УДК 378:323

В. И. ВАСИЛЬЕВ, Т. А. ИВАНОВА

РАЗРАБОТКА МЕТОДОЛОГИЧЕСКИХ ОСНОВ СОЗДАНИЯ И ВНЕДРЕНИЯ КОМПЛЕКСНОЙ СИСТЕМЫ БЕЗОПАСНОСТИ ВУЗА

Рассмотрены проблемы проектирования комплексных систем безопасности вузов. Приведено содержание концепции создания таких систем. Рассмотрена последовательность действий при проектировании. *Комплексная система безопасности; концепция; угроза; ресурс; риск; эффективность; оптимизация*

ВВЕДЕНИЕ

В последние годы резко возросла опасность техногенных катастроф и террористических актов как во всем мире, так и на территории Российской Федерации. В связи с этим назрела настоятельная необходимость в повышенном внимании к обеспечению безопасности в местах размещения материальных ценностей и финансовых активов, а также большого скопления людей. Причем именно защита человеческой жизни должна стать задачей первой важности при построении любой системы безопасности. Особое значение приобретает потребность в создании комплексных систем безопасности различных видов учебных заведений, включая высшие учебные заведения. Данная работа посвящена рассмотрению проблем, возникающих при проектировании подобных систем безопасности.

1. КОНЦЕПЦИЯ СОЗДАНИЯ КОМПЛЕКСНОЙ СИСТЕМЫ БЕЗОПАСНОСТИ ВУЗА

Следует отметить, что вуз в первую очередь является социальным институтом, предназначение которого – воспитание и профессиональная подготовка специалистов в различных областях жизнедеятельности общества. От качества и непрерывности такой подготовки зависит уровень развития экономики и общества в целом.

При создании комплексных систем безопасности (КСБ) вуза необходимо учитывать следующие факторы:

1) основная функция вуза – образовательная, следовательно, защите подлежат как знания, передаваемые в процессе обучения, так и люди, являющиеся носителями данных знаний;

2) наряду с образовательной функцией, вуз выполняет большой объем научных исследований, ход и результаты которых также должны быть защищены от различных угроз;

3) территория вуза, как правило, занимает обширную площадь, а здания учебных корпусов характеризуются значительной пространственной рассредоточенностью;

4) на территории вуза всегда присутствует массовое скопление людей – преподавателей, студентов, сотрудников, посетителей.

Необходимость создания КСБ вузов нормативно закреплена в Целевой программе на 2004-2007 годы «Безопасность образовательного учреждения», утвержденной приказом №31 Минобразования России от 12.01.2004 г.

При создании типового проекта КСБ вуза существует целый ряд трудностей. Одна из них – отсутствие нормативно-правового обеспечения КСБ, включающего в себя:

1) концепцию построения КСБ вуза;

2) Положение о КСБ;

3) служебные инструкции администраторов безопасности;

4) типовую политику безопасности вуза.

Разработка концепции обеспечения комплексной безопасности вуза, являющейся методической основой для всех проводимых мероприятий по обеспечению безопасности, является нетривиальной задачей. Данная концепция должна представлять собой научно обоснованную систему взглядов, определяющих основные направления, условия и порядок практического решения задач защиты основных компонент образовательного и научного процесса от противоправных действий. Под безопасностью вуза при этом понимается состояние защищенности его людских и информационных ресурсов, а также материальных ценностей от внутренних и внешних угроз. Под состоянием защищенности понимается умение и способность составляющих КСБ надежно противостоять любым попыткам злоумышленников, персонала и случайных посетителей нанести ущерб объектам, подлежащим защите [1].

В концепции обеспечения безопасности должны быть описаны основные подсистемы КСБ, их взаимодействие друг с другом, проведен анализ состава объектов защиты и угроз, оценка риска и приведены общие рекомендации по составу контрмер для актуальных угроз и порядку их применения.

