ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ И ЗАЩИТА ИНФОРМАЦИИ

Классификация информационных систем

Федоров Дмитрий Николаевич
dnf@dnf.su

VII

РАЗДЕЛЫ ТЕМЫ

- Терминология и постановка задачи
- Основные регламенты классификации
- Классификация информационных объектов
- Классификация средств обработки информации: стандарт CCITSE
- Контроль классификации
- Приложения

Раздел 1

ТЕРМИНОЛОГИЯ И ПОСТАНОВКА ЗАДАЧ

- Классификация субъектов и объектов информационной безопасности (ИБ), а также применяемых на предприятии средств работы с информацией — один из важнейших этапов построения комплексной системы безопасности.
- От корректности и тщательности ее проведения зависит то, насколько адекватно меры безопасности будут отражать специфику бизнес-процесса, и то, насколько удачно будут распределены материальные вложения в систему ИБ.

ОБЪЕКТЫ, СУБЪЕКТЫ И СРЕДСТВА РАБОТЫ

- Объект – информация: создаваемая, хранимая, обрабатываемая, отправляемая или принимаемая.
- Субъект - любой пользователь системы, ориентированный как на производственные или иные задачи, так и на поддержку самой системы (администратор).
- Средство работы с информацией — это набор аппаратного и программного обеспечения, с помощью которого производится работа в системе, т. е. субъекты воздействуют на объекты.

КЛАССИФИКАЦИЯ

- объектов — по степени их важности для предприятия;
- средств работы с информацией — по их способности поддерживать предопределенный уровень информационной безопасности;
- субъектов — по степени их допуска к работе с тем или иным объектом (или на том или ином средстве работы с информацией).

После проведения классификации остается только привести в соответствие три составляющих — **объект** данной категории чувствительности обрабатывается только средством соответствующей категории надежности **субъектом** соответствующей категории доступа. Если не найдено средство или субъект соответствующего уровня — нужно сделать обновление или докупить средства и произвести обучение или прием на работу новых пользователей

ОСОБЕННОСТИ ПОЛЬЗОВАТЕЛЕЙ

В современном информационном пространстве необходимо учитывать не только общий уровень благонадежности пользователя, но и такие факторы как:

- общая квалификация или способность работать в информационной системе, не внося в нее сбоев из-за человеческого фактора.
- подготовка пользователя в сфере информационной безопасности или осведомленность его в вопросах установленных процедур безопасности.

Раздел 2

ОСНОВНЫЕ РЕГЛАМЕНТЫ КЛАССИФИКАЦИИ

КРИТЕРИИ ОПРЕДЕЛЕНИЯ УРОВНЯ БЕЗОПАСНОСТИ СИСТЕМ

Словосочетания «на слуху» для специалистов информационной безопасности: "Оранжевая книга", "Красная книга", Общие критерии (Common Criteria), TCPEC, ITSEC и др.

- Оранжевая книга (DoD 5200.28-STD — Trusted Computer Systems Evaluation Criteria) — выпущенные Министерством обороны США критерии оценки уровня безопасности компьютерных систем как таковых.
- Красная книга (NCSC-TG-005 — Trusted Network Interpretation of the Trusted Computer System Evaluation Criteria) — расширение этих критериев для случаев использования компьютерных систем в информационной сети.

В РОССИИ

В России существуют свои нормативные документы Государственной технической комиссии при Президенте Российской Федерации по вопросам информационной безопасности.

- Классификация автоматизированных систем и требования по защите информации
- Показатели защищенности от несанкционированного доступа к информации
- Положение по аттестации объектов информатизации по требованиям безопасности информации и др

Раздел 3

КЛАССИФИКАЦИЯ ИНФОРМАЦИОННЫХ ОБЪЕКТОВ

СФЕРЫ ПРИМЕНЕНИЯ И ОСОБЕННОСТИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ОБЪЕКТОВ

- Пример 1. Государственное учреждение закрытого типа, аналогичное министерству обороны или службе разведки. Для таких учреждений обычно на первом месте стоит понятие **конфиденциальности**, поэтому скорее будет допущена возможность повреждения или уничтожения информации, чем ее разглашение.
- Пример 2. Банк. Если в качестве объекта выступает, например, значение суммы финансовых средств на счету клиента (остаток), то главная задача банка — **обеспечить невозможность ее несанкционированного изменения** (целостность). При этом в экстраординарных ситуациях можно пойти на временное отсутствие доступа к счету или разглашение данных.
- Пример 3. Поставщик интернет-услуг (бесплатный почтовый сервер). Обычно для такого учреждения очень важно обеспечить возможность постоянного доступа пользователей к сервису (скорость интернета пользователей так же важна). Конфиденциальность и целостность остаются также важными, но не всегда первостепенными требованиями.

