Лекция № 4
Система информационной безопасности

Система информационной безопасности есть такое состояние организации, в котором информационная структура способна успешно, устойчиво и непрерывно функционировать развиваясь в условиях интенсивного воздействия внешних и внутренних факторов, оказывающих на нее как стабилизирующее, так и деструктивное воздействие.

Инсайдеры вступающие в преступный сговор с хакерами являются, безусловно, самой опасной угрозой для устойчивого и непрерывного функционирования информационной структуры. Для защиты от внутренних угроз необходим целый комплекс различных мер.

Мы представляем этот комплекс, на первом этапе, в двух направлениях.

Первое направление: основными организационными мерами защиты информационных ресурсов является разработка и четкое следование общей государственной политике информационной безопасности.

Во главу угла поставлена модель противоборства собственника и злоумышленника, в частности инсайдера, причем сразу же делаются основные акценты «Наибольшими возможностями для нанесения ущерба [организации]… обладает ее собственный персонал. В этом случае содержанием деятельности злоумышленника является нецелевое использование предоставленного контроля над информационными активами, а также сокрытие следов своей деятельности. Внешний злоумышленник скорее да, чем нет, может иметь сообщника (ов) внутри организации».

Для борьбы с угрозами стандарты рекомендуют не только проверенные временем методики типа моделирования угроз, создания политики и системы управления информационной безопасностью, но и выделение службы безопасности в отдельное подразделение в рамках акмеологической службы.

Разработчики стандартов предупреждают, что «любые защитные меры в силу ряда объективных причин со временем имеют тенденцию к ослаблению своей эффективности, в результате чего общий уровень безопасности может снижаться». То есть организациям необходимо управлять информационной безопасностью, чтобы предотвратить возрастание рисков создавая соответствующие системы.

Однако ни один стандарт не дает четких рекомендаций по механизмам внутреннего контроля собственного персонала, это вполне объяснимо, так

как нормативные акты содержат лишь общие положения. Практически вся линейка книг COBIT5: Enabling Information изобилует рекомендательно назидательными оборотами речи, не давая ни одного практического совета по оценке уровня компетентности персонала обслуживающего критические узлы инфраструктуры. Таким образом, тема внутреннего контроля не скоро будет раскрыта и вероятно выйдет в других, сейчас разрабатываемых стандартах.

Второе направление: деятельность по акмеологическому отбору и сопровождению персонала служб информационной безопасности. Проведение постоянного акмеологического мониторинга сотрудников как подразделений информационной безопасности, так и пользователей системы – обязательная мера, которая должна входить в комплексную программу обеспечения информационной безопасности организации.

Создание системы оценки личности, одинаково сбалансированной с точки зрения точности, объективности, простоты и понятности позволит неукоснительно следовать принципам «знай своего служащего», нашедшим отражение и в международных, и в отечественных стандартах безопасности. Это положение нашло свое отражение в стандарте Банка России «Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Общие положения» (СТО БР ИББС-1.0–2006).

Основными задачами системы Информационной Безопасности являются:

- Проведение аудита системы безопасности информационно-вычислительной инфраструктуры с целью выработки единой Политики Информационной Безопасности.
- Организация системы менеджмента ИБ.
- Определение ценности, критичности и жизненного цикла обслуживаемых информационных ресурсов.
    - ✓ человеческий;
    - ✓ информационный;
    - ✓ технологический;
    - ✓ программный.
- Личностно-профессиональная диагностика специалистов в соответствии с ценностью, критичностью и жизненным циклом соответствующего ресурса.

- Расчет вероятности риска утечки конфиденциальной информации и возможных материальных потерь (в том числе и через человеческий ресурс).
- Финансово экономическое обоснование внедрения изменений в систему ИБ.
- Постоянный технический мониторинг системы – контроль информационных, физических, программных ресурсов

Работа по проведению анализа системы информационной безопасности проводится с использованием подхода полного анализа исследуемой инфраструктуры.

