На правах рукописи

ИВАНОВА Татьяна Александровна

МЕТОДИЧЕСКОЕ И АЛГОРИТМИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ОРГАНИЗАЦИОННО-ТЕХНИЧЕСКОГО УПРАВЛЕНИЯ КОМПЛЕКСНОЙ БЕЗОПАСНОСТЬЮ ВЫСШЕГО УЧЕБНОГО ЗАВЕДЕНИЯ

Специальность – 05.13.10
Управление в социальных и экономических системах

АВТОРЕФЕРАТ
диссертации на соискание ученой степени
кандидата технических наук

Уфа–2009

Работа выполнена на кафедре вычислительной техники и защиты информации
ГОУ ВПО «Уфимский государственный авиационный технический университет»

Научный руководитель	д-р техн. наук, проф. **Васильев Владимир Иванович**
Официальные оппоненты	д-р техн. наук, проф. **Черняховская Лилия Рашитовна** канд. техн. наук, доц. **Дуленко Вячеслав Алексеевич**
Ведущая организация	Башкирский государственный университет

Защита диссертации состоится 30 октября в _____ часов
на заседании диссертационного совета Д-212.288.03
при Уфимском государственном авиационном техническом университете
по адресу: 450000, г. Уфа, ул. К. Маркса, 12

С диссертацией можно ознакомиться в библиотеке университета

Автореферат разослан _____ сентября 2009 г.

Ученый секретарь
диссертационного совета
д-р техн. наук, проф. В.В. Миронов

ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

Актуальность темы

В стенах высших учебных заведений трудится и обучается большое количество высококвалифицированных педагогов, научных сотрудников и молодежи, составляющей интеллектуальный и трудовой потенциал нашей страны. В связи с чем задача обеспечения безопасности высших учебных заведений имеет огромное значение в современных условиях. Повышенная опасность пожаров, проведения диверсионно-террористических акций, совершения краж также обостряет проблему обеспечения безопасности материальных, финансовых и людских ресурсов вузов.

Следует отметить, что в области обеспечения и управления безопасностью вузов существует целый ряд проблем: недостаточная оснащенность техническими средствами обеспечения безопасности образовательных учреждений различного уровня; значительный физический и моральный износ существующего оборудования обеспечения безопасности; отсутствие специализированной подготовки у лиц, ответственных за безопасность вуза, позволяющей грамотно и оптимально распределить выделяемое на обеспечение безопасности целевое финансирование.

Существующие подходы к организационно-техническому управлению безопасностью позволяют разрабатывать комплексы технических средств безопасности (КТСБ) в основном для коммерческих предприятий или режимных объектов. Однако образовательные учреждения обладают собственной спецификой, обусловливающей и особенность организационно-технического управления их безопасностью. Проектировщики КТСБ вузов сталкиваются со следующими трудностями: отсутствие специализированных методик оценки текущего состояния обеспечения безопасности вуза; неопределенность и специфичность дестабилизирующих факторов, воздействующих на защищаемые ресурсы вуза; отсутствие отработанных методов, методик и алгоритмов разработки и оценки эффективности КТСБ образовательных учреждений.

Таким образом, тема данной диссертационной работы, посвященная разработке методического и алгоритмического обеспечения организационно-технического управления комплексной безопасностью вуза, является актуальной.

Объект исследования – система организационно-технического управления (СОТУ) комплексной безопасностью высшего учебного заведения.

Предмет исследования – методическое и алгоритмическое обеспечение СОТУ.

Цель и задачи исследования

Целью исследования является повышение эффективности организационно-технического управления комплексной безопасностью вуза путем разработки соответствующего методического и алгоритмического обеспечения. Для выполнения поставленной цели сформулированы следующие задачи:

1. Разработать комплекс системных моделей бизнес-процессов по созданию подсистемы организационно-технического управления безопасностью вуза и методику оценки текущего состояния данной подсистемы.

