Разработка политики безопасности организации

Организационно-правовое обеспечение информационной безопасности

Выполнил Рывкин Л.С.
Группа КС-82-10

Главные темы

- Что такое политика безопасности
- Что нужно, чтобы её составить
- Каким образом её составить

Информационная безопасность организации

Это состояние защищённости интересов организации в условиях угроз в информационной сфере

Защищённость организации достигается обеспечением

- Конфиденциальности
- Целостности
- Доступности

Её информационных активов

Активы – то, чем организация располагает и что использует в своей деятельности

Политика безопасности

Это система документов, регламентирующих деятельность обеспечения информационной безопасности в организации

Набор документов должен отражать:

- Цели – то, чего необходимо достичь обеспечением информационной безопасности
- Стратегии – способы достижения поставленных целей.
- Политики – различные правила, которые следует соблюдать при реализации стратегий
- Процедуры – это методы реализации политик

I уровень

Политика ИБ

II уровень

Положение
о конфиденциальной
информации

Положение
о службе ИБ

III уровень

Инструкции

Процедуры

Регламенты

С чего начать: анализ угроз

Угроза обладает способностью наносить ущерб активам и, следовательно, организации в целом

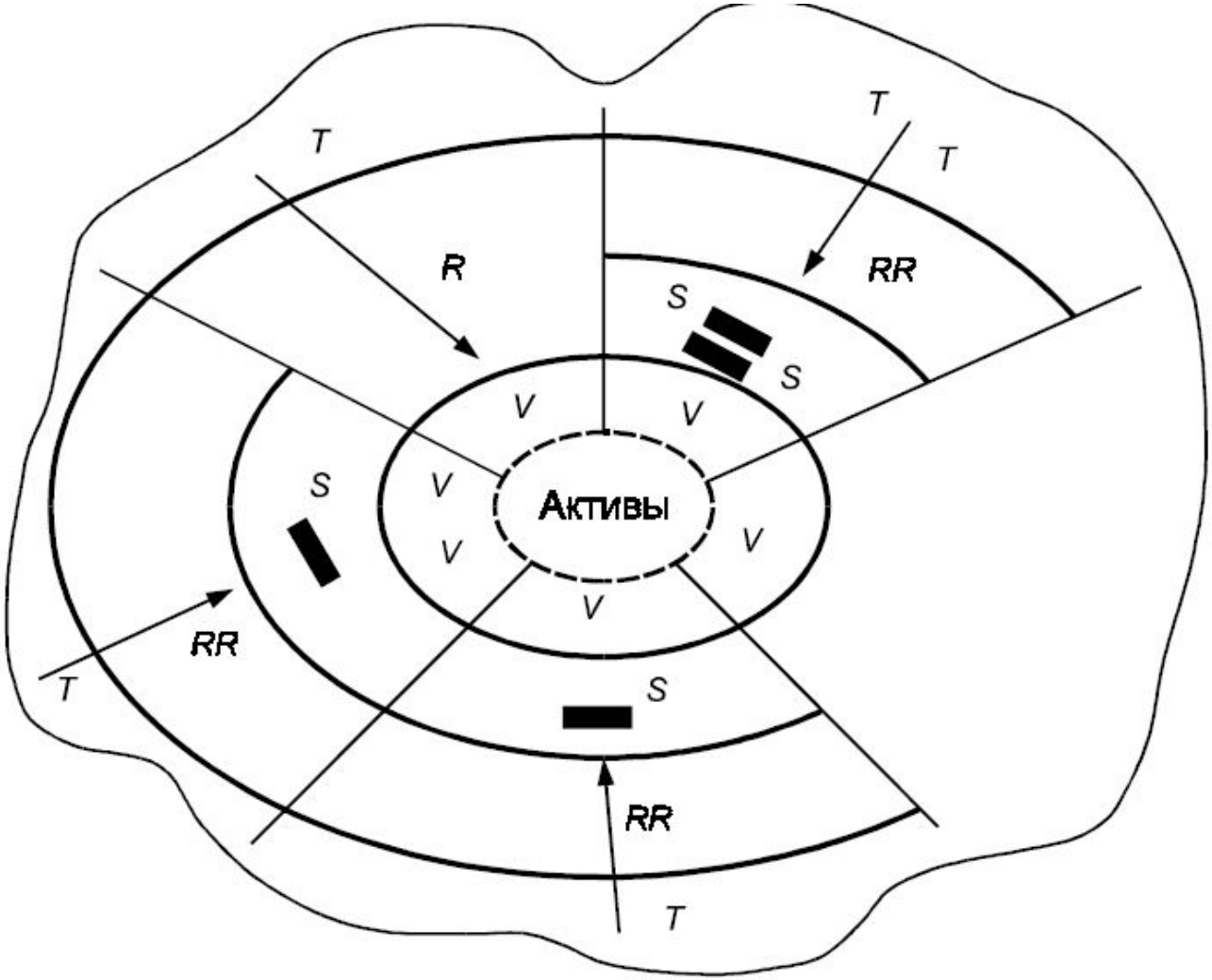
Ущерб активам может быть нанесен только при наличии у них уязвимости