Данный подход (аудит) применяется в случае повышенных требований в области информационной безопасности. Здесь производится оценка ценности ресурсов, определяется характеристика рисков и уязвимостей ресурсов.

В данном случае используется следующая концептуальная модель построения системы информационной безопасности, основанная на проведении анализа информационных рисков исследуемого объекта (рис. 3.1).

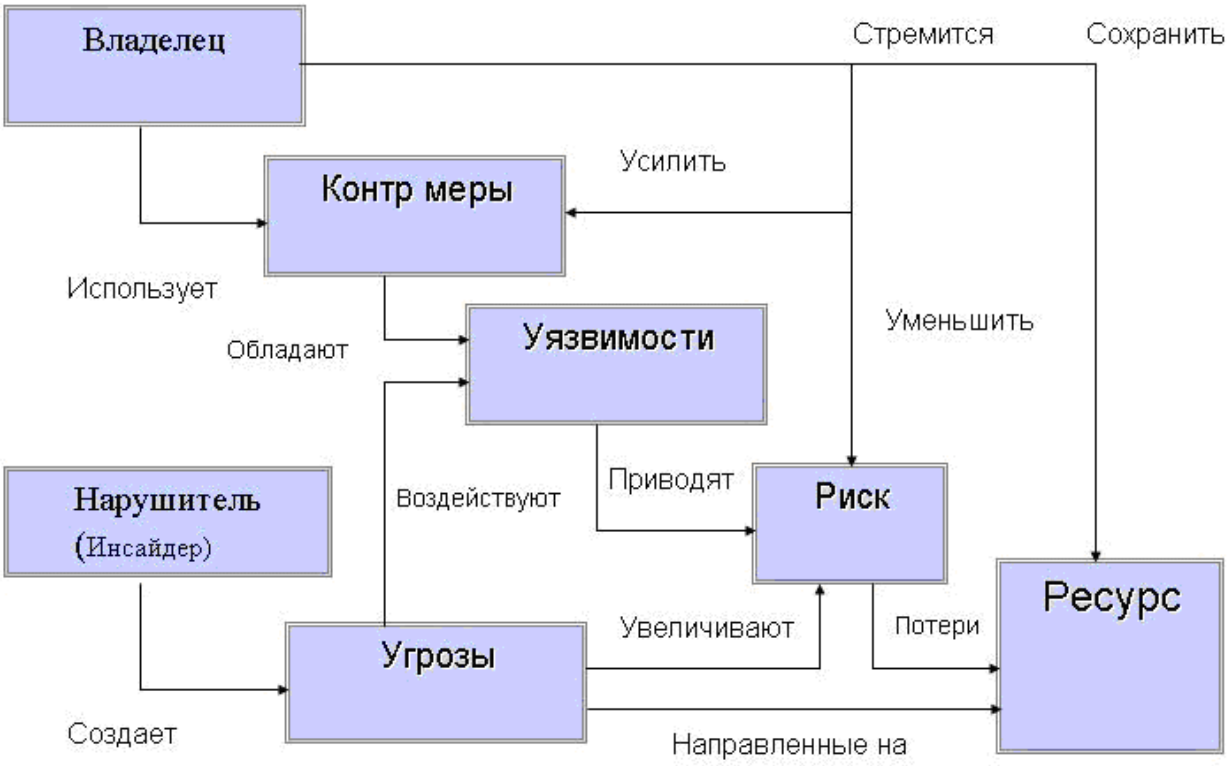

Рис. 3.1 Модель построения системы ИБ. Европейский стандарт ISO/IEC 15408

Данная модель отражает сложившиеся на практике концептуальные основы Российского подхода к обеспечению информационной безопасности, а также полностью соответствует европейскому стандарту ISO/IEC 15408 «Информационная технология — методы защиты — критерии оценки информационной безопасности» и «международному стандарту безопасности информационных систем» ISO 17799. А также стандарту банка России «Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Общие положения» (СТО БР ИББС-1.0–2006), где впервые была обозначена проблема *инсайдеров*, собственных сотрудников банка.