Для каждой сферы возможна своя модель классификации.

Для удобства дальнейших ссылок на класс категории введем буквенно-цифровое обозначение (литера "Д" означает "доступность", "Ц" — "целостность"* "К" — "конфиденциальность", цифры возрастают с убыванием значимости критерия).

ПРИМЕРНАЯ МОДЕЛЬ (СХЕМА) КЛАССИФИКАЦИИ

- По наличию (доступность)
- По несанкционированной модификации (целостность)
- По разглашению (конфиденциальность)
- Для более сложных способов работы с объектами можно дополнительно ввести понятие важности по неотрекаемости и понятие важности по учету. Проанализировав общую схему классификации информационных объектов, несложно распространить ее и на другие понятия.

ПО НАЛИЧИЮ (ДОСТУПНОСТЬ)

- Критическая — без нее работа субъекта останавливается (ДО).
- Очень важная — без нее можно работать, но очень короткое время (Д1).
- Важная — без нее можно работать некоторое время, но рано или поздно она понадобится (Д2).
- Полезная — без нее можно работать, но ее использование экономит ресурсы (Д3).
- Несущественная — устаревшая или неиспользуемая, не влияющая на работу субъекта (Д4).
- Вредная — ее наличие требует обработки, а обработка ведет к расходу ресурсов, не давая результатов либо принося ущерб (Д5). (В определенных организациях может понадобиться и такой параметр.)

ПО НЕСАНКЦИОНИРОВАННОЙ МОДИФИКАЦИИ (ЦЕЛОСТНОСТЬ)

- Критическая — ее несанкционированное изменение приведет к неправильной работе всего субъекта или значительной его части; последствия модификации необратимы (ЦО).
- Очень важная — ее несанкционированное изменение приведет к неправильной работе субъекта через некоторое время, если не будут предприняты некоторые действия; последствия модификации необратимы (Ц1).
- Важная — ее несанкционированное изменение приведет к неправильной работе части субъекта через некоторое время, если не будут предприняты некоторые действия; последствия модификации обратимы (Ц2).
- Значимая — ее несанкционированное изменение скажется через некоторое время, но не приведет к сбою в работе субъекта; последствия модификации обратимы (Ц3).
- Незначимая — ее несанкционированное изменение не скажется на работе системы (Ц4).

ПО РАЗГЛАШЕНИЮ (КОНФИДЕНЦИАЛЬНОСТЬ)

- Критическая — разглашение информации приведет к краху работы субъекта или к очень значительным материальным потерям (КО).
- Очень важная — разглашение приведет к значительным материальным потерям, если не будут предприняты некоторые действия (К1).
- Важная — разглашение приведет к некоторым материальным (может быть, косвенным) или моральным потерям, если не будут предприняты некоторые действия (К2).
- Значимая — приносит скорее моральный ущерб, может быть использована только в определенных ситуациях (К3).
- Малозначимая — может принести моральный ущерб в очень редких случаях (К4).
- Незначимая — не влияет на работу субъекта (К5).

СТАДИИ ЖИЗНЕННОГО ЦИКЛА КАТЕГОРИЙ ИНФОРМАЦИИ

- Информация используется в операционном режиме, т. е. принимает участие в производственном цикле и бывает востребована практически постоянно.
- Информация используется в архивном режиме, т. е. не принимает непосредственного участия в производственном цикле, но периодически требуется для аналитической или другой деятельности.
- Информация хранится в архивном режиме для обеспечения соответствия требованиям сохранения (например, вышестоящей организации), практически не нужна самому предприятию.

