П р а к т и ч е с к а я р а б о т а № 2

АНАЛИЗ УГРОЗ И УЯЗВИМОСТЕЙ БЕЗОПАСНОСТИ ТЕЛЕКОММУНИКАЦИОННОЙ СИСТЕМЫ

Цель работы. Изучить типовой алгоритм описания информационной системы. Приобрести практические навыки по его применению. Научиться идентифицировать угрозы информационной системы, их источники и методы планирования.

Краткие сведения из теории

На этапе описания информационной системы (ИС) необходимо указать цели ее создания, границы, информационные ресурсы, требования в области информационной безопасности (ИБ) и компонентов управления информационной системой и режимом ИБ.

Описание рекомендуется делать в соответствии со следующим планом:
– аппаратные средства ИС, их конфигурация;
– используемое программное обеспечение (ПО);
– интерфейсы системы, то есть внешние и внутренние связи с позиции информационной технологии;
– типы данных и информации;
– персонал, работающий в данной ИС (обязанности);
– миссия данной ИС (основные цели);
– критичные типы данных и информационные процессы;
– функциональные требования к ИС;
– категории пользователей системы и обслуживающего персонала;
– формальные требования в области ИБ, применимые к данной ИС (законодательство, ведомственные стандарты и т. д.);
– архитектура подсистемы ИБ;
– топология локальной сети;
– программно-технические средства обеспечения ИБ;
– входные и выходные потоки данных;
– система управления в данной ИС (должностные инструкции, система планирования в сфере обеспечения ИБ);
– существующая система управления в области ИБ (резервное копирование, процедуры реагирования на нештатные ситуации, инструкции по ИБ, контроль поддержания режима ИБ и т. д.);
– организация физической безопасности;

– управление и контроль внешней по отношению к ИС средой (климатическими параметрами, электропитанием, защитой от затоплений, агрессив- ной среды и т. д.).

Активы организации – все, что имеет ценность для организации в интересах достижения целей деятельности и находится в ее распоряжении. К активам организации могут относиться:

– информационные активы, в том числе различные виды информации, циркулирующие в информационной системе (служебная, управляющая, аналитическая, деловая и т. д.) на всех этапах жизненного цикла (генерация, хранение, обработка, передача, уничтожение);

– выпускаемая продукция и/или оказываемые услуги;

–аппаратура: процессоры, модули, клавиатуры, терминалы, рабочие станции, персональные компьютеры, принтеры, дисководы, коммуникационные линии, терминальные серверы, маршрутизаторы;

–программное обеспечение: исходные тексты, объектные модули, утилиты, диагностические программы, операционные системы, коммуникационные программы;

–данные: обрабатываемые, непосредственно доступные, архивированные, сохраненные в виде резервной копии, регистрационные журналы, базы данных, передаваемые по коммуникационным линиям;

– пользователи, обслуживающий персонал;

– документация: по программам, по аппаратуре, системная, по административным процедурам;

– расходные материалы: бумага, формы, красящая лента, магнитные носители.

Для системы, находящееся в стадии проектирования, и для уже существующей системы характер описания и степень подробности ответов будут разными. В первом случае (стадия проектирования) достаточно указать общие требования в области ИБ.

Анализ угроз информационной безопасности.

Под угрозой информационной безопасности объекта понимаются возможные воздействия на него, приводящие к ущербу. Источник угрозы – это потенциальные антропогенные, техногенные или стихийные носители угрозы безопасности.

Уязвимость объекта – это присущие объекту причины, приводящие к нарушению безопасности информации на объекте.

А т а к а – это возможные последствия реализации угрозы при взаимодействии источника угрозы через имеющиеся уязвимости. Атака – это всегда пара «источник – уязвимость», реализующая угрозу и приводящая к ущербу.