Лекция № 5
Человеческий ресурс в системе информационной безопасности

«Наибольшими возможностями для нанесения ущерба [организации]… обладает ее собственный персонал. (Инсайдер). В этом случае содержанием деятельности злоумышленника является не целевое использование предоставленного контроля над информационными ресурсами, а также сокрытие следов своей деятельности. Внешний злоумышленник скорее да, чем нет, может иметь сообщника (ов) внутри организации».

Внешним злоумышленником или нарушителем может быть террорист, уголовный элемент, конкурент, уголовный рецидивист, вступивший в преступный сговор с инсайдером через хакера.

В настоящее время для борьбы с угрозами применимы не только проверенные временем методики моделирования угроз, но также необходимо внедрение постоянного акмеологического мониторинга личностно-профессионального развития сотрудников (человеческого ресурса) как составной части политики Информационной Безопасности.

Представленная модель информационной безопасности устанавливает отношения между совокупностью объективных внешних и внутренних факторов и их влияния на состояние информационной безопасности на объекте и сохранностью (защищенностью) материальных или информационных ресурсов.

Одна из главных задач, решаемая в ходе проведения работы, – оценивание риска в информационной системе по каждому из информационных ресурсов (рис 3.2).

На этапе физического описания объекта определяется, наличие и состояние ресурса. Изучается его ценность, критичность и жизненный цикл каждого из отдельно взятых ресурсов.

Ресурсы объекта информатизации – это используемые информационные технологии, собственно информация и потоки данных, а также специалисты, управляющие данными ресурсами.

Защите подлежат в первую очередь информационные ресурсы, критичные с точки зрения информационной безопасности.

Под информационным ресурсом объекта информатизации понимаются прикладные автоматизированные информационные системы хранения и

обработки баз данных, а также персонал, обслуживающий информационную структуру организации (инсайдеры).