Уязвимость – это недостаток в системе, при котором возможно реализация угрозы – инцидента информационной безопасности. Наличие уязвимость даёт шанс угрозе проявить себя с некоторой вероятность, то есть создаёт риск

Риск – это влияние неопределённостей на процесс достижения поставленных целей

Последовательность действий

- Идентификация активов
- Определение угроз, уязвимостей, их комбинаций
- Количественная оценка рисков
- Определение защитных мер
- Оценка остаточного риска



R — риск; *RR* — остаточный риск; *S* — защитная мера; *T* — угроза; *V* — уязвимость актива

Разработка политики безопасности

I. Цели, которые преследует ИБ организации
II. Стратегия ИБ организации
III. Набор мер обеспечения ИБ организации
IV. Инструкции

Цель ИБ организации

Цель – высокоуровневая задача, обычно в очень широких рамках.

Пример:

Организация – оператор базы персональных данных.

Тогда одна из целей, которая может стоять перед ИБ – доказать потенциальным клиентам, что их персональные данные хорошо защищены.

Стратегия ИБ

Ответить на ряд вопросов и распределить приоритеты обеспечения ИБ.

Примеры:

- В каком состоянии находится информационная безопасность сейчас, и в каком направлении необходимо двигаться дальше?
- Какие из задач информационной безопасности наиболее приоритетны?
- Какие задачи краткосрочные, а какие – долгосрочные?

Меры ИБ

Шаг №1: Определение базового набора мер

Базовый набор мер определяется задачами, поставленными перед ИБ.

К примеру, перед организацией стоит вопрос обеспечения безопасности персональных данных пользователей.

Существует ряд стандартов, в которых содержится набор мер по обеспечению безопасности ПД для обеспечения некоторого установленного уровня защищённости. Базовый набор мер можно взять из них

Меры ИБ

Шаг №2: Адаптация набора мер с учетом структурно-функциональных характеристик информационной системы, информационных технологий, особенностей функционирования информационной системы

В том числе исключение из базового набора мер, непосредственно связанных с информационными технологиями, не используемыми в информационной системе

Меры ИБ

Шаг №3: Уточнение перечня мер с учётом актуальных угроз

Уточнение адаптированного базового набора мер по обеспечению безопасности с учетом не выбранных ранее мер, приведенных в приложении к настоящему документу, в результате чего определяются меры по обеспечению ИБ, направленные на нейтрализацию всех актуальных угроз для конкретной информационной системы.

Инструкции ИБ

За реализацию политики ИБ отвечают должностные инструкции, которые могут содержать алгоритм пошаговой реализации конкретной меры выбранным способом; различные регламенты, к примеру, регламент оценки рисков, или регламент проведения внутреннего аудита.

Выбор реализации зависит от экономической целесообразности, от субъективных факторов (личные предпочтения при выборе того или иного программного продукта), а может быть и строго регламентирован законодательно (использование только сертифицированных средств). Также он может быть обоснован анализом каких-либо характеристик, наиболее подходящих для применения. Какое-либо средство может быть предпочтено другим потому, что оно апробировано, надёжно, или хорошо сочетается с информационной системой в целом.

Заключение

Обеспечение информационной безопасности – это процесс, непрерывный для всего времени функционирования организации. Со временем происходит внедрение новых технологий, которые порождают всё новые уязвимости.

Поэтому разработка политики информационной безопасности должна иметь циклический характер; необходимо, чтобы существующая политика совершенствовалась и пересматривалась, и только так она будет соответствовать возложенным на неё задачам.

Спасибо за внимание