Главными целями КСБ вуза являются:

– обеспечение устойчивого функционирования образовательного учреждения и предотвращение угроз его безопасности;

– охрана жизни и здоровья людей;

– недопущение террористических актов на территории учреждения и приписанных к нему объектов;

– недопущение хищения финансовых и материально-технических средств;

– недопущение порчи и уничтожения имущества и ценностей;

– недопущение разглашения, утраты, утечки, искажения и уничтожения информации ограниченного доступа.

Для того чтобы КСБ наиболее эффективно удовлетворяла поставленным целям, необходим системный подход к процессу ее проектирования. При этом различают две возможные постановки задачи проектирования:

1) создание КСБ «с нуля», или проектирование «сверху»: формулируются цели КСБ, выполняемые задачи, функции системы, в соответствии с этим выбирается состав основных функциональных подсистем и структура их взаимодействия;

2) модернизация существующей КСБ, или проектирование «снизу». В данном случае определяются перечень угроз и уязвимостей сложившейся системы безопасности, подбираются дополнительные средства безопасности, при необходимости осуществляется интеграция подсистем.

На практике чаще всего проектировщики сталкиваются со второй постановкой задачи, так как на реальных объектах (в данном случае в вузе) уже существует определенная сложившаяся структура системы безопасности. Оценка ее эффективности и достаточности, при этом, как правило, входит в процесс проектирования.

2. ЭТАПЫ ПРОЕКТИРОВАНИЯ КСБ

Процесс проектирования, с позиций системного подхода, подразумевает выполнение определенных последовательных этапов, направленных на решение следующих вопросов:

1) Предпроектное обследование объекта. На данном этапе определяется состав ресурсов объекта, подлежащих защите, состав угроз, актуальных для ресурсов, оцениваются их количественные характеристики.

Как уже отмечалось, объектами защиты (т.е. ресурсами, подлежащими защите) в вузе являются:

1. Людские ресурсы (студенты, профессорско-преподавательский состав, сотрудники университета);

2. Информационные ресурсы (информация, составляющая государственную тайну, иная информация с ограниченным доступом, в том числе конфиденциальная, предоставленная в виде документов и массивов, независимо от формы и вида их представления);

3. Финансовые средства, материальные ценности.

Для каждого ресурса определяется его количественная характеристика – ценность для владельца или пользователя. Для финансовых средств и материальных ресурсов определение ценности не составляет труда – это их денежный эквивалент. При определении ценности людских и информационных ресурсов возникают затруднения – их оценка в денежном эквиваленте невозможна или затруднена. Для этой цели возможно использование нечетких или лингвистических переменных. Например, ценность какого-либо информационного ресурса может быть «высокой», «средней» или «малой». Стоит отметить, что первейшей задачей для КСБ должна стать именно защита людей от терактов и других угроз их жизни и здоровью.

Определение полного списка воздействующих на объект угроз является следующим шагом. Угрозы классифицируют по объекту воздействия (информация, люди, материальные ресурсы), субъекту воздействия, локализации (внутренние, внешние). По субъекту воздействия можно выделить три наиболее вероятные модели злоумышленников:

1. Террорист (обычно хорошо экипирован, имеет план зданий и помещений, обладает навыками преодоления преград и средств охраны, мотивация – уничтожение имущества и людей, характерная угроза – теракт);

2. Студент (экипировка отсутствует, представляет расположение зданий и помещений, навыки преодоления средств охраны отсутствуют, мотивация – психологическая тяга к деструктивным действиям, характерная угроза – вандализм);

3. Случайный посетитель (экипировка отсутствует, чаще всего не представляет расположение зданий и помещений, навыки преодоления средств охраны отсутствуют, мотивация – психологическая тяга к противоправным действиям, характерная угроза – кража).

В качестве количественной характеристики угрозы обычно используется вероятность ее возникновения. При этом возможен сбор статистики по данной угрозе и определение средней частоты ее возникновения или задание субъективной вероятности возникновения угрозы. Использование аппарата лингвистических переменных возможно и в данном случае.