2. Разработать структурную модель вуза как объекта управления безопасностью, а также алгоритм и модель анализа риска (потенциального ущерба) для ресурсов вуза.

3. Разработать критерии оценки эффективности подсистемы организационно-технического управления безопасностью вуза и алгоритм, используемый в рамках данной подсистемы для оптимизации состава комплекса технических средств безопасности (КТСБ), основанный на применении генетических алгоритмов.

4. Провести апробацию разработанных моделей, методик и алгоритмов с использованием исследовательского прототипа системы поддержки принятия решений (СППР) по организационно-техническому управлению безопасностью вуза.

Методы исследования

При работе над диссертацией использовались методы системного анализа, теории множеств, теории вероятности, теории управления и принятия решений, методы оптимизации. Для оценки эффективности предлагаемых решений использовались методы математического и имитационного моделирования.

Результаты, выносимые на защиту

1. Комплекс системных моделей бизнес-процессов по созданию подсистемы организационно-технического управления безопасностью вуза и методика оценки текущего состояния данной подсистемы.

2. Модель анализа риска для ресурсов вуза, основанная на модели системы с полным перекрытием каналов воздействия угроз и использовании марковских моделей.

3. Алгоритм оптимизации состава КТСБ, являющегося составной частью подсистемы организационно-технического управления безопасностью вуза, основанный на максимизации комплексного показателя эффективности с помощью генетического алгоритма.

4. Исследовательский прототип СППР по организационно-техническому управлению безопасностью вуза.

Научная новизна результатов

Научная новизна работы заключается в следующем:

1. Предложен комплекс системных моделей бизнес-процессов по созданию подсистемы организационно-технического управления безопасностью вуза, разработанных с использованием SADT-методологии, а также методика оценки текущего состояния данной подсистемы, основанная на построении модели жизненного цикла указанной подсистемы, позволяющие, в отличие от существующих моделей и методик, оценить как фактическое состояние подсистемы организационно-технического управления безопасностью вуза, так и тенденции его изменения.

2. Предложены структурная модель вуза и основанные на данной модели ал-

горитм и модель анализа риска, отличающиеся от известных моделей тем, что данные модели позволяют выявить взаимосвязи защищаемых ресурсов вуза, провести оценку вероятностей угроз (проникновения злоумышленников) с помощью марковских моделей, оценить потенциальный ущерб от воздействия данных угроз, а также обоснованно предъявить требования к структуре и составу КТСБ.

3. Разработан алгоритм оптимизации состава технических средств безопасности, основанный на использовании генетического алгоритма, позволяющего, по сравнению с традиционными методами многопараметрической оптимизации, снизить вычислительные затраты и время поиска оптимального решения на множестве большого числа альтернатив.

4. Разработан прототип СППР, позволяющий на основе единой информационной системы объединить предложенные методики, модели и алгоритмы организационно-технического управления безопасностью вуза.

Практическая значимость и внедрение результатов

Практическая ценность результатов, полученных в диссертации, заключается в разработке:

– комплекса системных моделей бизнес-процессов по созданию подсистемы организационно-технического управления безопасностью вуза и методики оценки текущего состояния данной подсистемы, основанной на построении модели жизненного цикла подсистемы организационно-технического управления безопасностью вуза;

– модели анализа риска, основанной на модели системы с полным перекрытием каналов воздействия угроз и использовании марковских моделей;

– алгоритма оптимизации состава технических средств безопасности, основанного на применении генетических алгоритмов;

– прототипа СППР по организационно-техническому управлению безопасностью вуза.

Предложенные методики, модели и алгоритмы позволяют повысить эффективность организационно-технического управления безопасностью вуза, снизить временные затраты на процесс разработки СОТУ, снизить потенциальный ущерб для ресурсов вуза и суммарную стоимость технических средств безопасности при внедрении оптимизированного варианта КТСБ.

Основные результаты диссертационной работы внедрены в Уфимском государственном авиационном техническом университете.

