УДК 004.056.5

УПРАВЛЕНИЕ СИСТЕМОЙ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Яковлев П.С., Кулистов Е.В., Булакина О.Н., Булакина А.Н., Максименко Л.Н., Хрусталев В.И.
Научный руководитель – профессор Булакина Е.Н.

Сибирский федеральный университет

Целями системы информационной безопасности (ИБ) являются:

−обеспечение устойчивого функционирования объекта, предотвращение угроз его безопасности, защита законных интересов “Заказчика” от противоправных посягательств, недопущение хищения финансовых средств, разглашения, утраты, утечки, искажения и уничтожения служебной информации, обеспечение нормальной производственной деятельности всех подразделений объекта;

−повышение качества предоставляемых услуг и гарантий безопасности имущественных прав и интересов клиентов.

Достижение целей возможно в ходе решения следующих основных задач:

−отнесение информации к категории ограниченного доступа (служебной тайне);

−прогнозирование и своевременное выявление угроз безопасности информационным ресурсам, причин и условий, способствующих нанесению финансового, материального и морального ущерба, нарушению его нормального функционирования и развития;

−создание условий функционирования с наименьшей вероятностью реализации угроз безопасности информационным ресурсам и нанесения различных видов ущерба;

−создание механизма и условий оперативного реагирования на угрозы информационной безопасности и проявления негативных тенденций в функционировании, эффективное пресечение посягательств на ресурсы на основе правовых, организационных и технических мер и средств обеспечения безопасности;

−создание условий для максимально возможного возмещения и локализации ущерба, наносимого неправомерными действиями физических и юридических лиц, ослабление негативного влияния последствий нарушения информационной безопасности на достижение стратегических целей.

Модель построения системы информационной безопасности

При выполнении работ можно использовать следующую модель построения системы информационной безопасности (рисунок 1), основанную на адаптации ОК (ISO 15408) и проведении анализа риска (ISO 17799).

Эта модель соответствует специальным нормативным документам по обеспечению информационной безопасности, принятым в Российской Федерации, международному стандарту ISO/IEC 15408 "Информационная технология - методы защиты - критерии оценки информационной безопасности", стандарту ISO/IEC 17799 "Управление информационной безопасностью", и учитывает тенденции развития отечественной нормативной базы (в частности, Гостехкомиссии РФ) по вопросам информационной безопасности.

Представленная модель информационной безопасности - это совокупность объективных внешних и внутренних факторов и их влияние на состояние

информационной безопасности на объекте и на сохранность материальных или информационных ресурсов.

