ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ И ЗАЩИТА ИНФОРМАЦИИ

Инвентаризация информационных систем

Федоров Дмитрий Николаевич
dnf@dnf.su

VI

РАЗДЕЛЫ ТЕМЫ

- Инвентаризация информационных систем
- Классификация информационных систем
- Роли и ответственность субъектов
- Принципы распределения прав и ответственности
- Модель информационных потоков

Раздел 1

ИНВЕНТАРИЗАЦИЯ ИНФОРМАЦИОННЫХ СИСТЕМ

ВВЕДЕНИЕ

- Данная тема относится в области информационной безопасности, называемой "Анализ и управление рисками".
- Прежде чем начинать строить защиту информационного пространства, необходимо перейти от абстрактных понятий "объект/субъект" к конкретным информационным системам или, проще говоря, ответить на вопрос: а что мы будем защищать?

ОБЩИЙ ХАРАКТЕР ИНВЕНТАРИЗАЦИИ ИНФОРМАЦИОННЫХ СИСТЕМ

- Инвентаризация — в данном случае это составление списка систем, т. е. объектов, которые будут подлежать защите, и субъектов, которые задействованы в данном информационном пространстве, и будут влиять на информационную защиту системы.
- При этом необходимо не просто составить список, а указать ряд особенностей той или иной системы с точки зрения информационной безопасности. Чем подробнее сделать это на начальном этапе, тем легче будет дальше производить уточнения и строить окончательную модель защиты.
- Данная работа обычно инициируется службой информационной безопасности, но выполняется обычно с привлечением специалистов других служб (администратор системы или ее активные пользователи).

СПОСОБ ПРОВЕДЕНИЯ ИНВЕНТАРИЗАЦИИ

- На первом этапе уполномоченный специалист службы информационной безопасности составляет, при необходимости консультируясь с подразделением информационных технологий:
  - общий список объектов/систем и связанных с ними субъектов.
  - затем в этот список вносятся первичные характеристики объектов с целью описать их именно с точки зрения информационной безопасности.
- На следующем этапе начинается работа с администраторами, пользователями и/или бизнес-менеджерами объектов и систем. В рамках заданных специалистом по безопасности характеристик они производят уточнения и дополнения описаний объектов, с тем чтобы описать де-факто сложившиеся процедуры и способы работы с системой для выявления в дальнейшем возможных уязвимостей и угроз. Извлечение данных о субъектах специалист по безопасности может производить самостоятельно, опираясь на данные, полученные из описаний работы с объектами/системами, либо он может выделить его в отдельный раздел, ориентированный только на субъектов.

СХЕМА ПРОВЕДЕНИЯ ОБСЛЕДОВАНИЯ

- Общее знакомство с системой, визуальный осмотр физического размещения, отдельных компонент или составляющих.
- Предварительная беседа с администратором/менеджером об общем направлении функционирования системы.
- Ознакомление с документацией по информационной системе.
- Составление описания системы с точки зрения информационной безопасности.
- Уточнение описания на основе работы с документацией и с привлеченными специалистами.

ПАРАМЕТРЫ СТРУКТУРИРОВАНИЯ ХАРАКТЕРИСТИК СИСТЕМЫ

- аппаратное обеспечение информационной системы (компьютеры, модемы, маршрутизаторы, мосты, повторители, принтеры и прочие периферийные устройства);
- сетевое обеспечение (сетевые кабели, разъемы, розетки, коннекторы и т. п.);
- системное программное обеспечение (операционная система, другие средства создания среды работы, например, программы резервного копирования или СУБД);
- прикладное программное обеспечение, т. е. программы, выполняющие собственно функции производственные, вспомогательные и сопутствующие производству;
- организационное обеспечение, т. е. пользователи или субъекты системы и их функциональные обязанности в системе;
- нормативное обеспечение — правила и инструкции работы с системой, возможно, отдельные выдержки из них;
- данные — информация, которая используется в работе системы в ее производственном значении.

ЧТО СЧИТАТЬ ОБЪЕКТОМ СИСТЕМЫ

Необходимо определиться с тем, что считать отдельным объектом системы, подлежащим защите.

- Отдельный компьютер?
- Отдельный логический модуль?
- Если взять в качестве примера систему с трехзвенной архитектурой (клиент—сервер приложений—сервер данных), то в зависимости от особенностей, классификация может быть различной. Можно посчитать всю систему единым объектом, а можно каждое звено рассматривать отдельно (получив три объекта).