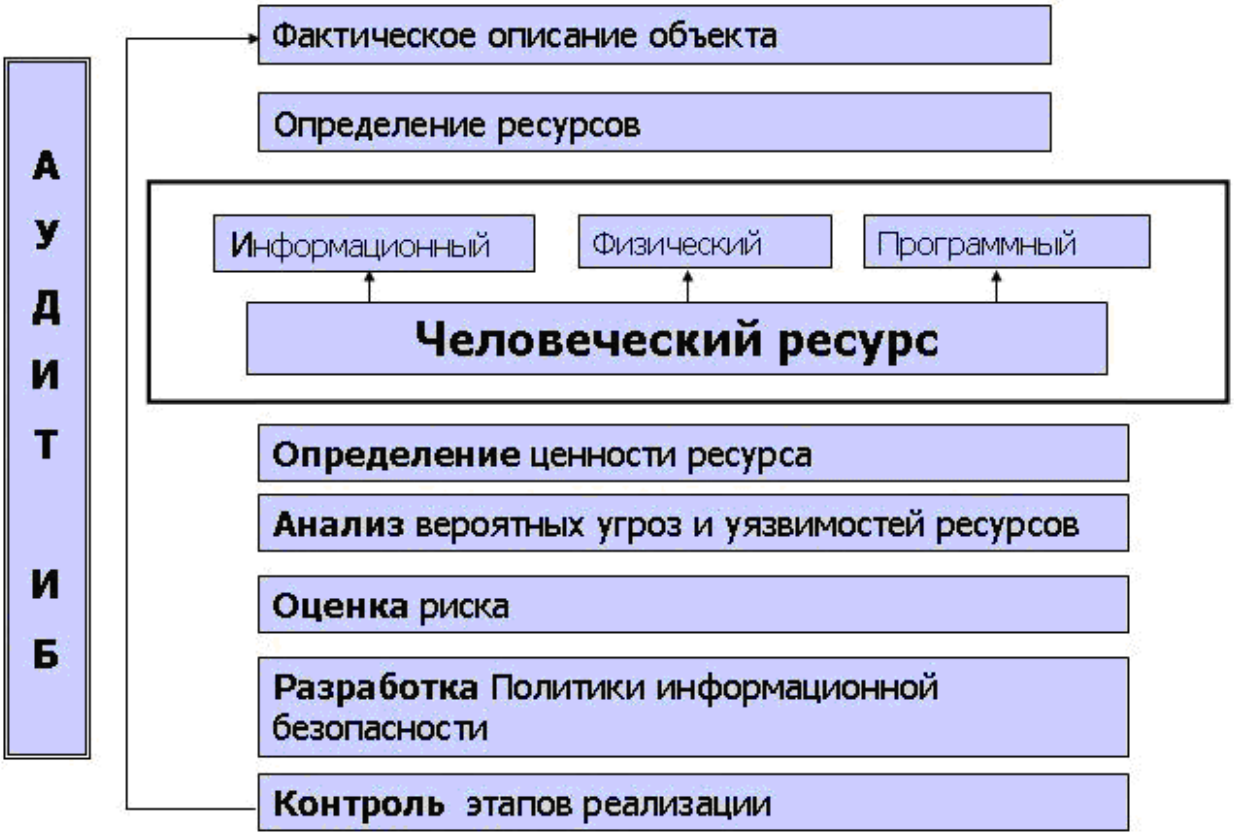

Рис. 3.2 Порядок оценки ресурсов информационной системы

Под физическим ресурсом объекта информатизации понимается физическое наличие компьютеров, серверов, сетевого и коммутационного оборудования.

Программный ресурс состоит из комплекса программ осуществляющих управление, хранение, обработку, данных, а также управления информационными и физическими ресурсами.

Определение ценности информационных ресурсов является необходимым элементом анализа риска. Человеческий ресурс на сегодняшний день самый важный из основных ресурсов в системе информационной безопасности. Как видно из рисунка, все четыре ресурса взаимосвязаны между собой. И в любом случае человеческий фактор управляет, влияет и обеспечивает жизненные циклы ресурсов.

Результатом аудита системы является итоговая оценка вероятности суммы рисков, в том числе и с учетом человеческого фактора

(потенциального ущерба от реализации информационных угроз). На основе обобщенных данных предлагается комплекс мероприятий по повышению уровня информационной безопасности объектов информатизации. Разрабатывается Политика Информационной Безопасности объекта информатизации. Заключительным этапом является мониторинг – постоянный контроль этапов реализации Политики Информационной Безопасности, частью которой является постоянный мониторинг сотрудников на предмет их компетентности.

В соответствии с принятой концептуальной моделью системы информационной безопасности, основным дестабилизирующим фактором, создающим угрозы информационной безопасности являются нарушители информационной безопасности, как внутренние, так и внешние. Представленные в таблице 3.1.

Внешние нарушители (аутсайдеры)	**Внутренние нарушители** (инсайдеры)
Преступные организации	Системные администраторы
Конкурирующие организации	Программисты
Клиенты	Пользователи (работники)
Хакеры	Руководители
	Сотрудники, уволенные с работы

Таблица 3.1.

Моделирование профиля нарушителя позволяет сформировать представление о его возможностях, направлениях его действий и в конечном итоге, построить вероятностную модель воздействий (угроз) нарушителя на систему информационной безопасности.

Каждая группа вероятных нарушителей анализируется отдельно. В частности, по следующим параметрам:

- категории лиц, к которым может принадлежать нарушитель;
- цели действий нарушителя;
- способы достижения целей и порядок решения задач;
- сведения, необходимые нарушителю и период их актуальности;
- квалификация нарушителя и его техническая оснащённость;
- характер действий нарушителя и наносимый ущерб.

Ресурсы объекта информатизации – это используемые информационные технологии, собственно информация и потоки данных, а также специалисты, управляющие данными ресурсами. Защите подлежат в первую очередь информационные ресурсы, *критичные с точки зрения информационной безопасности.* Под информационным ресурсом объекта информатизации понимаются прикладные автоматизированные информационные системы хранения и обработки баз данных, а также персонал, обслуживающий информационно-вычислительную инфраструктуру (инсайдеры). Человеческий ресурс на сегодняшний день самый важный из основных ресурсов в системе информационной безопасности. Все четыре ресурса (рис. 3.3) взаимосвязаны между собой и в любом случае человеческий фактор управляет, влияет и обеспечивает жизненные циклы ресурсов.

В человеческий ресурс входит руководство, аппарат управления, менеджеры высшей категории. Также пользователи системы, служащие, имеющие доступ к информационным ресурсам на основании распоряжений о допуске.

В данной работе нас будет интересовать не только инженерный состав, но и в первую очередь руководители ИТ структур.