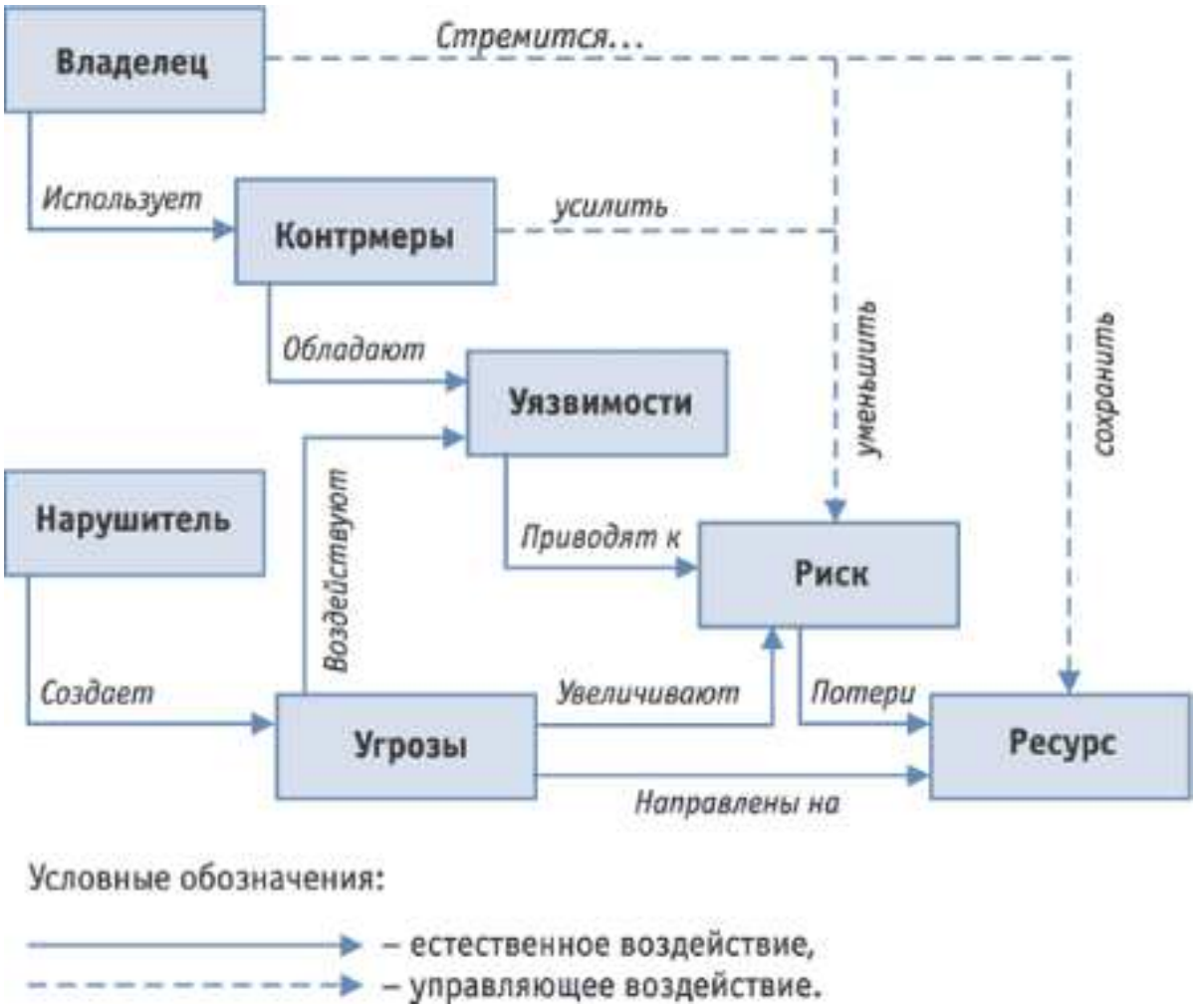

Рис. 1. Модель построения системы информационной безопасности предприятия

Рассматриваются следующие факторы:

–угрозы информационной безопасности, характеризующиеся вероятностью возникновения и вероятностью реализации;

–уязвимости информационной системы или системы контрмер (системы информационной безопасности), влияющие на вероятность реализации угрозы;

–риск - фактор, отражающий возможный ущерб организации в результате реализации угрозы информационной безопасности: утечки информации и ее неправомерного использования (риск в конечном итоге отражает вероятные финансовые потери - прямые или косвенные).

Для построения сбалансированной системы информационной безопасности предполагается первоначально провести анализ рисков в области информационной безопасности. Затем определить оптимальный уровень риска для организации на основе заданного критерия. Систему информационной безопасности (контрмеры) предстоит построить таким образом, чтобы достичь заданного уровня риска.

Построение модели информационной технологии

При построении модели будут учитываться взаимосвязи между ресурсами. Например, выход из строя какого-либо оборудования может привести к потере данных или выходу из строя другого критически важного элемента системы. Подобные взаимосвязи определяют основу построения модели организации с точки зрения ИБ.

Эта модель, в соответствие с предлагаемой методикой, строится следующим образом: для выделенных ресурсов определяется их ценность, как с точки зрения ассоциированных с ними возможных финансовых потерь, так и с точки зрения ущерба репутации организации, дезорганизации ее деятельности, нематериального ущерба от разглашения конфиденциальной информации и т. д. Затем описываются взаимосвязи ресурсов, определяются угрозы безопасности и оцениваются вероятности их реализации.

Выбор контрмер

На основе построенной модели можно обоснованно выбрать систему контрмер, снижающих риски до допустимых уровней и обладающих наибольшей ценовой эффективностью. Частью системы контрмер будут являться рекомендации по проведению регулярных проверок эффективности системы защиты.

Управление рисками

Обеспечение повышенных требований к ИБ предполагает соответствующие мероприятия на всех этапах жизненного цикла информационных технологий. Планирование этих мероприятий производится по завершении этапа анализа рисков и выбора контрмер. Обязательной составной частью этих планов является периодическая проверка соответствия существующего режима ИБ политике безопасности, сертификация информационной системы (технологии) на соответствие требованиям определенного стандарта безопасности.

Оценка достигаемой защищенности

В завершение работ, можно будет определить меру гарантии безопасности информационной среды, основанную на оценке, с которой можно доверять информационной среде объекта. Данный подход предполагает, что большая гарантия следует из применения больших усилий при проведении оценки безопасности.

Адекватность оценки основана на:

−вовлечении в процесс оценки большего числа элементов информационной среды объекта;

−глубине, достигаемой за счет использования при проектировании системы обеспечения безопасности большего числа проектов и описаний деталей выполнения;

−строгости, которая заключается в применении большего числа инструментов поиска и методов, направленных на обнаружение менее очевидных уязвимостей или на уменьшение вероятности их наличия.

Построение профиля защиты

На этом этапе разрабатывается система защиты информационной среды ”Заказчика”. Производится оценка доступных средств, осуществляется анализ и планирование разработки и интеграции средств защиты (рисунок 2). Необходимым

элементом работы является утверждение у Заказчика допустимого риска объекта защиты.

Рис. 2. Алгоритм оценивания информационных рисков

Предъявление повышенных требований к информационной безопасности предполагает соответствующие мероприятия на всех этапах жизненного цикла информационных технологий. Планирование этих мероприятий производится по завершении этапа анализа рисков и выбора контрмер. Обязательной составной частью системы является периодическая проверка соответствия существующего режима ИБ политике безопасности, сертификация информационной технологии на соответствие требованиям определенного стандарта безопасности. Работа по построению системы

защиты объекта начинается с построения профиля защиты данного объекта. При этом часть этой работы уже была проделана при проведении анализа рисков.