С ЧЕГО НАЧАТЬ: НОРМАТИВНЫЕ ДОКУМЕНТЫ И КРУГ РЕСПОНДЕНТОВ

С ЧЕГО НАЧАТЬ: НОРМАТИВНЫЕ ДОКУМЕНТЫ И КРУГ РЕСПОНДЕНТОВ

- Перед началом инвентаризации необходимо разработать, согласовать и утвердить порядок и методику проведения обследования. Этот документ (или документы) должен содержать цели и принципы проведения данного мероприятия, с тем чтобы они были прозрачны для тех, кто будет вовлечен в процесс
- В методической части документа должно быть описано, что нужно сделать привлеченным специалистам, чтобы выполнить свою работу. Целесообразно укомплектовать документ в качестве приложения анкетой, которую структурировать таким образом, чтобы максимально облегчить ее заполнение — выбор из уже имеющихся вариантов, числовые оценки и т. д.

ПРИНЦИПЫ ПРОВЕДЕНИЯ ИНВЕНТАРИЗАЦИИ

- Принцип единообразного подхода подразумевает рассмотрение любого объекта/системы с точки зрения технологии создания, обработки, хранения, отправки или приема информации.
- Принцип объективности означает подход с позиций оценки информационной безопасности при критическом анализе системы/объекта.
- Принцип многоуровневого подхода означает рассмотрение объекта/системы путем разделения его на составные части (аппаратное обеспечение, программное обеспечение и т. п.).
- Принцип сопряжения означает, что необходимо указать, от каких систем информация поступает в данную, и в какие системы информация направляется от данной.

НАПРАВЛЕНИЯ ПРОВЕДЕНИЯ ИНВЕНТАРИЗАЦИИ

- Физическое — описывает географическое расположение и размещение системы или отдельных компонент с учетом описания подсистем разграничения доступа.
- Технологическое — описывает используемые технические средства (аппаратное и программное обеспечение, алгоритмы и схемы и т. п.).
- Функциональное — описывает место системы в производственном процессе и выполняемые задачи.
- Организационное — описывает персонал, задействованный в работе системы, и его обязанности.
- Нормативное — описывает имеющиеся документы, регламентирующие работу системы.
- Информационное (в смысле данных) — описывает производственный или бизнес-характер информации, с которой работает система.

ОБЪЕМ СОБИРАЕМОЙ ИНФОРМАЦИИ (ПРИМЕР)

- Список программного обеспечения с рядом ключевых характеристик (производитель, номер версии, дата установки, назначение, если есть возможность — контрольная сумма файлов) с классификацией по параметрам:
  - категория применения (общее, специализированное, индивидуальное);
  - функциональное назначение (производственная или иного рода задача, для которой используется данное программное обеспечение);
  - принадлежность пользователю (кто управляет использованием данного программного обеспечения, т. е. его администратор);
  - размещение компонент программного обеспечения (рабочие станции, серверы);
  - способы доступа (локальный, удаленный).
- Дополнительно в порядке инвентаризации стоит предусмотреть формы документов, которые будут использованы, а именно:
  - опросные листы или анкеты — источник получения данных для анализа;
  - промежуточные документы — средства обработки данных;
  - отчеты — результат проведенного обследования.

ФИКСАЦИЯ ДЕТАЛЕЙ ПРИ РАБОТЕ ПО НАПРАВЛЕНИЯМ (1 ИЗ 5)

- По физическому размещению:
  - здание, помещение;
  - номера телефонов помещений;
  - механизмы контроля доступа в помещение и другие защитные механизмы;
  - номера или адреса сетевых точек;
  - ответственный за помещение, если таковой существует.
- По аппаратному обеспечению:
  - физическое размещение в помещении;
  - наименование фирмы-производителя;
  - серийный номер;
  - функциональное назначение в системе;
  - встроенные механизмы защиты;
  - адреса портов и прочие сетевые адреса (MAC, IP и др.);
  - ответственный за данную единицу оборудования, если есть.

ФИКСАЦИЯ ДЕТАЛЕЙ ПРИ РАБОТЕ ПО НАПРАВЛЕНИЯМ (2 ИЗ 5)

- По программному обеспечению (кроме уже указанных параметров):
  - производитель;
  - номер версии;
  - встроенные механизмы защиты;
  - статистика сбоев, если есть.
- По функциональному назначению (данный раздел очень зависит от особенностей производства, но скорее всего следующие пункты должны присутствовать):
  - какие подразделения являются потребителем данных системы;
  - кто занимается технической поддержкой системы;
  - роль системы в общем производственном цикле.