Раздел 4

КЛАССИФИКАЦИЯ СРЕДСТВ ОБРАБОТКИ ИНФОРМАЦИИ: СТАНДАРТ CCITSE. КРАТКИЙ ОБЗОР СТАНДАРТА

ДОКУМЕНТЫ

- CCITSE (Common Criteria for Information Technology Security Evaluation — Общие критерии оценки безопасности информационных систем ОКОБИС)
- Стандарт ISO 17799 (International Security Standard — Международный стандарт по безопасности) - наследник британского стандарта BS7799

Мы рассмотрим первый документ, поскольку:

- Это качественно разработанный и продолжающий совершенствоваться документ, в создании которого принимают участие высокопрофессиональные специалисты из Великобритании, Германии, Канады, Нидерландов, США и Франции.
- По оценкам многих специалистов, этот проект может стать единым стандартом для документов такого характера, заменив собой существующие национальные стандарты.
- Что касается ISO 17799, то, к сожалению, в настоящее время его нет в свободном доступе в Интернете, поэтому его обсуждение затруднено.

СТРУКТУРА CCITSE

- Использована версия 2.1 документа CCITSE [CC1], которая доступна в Интернете. Сравнивая ее с предыдущей версией, можно предположить, что основные характеристики документа сформированы и будут перенесены в более поздние версии.
- Документ состоит из трех частей, общим размером более 600 страниц.
  - Первая часть - «Введение и общая модель»
  - Вторая часть – «Требования к функциональности безопасности»
  - Третья часть – «Требования к достоверности безопасности» (не рассматривается в курсе)

ЧАСТЬ 1: «ВВЕДЕНИЕ И ОБЩАЯ МОДЕЛЬ» - 1

- В первой части документа говорится, что данные критерии являются составной частью общего процесса оценки наряду с такими понятиями, как методика оценки и схема оценки, которые не входят в сферу рассмотрения данного документа. Вводится понятие предмета оценки (англ. Target of Evaluation — TOE), в качестве примера к которому отнесены операционная система, компьютерная сеть, распределенная система или приложение. Также указаны ссылки на понятия конфиденциальности, целостности и доступности. Кроме того здесь представлены принципы формирования целей информационной безопасности для выбора и определения требований и создания спецификаций для продуктов и систем.
- Документ разделяет потенциальных его читателей на три группы — потребитель, разработчик и специалист по оценке.

ЧАСТЬ 1: «ВВЕДЕНИЕ И ОБЩАЯ МОДЕЛЬ» - 2

- Дополнительно в этой части даны простые и понятные схематические интерпретации различных аспектов безопасности, таких как "Концепция и связи в рамках безопасности", "Концепция и связи в рамках оценки", "Модель развития предмета оценки", "Процесс оценки предмета" и др. Также определен подход к оценке путем разделения предмета на классы, семейства и компоненты, и использования требований к безопасности.

ЧАСТЬ 2: «ТРЕБОВАНИЯ К ФУНКЦИОНАЛЬНОСТИ БЕЗОПАСНОСТИ»

- Данный раздел основан на части 2 стандарта CCITSE.
- В начале документа рассмотрено соответствие между понятиями "класс", "семейство" и "компонент", определяемых по возрастанию уровня иерархии.
- Компонент — наименьшее разделяемое множество элементов, которые могут быть включены в профиль защиты или предмет безопасности (англ. Protection Profile / Security Target — PP/ST).
- Семейство — группа компонент, которые объединяются общими целями безопасности, но могут различаться способом реализации или деталями.
- Класс — группа семейств, которые объединены общей направленностью.
- При этом профиль защиты — это независимое от уровня иерархии множество требований по безопасности для предмета оценки, которое соответствует требованиям потребителя, а предмет безопасности — это множество требований и спецификаций, используемых как основа для оценки предопределенного предмета оценки.

ПАРАМЕТРЫ «КЛАССА»

Класс определяется своим:

- уникальным 3-символьным наименованием, необходимым для идентификации и определения категории,
- описанием, которое выражает общую цель или подход семейств, составляющих класс, для соответствия целям безопасности.

