Анисимов Е.В. Методика построения системы информационной безопасности организации. // Проблемы информатики в образовании, управлении, экономике и технике: Сб. статей VIII Всерос. научно-техн. конф. – Пенза: ПДЗ, 2008. – С. 110-112.

МЕТОДИКА ПОСТРОЕНИЯ СИСТЕМЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ОРГАНИЗАЦИИ

Е.В. Анисимов

Астраханский государственный технический университет,
г. Астрахань

Основными целями системы информационной безопасности (ИБ) являются обеспечение устойчивого функционирования объекта, предотвращение угроз его безопасности, защита законных интересов организации от противоправных посягательств, недопущение хищения финансовых средств, разглашения, утраты, утечки, искажения и уничтожения служебной информации, обеспечение нормальной производственной деятельности всех подразделений объекта.

Еще одной целью системы информационной безопасности для организации является повышение качества предоставляемых услуг и гарантий безопасности, имущественных прав и интересов клиентов.

Задачами системы информационной безопасности являются:

– отнесение информации к категории ограниченного доступа (коммерческой 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 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.

При построении модели информационной безопасности рассматриваются следующие объективные факторы:

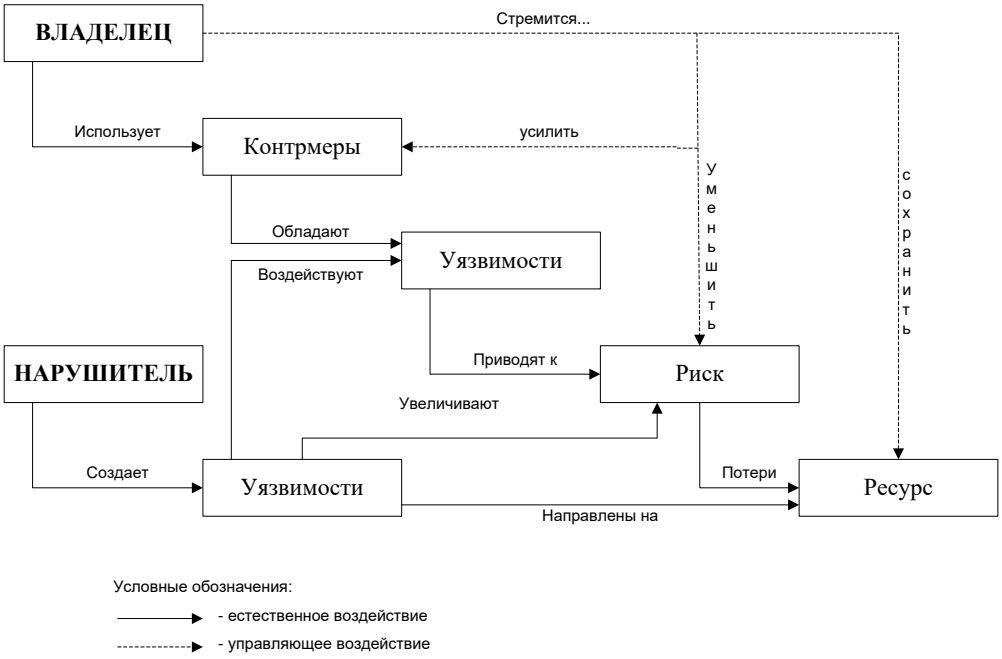
угрозы информационной безопасности, характеризующиеся вероятностью возникновения и вероятностью реализации;

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) необходимо построить таким образом, чтобы достичь заданного уровня риска.

При построении модели должны учитываться взаимосвязи между ресурсами. Ресурсами могут быть средства вычислительной техники, программное обеспечение, данные. Примерами внешних элементов являются сети связи, внешние сервисы и т.п. 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 соответствии 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. Пример такой модели представлен на рисунке.



Модель построения системы информационной безопасности организации

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.