ФИКСАЦИЯ ДЕТАЛЕЙ ПРИ РАБОТЕ ПО НАПРАВЛЕНИЯМ (3 ИЗ 5)

- По организационному обеспечению:
  - функциональные и/или должностные обязанности персонала;
  - профессиональный уровень подготовки персонала (образование, дополнительное обучение);
  - существующие процедуры по **обеспечению безопасности**;
  - временной график выполнения работ в системе;
  - логические схемы движения информации между пользователями.
- По нормативному обеспечению:
  - список имеющихся документов — правил, инструкций и т. п.;
  - отдельно — документы по безопасности;
  - даты последнего внесения изменений в документы;
  - сертификаты на аппаратное и/или программное обеспечение.

ФИКСАЦИЯ ДЕТАЛЕЙ ПРИ РАБОТЕ ПО НАПРАВЛЕНИЯМ (4 ИЗ 5)

- По данным (этот раздел также очень зависит от особенностей производства, но следующие пункты обязательны вне зависимости от его специфики):
  - откуда поступают данные для системы;
  - куда поступают данные от системы;
  - какая работа с данными происходит в системе;
  - формат хранения данных в системе;
  - вид данных — первичные таблицы данных, транзакции, отчеты и т. п.;
  - логические схемы движения информации между объектами.

КОНТРОЛЬ ИНВЕНТАРИЗАЦИИ

КОМУ ВАЖЕН КОНТРОЛЬ ИНВЕНТАРИЗАЦИИ

- Аудиторы, проводящие проверку качества работы службы информационной безопасности предприятия, например, для вынесения решения об общем уровне надежности организации;
- Руководитель предприятия, проверяющий качество работы своей или, особенно, нанятой со стороны команды по созданию или совершенствованию информационной защиты;
- Привлеченная команда по созданию или совершенствованию информационной защиты для того, чтобы понять, какая работа и насколько качественно уже была проделана.

КРАТКИЙ КОНСПЕКТ ПРОВЕДЕНИЯ ТАКОЙ ПРОВЕРКИ

1. Для анализа результатов следует получить отчеты по выполненной инвентаризации, структурированные по информационным системам.
2. Если результаты инвентаризации присутствуют, необходимо ознакомиться с порядком и методикой ее проведения, а также анкетами и опросными листами, если таковые имеются. Эти документы прояснят, насколько можно доверять результатам инвентаризации в том смысле, что они не взяты из головы специалистов службы безопасности, проводивших обследование.
3. Следует обратиться к письменным результатам инвентаризации (стандартным или заранее подготовленным по запросу соответствующим специалистом) и оценить, как найденная характеристика или особенность отражена в представленных документах.

ПРИМЕРНАЯ КАТЕГОРИЯ ОЦЕНОК РЕЗУЛЬТАТОВ ПРОВЕРКИ

- В результирующих документах исследуемая система не упомянута вообще — очень плохо.
- Система описана, однако выявленная характеристика в ней не отражена, уполномоченный специалист ничего не может пояснить по этому поводу — плохо.
- Система описана, выявленная характеристика в ней не отражена, однако уполномоченный специалист без дополнительных усилий рассказывает по поводу особенностей выявленной характеристики — скорее всего формальные результаты инвентаризации просто устарели, либо оформлены не полностью.
- Система и соответствующая характеристика описаны достаточно подробно, чтобы служить основой для дальнейших оценок — инвентаризация проведена качественно.

МЕСТО ИНВЕНТАРИЗАЦИИ В ЖИЗНЕННОМ ЦИКЛЕ ПРЕДПРИЯТИЯ

- Для поддержания данных по инвентаризации в актуальном состоянии, необходимо выполнение ряда требований, а именно:
  - **служба информационной безопасности** в обязательном порядке должна быть вовлечена в процессы проектирования или приобретения новых систем, реконфигурации существующих, перемещений систем в информационном пространстве, как физически, так и логически, и во все другие процессы, которые производят изменения в существующем информационном пространстве, причем на самой ранней стадии;
  - сведения о приеме на работу новых сотрудников, перемещении по службе существующих, а также об отпусках, командировках, болезнях и увольнения сотрудников предприятия должны регулярно поступать в службу информационной безопасности.

Все материалы курса доступны для зарегистрированных пользователей Академии современных инфокоммуникационных технологий «АСИКТ»
www.acikt.ru