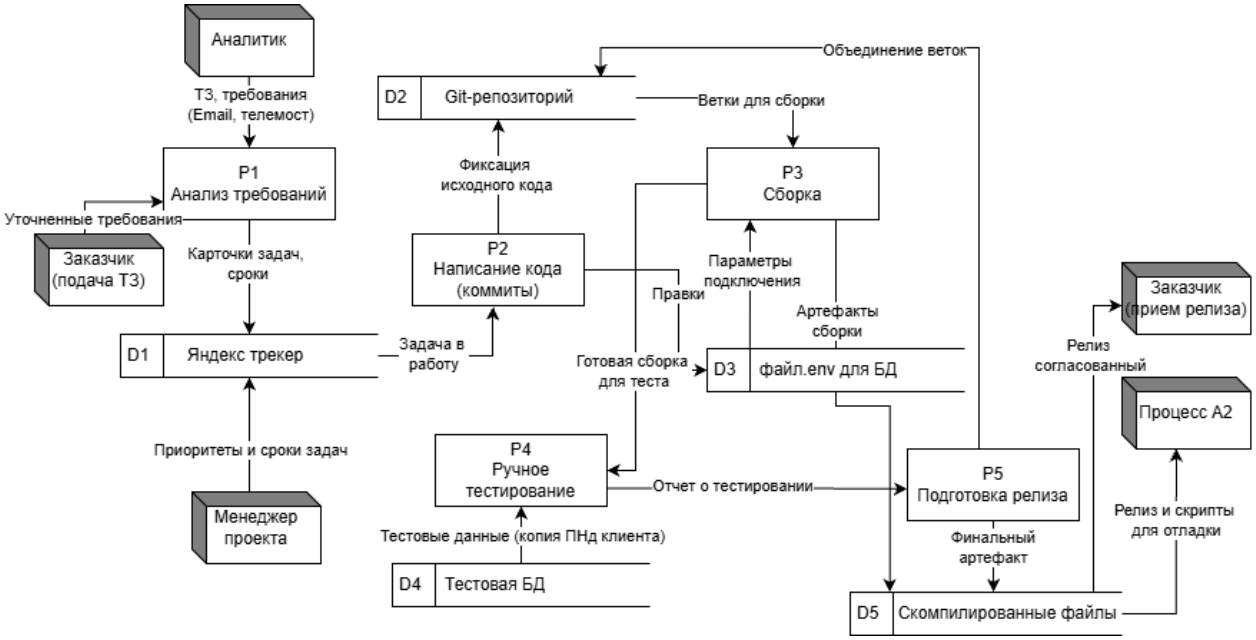


Рисунок 1. DFD процесса «Разработка и тестирование нового функционала ERP-решения»

Фрагмент реестра активов, полученный при применении DFD-моделирования к процессу разработки и тестирования в малой IT-компании, сформирован в таблице 2.

Таблица 2.

Перечень активов по результатам этапа 2

ID актива	Название актива	Источник (объект DFD)	Отсутствующая базовая мера защиты
A1	Техническое задание заказчика	Поток «Заказчик – P1»	Шифрование при передаче
A2	Уточненные требования аналитика	Поток «Аналитик – P1»	—
A3	Карточки задач, сроки	Поток «P1 – D1»	Логирование доступа
A4	Исходный код (коммит)	Поток «P2 – D2»	Двухфакторная аутентификация разработчиков

A5	Параметры подключения и пароли БД	Поток «D3 – P3», хранилище D3	Шифрование при хранении, разграничение доступа
A6	Тестовые данные с реальными ПДн	Поток «P4 – D4», хранилище D4	Обезличивание данных
A7	Отчет о тестировании	Поток «P4 – P5»	Разграничение доступа
A8	Готовый релиз модуля ERP	Поток «D5 – Заказчик»	Контроль целостности при передаче
A9	Яндекс Трекер (БД задач)	Хранилище D1	Логирование, разграничение доступа по проектам
A10	Git-репозиторий (исходный код)	Хранилище D2	Резервное копирование с проверкой, 2FA
A11	Тестовая БД PostgreSQL	Хранилище D4	Разграничение доступа, обезличивание

Как видно из реестра, применение DFD позволило выявить как очевидные активы (исходный код, задачи), так и «теневые» – тестовую базу данных, содержащую реальные персональные данные клиентов без обезличивания. Без визуализации потоков данных такие объекты часто пропускаются при традиционном анкетировании сотрудников.

Заключение

Для небольшой IT-компании предложенный порядок идентификации активов, основанный на DFD, можно считать практически оправданным. Его ценность связана прежде всего с тем, что схема процесса в явном виде фиксирует перемещение и точки хранения данных: при такой декомпозиции обнаруживаются сущности, которые при неструктурированном интервью обычно остаются вне поля зрения. Далее открывается возможность привязки каждого актива к конкретному элементу DFD (потоку или хранилищу), которая создает основу для последующей оценки уязвимостей и выбора точечных контрмер (в реестре сразу фиксируется отсутствующая базовая мера защиты). Существенно и то, что внедрение подхода не требует обязательного приобретения дорогостоящих инструментов: при участии команды двух штатных сотрудников работа выполнима за 2–3 рабочих дня. Тем самым использование DFD-моделирования для идентификации активов

подтверждает свою применимость на практике и повышает полноту, а также качество дальнейшей оценки рисков в области информационной безопасности.

Использованные источники:

1. Федеральный закон от 24.07.2007 N 209-ФЗ (ред. от 31.07.2025) "О развитии малого и среднего предпринимательства в Российской Федерации". Электронный доступ: https://www.consultant.ru/document/cons_doc_LAW_52144/ (дата обращения: 01.04.2026).

2. Постановление Правительства РФ от 04.04.2016 N 265 "О предельных значениях дохода, полученного от осуществления предпринимательской деятельности, для каждой категории субъектов малого и среднего предпринимательства". Электронный доступ: https://www.consultant.ru/document/cons_doc_LAW_196415/ (дата обращения: 01.04.2026).

3. ГОСТ Р ИСО/МЭК 27005-2010. Информационная технология. Методы и средства обеспечения безопасности. Менеджмент риска информационной безопасности. Взамен ГОСТ Р ИСО/МЭК ТО 13335-3-2007 и ГОСТ Р ИСО/ МЭК ТО 13335-4-2007.

4. Спицина И. А. Системный анализ и моделирование информационных систем: учебное пособие – Министерство науки и высшего образования Российской Федерации – Екатеринбург: Издательство Уральского университета, 2021. – 118 с.