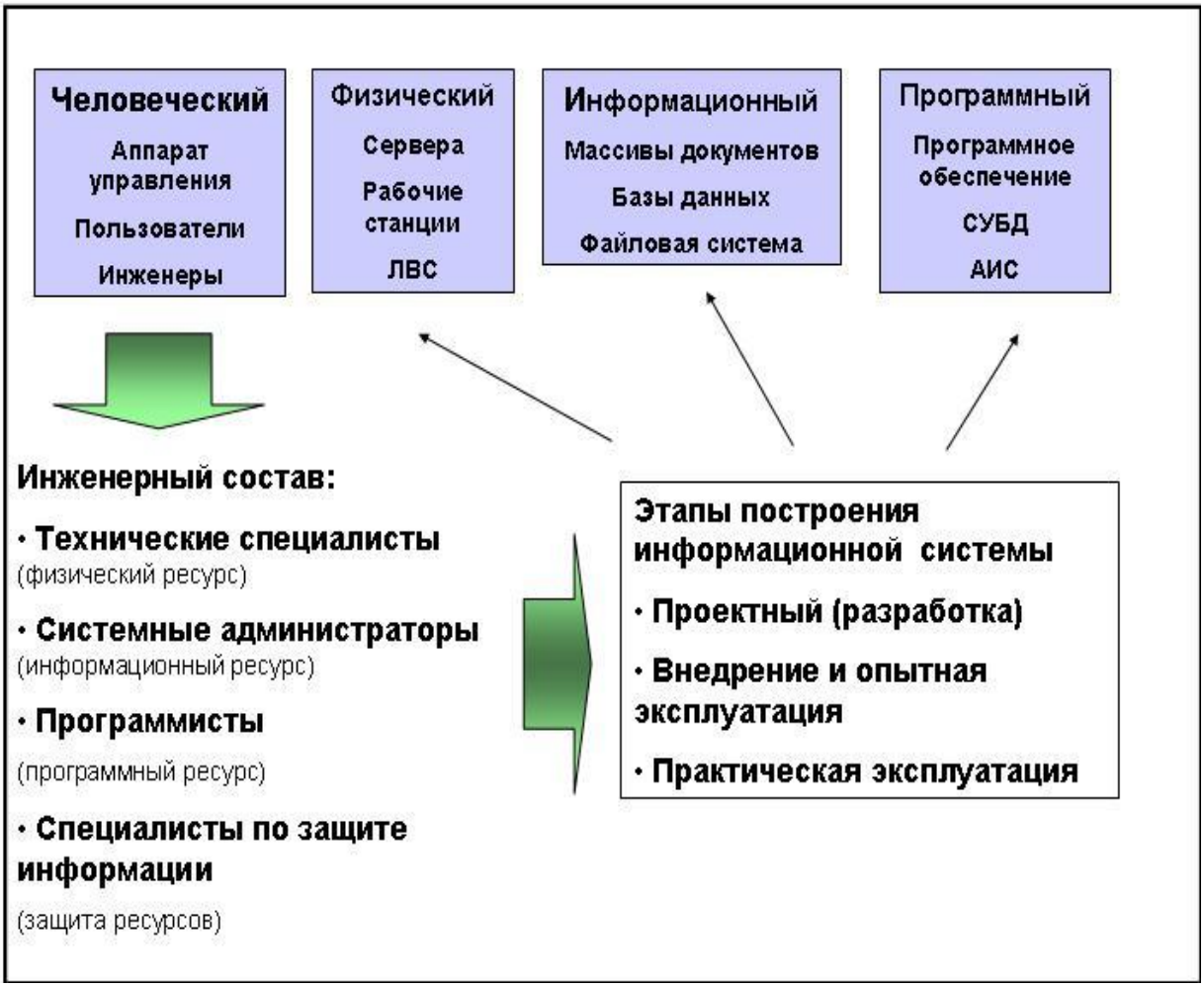

Рис. 3.3 Оценка человеческого ресурса по этапам разработки и эксплуатации системы/

Инженерный состав, в свою очередь, подразделяется на следующие категории:

- технические специалисты, обслуживающие физические ресурсы, сервера, рабочие станции, коммутационное и сетевое оборудование;

- программисты, основной задачей которых является поддержание в работоспособном состоянии программное обеспечение, а также написание и внедрение отдельных, самостоятельно написанных и откомпилированных блоков программ;

- системные администраторы, управляющие системой ресурсов на основании прописанных правил и законов работы информационно-вычислительной системы;

- специалисты по защите информации, выполняющие работы, связанные с обеспечением комплексной защиты информации на основе разработанных программ и методик.