2) Оценка риска. Производится оценка потенциального ущерба от воздействия угроз на ресурсы с использованием определенных на предпроектной стадии количественных характеристик угроз и ресурсов. При этом учитывается эффективность функционирующих на объекте средств безопасности. Данные средства делятся на средства обнаружения (ключевая характеристика – вероятность обнаружения) и средства задержки (ключевая характеристика – время задержки).

Вследствие наличия значительной неопределенности при определении характеристик ресурсов, угроз и эффективности средств безопасности, численные методы оценки риска не дают приемлемую точность вычислений. Решением данной проблемы может стать применение подхода, используемого при оценке соответствия информационной безопасности организаций банковской системы РФ [2]. Суть данного подхода заключается в заполнении опросников специалистами организаций по безопасности. После обработки результатов по определенной методике, на круговой (лепестковой) диаграмме отображаются

уровни обеспечения безопасности по различным составляющим (критериям) обеспечения системы безопасности. Введение нескольких категорий для итогового уровня безопасности КСБ позволяет определить достаточность существующей защиты и наметить пути ее повышения.

3) Этап проектирования. Результатом анализа риска является перечень уязвимых мест сложившейся системы безопасности, уровень безопасности в которых не удовлетворяет требуемому заказчиком уровню. С целью снижения риска, для каждой уязвимости подбираются соответствующие средства безопасности. Таким образом формируется архитектура КСБ, причем вариантов выбора конкретного оборудования может быть много. Каждый из таких вариантов обладает определенной эффективностью. Под эффективностью системы безопасности будем понимать степень соответствия КСБ своему целевому предназначению [3]. Эффективность КСБ зависит от надежностных характеристик технических средств, качества их функционирования, полноты и достоверности поступающей от технических средств информации. Численную оценку критерия эффективности, в общем случае, можно найти с помощью выражения:

$$E = f(N, K, D),$$

где E – показатель эффективности КСБ; N – надежность технических средств безопасности; K – качество функционирования этих технических средств; D – полнота и достоверность рабочей информации о состоянии объектов защиты.

Так как финансирование, выделяемое на создание систем безопасности, обычно ограничено, то выбор оборудования должен оптимизироваться. Возможны две постановки задачи оптимального выбора оборудования КСБ:

1. Максимизация показателя эффективности системы безопасности (E) при ограниченном объеме выделенных для этой цели финансовых средств (C):

$$E \to \max, \sum C \le C_{доп} .$$

2. Минимизация объема выделенных на создание системы безопасности финансовых средств, при достижении заданного уровня эффективности системы безопасности:

$$\sum C \to \min, E \ge E_{доп} .$$

ВЫВОДЫ

1. Оценка эффективности и выбор вариантов построения КСБ требует разработки специальных методов, основанных на использовании опыта и знаний экспертов.

2. Особое место занимают вопросы обеспечения мониторинга объектов защиты, управления текущим функционированием КСБ и реконфигурации (в случае необходимости) состава ее технических средств.

3. Рассмотренные выше проблемы методологического характера требуют разработки научно обоснованных инженерных методик анализа эффективности существующих и проектирования новых КСБ и их подсистем. Реализация данных методик, а также разработка комплекса нормативно-правовых документов позволят создать эффективную систему безопасности вуза, отражающую угрозы, направленные на противодействие осуществлению миссии университета – подготовка высококвалифицированных специалистов и научно-педагогических кадров как носителей и распространителей новых знаний, обладающих прогрессивным мировоззрением и способных обеспечить прогрессивные изменения в экономике России.

СПИСОК ЛИТЕРАТУРЫ

1. **Sec.ru.** Концепция безопасности коммерческого банка : публикации на Sec.ru [Электронный ресурс]. (http://daily.sec.ru).

2. Стандарт Банка России. Обеспечение информационной безопасности организаций Банковской системы Российской Федерации. Общие положения // Вестник банка России. 2004. № 68 (792). С. 25–43.

3. **Алексеев А. В.** Устойчивость функционирования СКБ крупных компаний. Основные факторы и меры по обеспечению / А. В. Алексеев, А. А. Фролов // Системы безопасности. 2005. № 4. С. 25–27.