# Цель инвентаризации IT-активов

Целью инвентаризации IT-активов является формирование перечня таких активов. Анализ данных об IT-активах и связях между ними помогает сформировать представление об IT-инфраструктуре организации. Результаты инвентаризации могут использоваться для определения и уточнения целевых и ключевых систем и точек проникновения.

В рамках концепции результативной кибербезопасности по результатам инвентаризации требуется получить информацию о следующих видах IT-активов:

* узлы сетевого периметра и локальной вычислительной сети (далее — ЛВС);
* сервисы, запущенные на узлах внешнего сетевого периметра;
* корпоративные беспроводные сети, в том числе гостевые;
* инфраструктура облачных сервисов.

Все вышеперечисленные активы (кроме узлов в ЛВС) должны оцениваться с точки зрения возможности получения доступа в ЛВС организации.

**IT-актив** — программное обеспечение или оборудование, которое используется в организации для обработки, хранения и передачи информации

**Инвентаризация IT-активов** — сбор сведений об IT-активах для получения представления об IT-инфраструктуре организации.

Для проведения инвентаризации могут быть использованы данные из уже имеющихся систем, в которых ведется учет IT-активов.

# Виды учета IT-активов

В организациях могут быть внедрены различные системы учета IT-активов:

1. Учет IT-активов для бухгалтерского учета.
2. Учет IT-активов для предоставления IT-услуг.
3. Учет IT-активов для обеспечения ИБ.

Нужно понимать, что IT-актив может учитываться по-разному (например, как имущество организации или как конфигурационная единица, участвующая в предоставлении IT-услуги), поэтому информация из других систем учета нуждается в дополнительном анализе. Характеристики систем учета IT-активов приведены в таблице 1.

*Таблица 1. Характеристики различных систем учета IT-активов*

| **Вид учета** | **Учет IT-активов для бухгалтерского учета** | **Учет IT-активов для предоставления IT-услуг** | **Учет IT-активов для обеспечения ИБ** |
| --- | --- | --- | --- |
| Цель учета | Регистрация и обобщение информации о состоянии IT-активов в денежном выражении | Предоставление IT-услуги в соответствии с соглашением об уровне обслуживания (SLA) или соглашением об операционном уровне (OLA) | Контроль за IT-ресурсами (в том числе исключение того, что работники могут использовать их в корыстных целях) |
| Цель инвентаризации | Проверка наличия IT-активов организации и состояния ее финансовых обязательств на определенную дату путем сличения фактических данных с данными бухгалтерского учета | Понимание влияния IT-активов на предоставление IT-услуги или продукта | Управление информационной безопасностью IT-активов |
| Пример используемого инструментария | Присвоение инвентарных номеров и нанесение их на IT-активы | База данных конфигурационных единиц (CMDB) | Система управления событиями и информацией о безопасности (SIEM-система) |
| Ценность информации для анализа защищенности | Низкая | Средняя | Высокая |

Один и тот же IT-актив может быть рассмотрен в различных системах учета и цели учета у них различаются, поэтому ценность результатов также разная.

# Методы проведения инвентаризации IT-активов в интересах результативной ИБ

Существуют следующие методы инвентаризации IT-активов:

1. Анализ информации, собранной из различных систем учета IT-активов, в том числе бухгалтерских.
2. Анализ архитектуры целевых систем, в том числе понимание их интеграционных взаимодействий, и анализ архитектуры корпоративной сети.
3. Анализ сети организации, в том числе сканирование доступных беспроводных точек доступа и обнаружение доступных для подключения сетевых розеток.
4. Анализ используемых облачных сервисов.
5. Анализ договоров с поставщиками IT-услуг.

# Как провести инвентаризацию IT-активов

Для проведения инвентаризации необходимо выполнить следующие восемь шагов.

| **Шаг** | **Описание шага** |
| --- | --- |
| Шаг 1. Определение рабочей группы по проведению инвентаризации | Для проведения инвентаризации создается рабочая группа, чей состав определяется в зависимости от размера организации и должен включать IT-специалистов и экспертов ИБ |
| Шаг 2. Анализ данных, полученных из различных систем учета IT-активов | В организации могут существовать различные системы учета IT-активов. Данные из этих систем учета должны быть проанализированы для понимания IT-инфраструктуры организации (например, из бухгалтерских систем можно взять имеющийся учет IT-активов, а также выявить обязательства перед поставщиками IT-услуг) |
| Шаг 3. Анализ архитектуры целевых систем из перечня недопустимых событий | Документация по архитектуре целевых систем из перечня недопустимых событий может послужить хорошим источником информации об IT-активах (компонентах целевых систем). Анализ этой документации поможет определить IT-активы и их роли в функционировании целевых систем |
| Шаг 4. Сканирование сети организации и инвентаризация ПО | Производится сканирование сетевого периметра и внутренней сети организации и инвентаризация установленного ПО. Используя сетевой сканер, можно выявить все активные узлы, находящиеся во внутренней сети и на периметре сети компании. Для сканирования рекомендуется использовать специализированные решения следующих классов:  - сканеры сети (например, Nmap);  - сканеры уязвимостей (например, MaxPatrol VM);  - сканеры беспроводных сетей (например, Aircrack-ng);  - специализированное или общесистемное ПО для инвентаризации ПО (например, OSC Inventory или Microsoft Configuration Manager).  Иногда можно использовать специализированные решения, которые имеют функцию сканирования и инвентаризации ПО (например, Kaspersky Security Center) |
| Шаг 5. Анализ используемых облачных сервисов | Все используемые облачные сервисы должны быть выявлены и проанализированы на предмет их связи с IT-инфраструктурой организации. Выявить облачные сервисы можно:  - В ходе интервьюирования работников IT-функции.  - Через анализ договоров с провайдерами облачных сервисов.  - Через анализ межсетевых взаимодействий с инфраструктурой облачных сервисов |
| Шаг 6. Анализ договоров с поставщиками IT-услуг | Договоры с поставщиками IT-услуг могут предоставить информацию об используемых IT-активах и потребляемых IT-услугах. Объем информации зависит от объема передачи IT-инфраструктуры на аутсорсинг |
| Шаг 7. Определение владельцев IT-актива | Для каждого IT-актива должен быть определен владелец IT-актива |
| Шаг 8. Формирование результатов инвентаризации IT-активов | Все результаты инвентаризации должны быть зафиксированы в форме отчета и объединены в реестр IT-активов, который должен содержать следующие поля:  - номер актива;  - наименование IT-актива;  - краткое описание (сервисы, службы, ПО, СЗИ);  - IP-адрес (при наличии) / MAC-адрес;  - тип IT-актива |

Результаты инвентаризации IT-активов могут быть использованы для определения ключевых систем и точек проникновения. Отчет должен содержать описание использованных методов и основных результатов, включающих реестр IT-активов. Объем и наполнение такого отчета зависят от масштаба IT-инфраструктуры организации.