ПАРАМЕТРЫ «СЕМЕЙСТВА»

- Уникальное 7-символьное (три символа от класса, подчеркивание и три символа от семейства) наименование, предоставляющее информацию для определения категории функционального семейства;
- Характер — описание целей безопасности (проблемы безопасности, которые могут быть разрешены с помощью компонент семейства) и функциональных требований (сумма всех требований к компонентам);
- Уровень компонента — информация для определения соответствующего компонента в рамках семейства, его описание и взаимосвязь с другими компонентами;
- Управление — информация, необходимая для организации управления компонентом, требования к которой указаны в соответствующем классе (класс FMT — Управление безопасностью);
- Аудит — информация по событиям, подлежащим аудиту, если соответствующая информация из класса FAU (Аудит безопасности) включена.

ПАРАМЕТРЫ «КОМПОНЕНТА»

- Идентификация — информация, состоящая из уникального наименования, отображающего назначение компонента;
- Имя, предназначенное для ссылок на компонент и отображающее класс и семейство компонента; иерархических связей с другими компонентами;

КЛАССЫ И ИХ СОСТАВЛЯЮЩИЕ (СЕМЕЙСТВА)

- Класс FAU — Аудит безопасности
- Класс FCO — Коммуникации
- Класс FCS — Поддержка криптографии
- Класс FDP — Защита данных пользователя
- Класс FIA — Идентификация и аутентификация
- Класс FMT — Управление безопасностью
- Класс FPR — Сокрытие данных
- Класс FPT — Защита системы
- Класс FRU — Использование ресурсов
- Класс FTA — Доступ к предмету оценки
- Класс FTP — Доверенные пути/каналы

Раздел 5

КОНТРОЛЬ КЛАССИФИКАЦИИ

КОНТРОЛЬ КЛАССИФИКАЦИИ ИНФОРМАЦИИ

Необходимо различать понятия классификации самой информации и классификации средств работы с информацией.

- Классификация информации представляет трудность в первую очередь спецификой работы самого предприятия. Поэтому, если классификация информации на предприятии присутствует, необходимо проверить порядок проведения процесса такой классификации. Если классификация производилась на основании умозаключений только представителей службы безопасности, то она может не отражать реальной потребности в защите информационных объектов.

КОНТРОЛЬ КЛАССИФИКАЦИИ СРЕДСТВ РАБОТЫ С ИНФОРМАЦИЕЙ

- Необходимо различать классификацию, проведенную силами самого предприятия (его службой информационной безопасности) и классификацию, произведенную третьей стороной (например, производителем системы).
- Широко известные, сертифицированные на определенную категорию, системы обычно (и это указывается в сертификационном документе) категоризируются в определенной конфигурации, на определенном оборудовании, в определенной среде и при других определенных условиях. А это значит, что система, сертифицированная по классу С2, вовсе не соответствует данной категории на конкретном предприятии по различным причинам (другое оборудование, особенности или ошибки конфигурации и пр.).
- В этом случае, с одной стороны, собственная категоризация (или перекатегоризация), возможно, окажется более точной. С другой стороны, собственная категоризация может не быть такой подробной, как [CC].

НЕОБХОДИМО

- Убедиться в том, как оценивались надежность механизмов безопасности (аутентификация, криптография и др.)
- Оценить возможность управления этими механизмами, защита данных и разграничение доступа к ним, устойчивость системы к сбоям, качество документации к системе, возможные уязвимости системы и остальные параметры, которые подлежат оценке.

ПРОВЕРКА СООТВЕТСТВИЯ ИНФОРМАЦИИ СРЕДСТВАМ РАБОТЫ С НЕЙ

Когда получены категории информации и средств работы с ней или аналоги этих категорий, необходимо убедиться, что работа с информацией данного уровня чувствительности действительно производится на данном средстве с возможностью поддержания заданного уровня. Такая проверка производится обычно одним из следующих способов:

- изучением описания работы системы;
- опросом администраторов и пользователей системы;
- тестовой работой проверяющего в системе, чаще всего в сопровождении администратора системы.

- Если подтверждение соответствия уровней информация/средство работы получено, можно утверждать, что классификация произведена правильно и работа производится в соответствии с классификацией.
- Если же обнаружены расхождения, необходима дополнительная проверка (в основном опросы уполномоченных сотрудников) для определения причин расхождений и способов их устранений, вплоть до полной переклассификации всех систем.

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