Апробация работы

Основные научные и практические результаты диссертационной работы докладывались и обсуждались на следующих конференциях:

– VI Международной научно-технической конференции «Проблемы техники и технологии телекоммуникации», Уфа, 2005;

– 7-й и 8-й Международных научно-практических конференциях «Информационная безопасность», Таганрог, 2005, 2006;

– 7-й, 8-й и 9-й Международных научных конференциях «Компьютерные науки и информационные технологии» (CSIT), Уфа, 2005, 2007, Карлс-

руэ, Германия, 2006;

– XXXII Международной молодёжной научной конференции «Гагаринские чтения», Москва, 2006;

– Российской научно-технической конференции «Мавлютовские чтения», Уфа, 2006;

– 2, 3 и 4-й Всероссийских зимних школах-семинарах аспирантов и молодых ученых (с международным участием) «Актуальные проблемы науки и техники», Уфа, 2007, 2008, 2009.

Публикации

Список публикаций по теме диссертационной работы содержит 12 работ, в том числе 11 материалов докладов международных и российских конференций и 1 статья в рецензируемом журнале из перечня ВАК.

Структура работы

Диссертационная работа состоит из введения, четырех глав, заключения, приложений и библиографического списка. Работа содержит 193 страницы машинописного текста, включая 56 рисунков и 18 таблиц. Библиографический список включает 107 наименований.

ОСНОВНОЕ СОДЕРЖАНИЕ РАБОТЫ

Во введении обоснована актуальность темы исследования, сформулированы цель и задачи исследования, определены научная новизна и практическая значимость работы, сформулированы основные результаты, выносимые на защиту.

В первой главе проанализировано состояние проблемы управления безопасностью вуза. Рассмотрены особенности вуза как объекта обеспечения безопасности, проведена классификация вуза по различным признакам. Проведенный анализ показал, что в настоящее время проблема управления безопасностью вузов стоит довольно остро, вследствие того, что данной тематике практически не уделено внимания в теории обеспечения безопасности. Однако вузы, в силу многих особенностей, являются весьма специфичными объектами, управление безопасностью которых требует особых подходов. Отмечается, что управление безопасностью вуза имеет две взаимосвязанные составляющие: организационную и техническую. То есть целенаправленные воздействия, которым подвергается вуз, могут иметь вид организационных мер (различные инструкции, регламенты и пр.) или же управление безопасностью может осуществляться путем применения специальных технических средств безопасности. В связи с этим, систему управления безопасностью вуза предложено рассматривать как систему организационно-технического управления (СОТУ). При этом, если в области организационной составляющей системы организационно-технического управления безопасностью накоплен обширный опыт практической работы (разработаны и применяются большое число различных инструк-

ций, регламентов и т.д.), то ситуация, сложившаяся с технической частью данной подсистемы, характеризуется рядом нерешенных проблем.

Основной целью организационно-технического управления комплексной безопасностью вуза является планирование и реализация комплекса технических средств безопасности (КТСБ), применение которого могло бы обеспечить заданный уровень безопасности. В главе рассмотрены текущее состояние и тенденции развития подсистем безопасности, входящих в состав КТСБ.

Проведен подробный анализ нормативных документов в области обеспечения безопасности. Выявлено, что категорирование объектов, а также проектирование составляющих КТСБ регламентированы довольно полно. Однако отсутствуют стандарты, содержащие подходы к разработке систем управления безопасностью различных объектов, в том числе вузов. Отмечается возможность использования для этой цели подходов, предлагаемых стандартами ISO/IEC 9001-2001, ISO/IEC 27001.

Рассмотрены существующие подходы к оценке эффективности систем безопасности, в том числе различные методики оценки риска. Показаны недостатки применения данных подходов, обоснована необходимость разработки модели оценки риска как показателя эффективности обеспечения безопасности. Проведен анализ методов оптимизации состава КТСБ.

По результатам проведенного анализа сформулированы цель и задачи исследования.

Во второй главе проводится разработка методического обеспечения СОТУ безопасностью вуза. Система организационно-технического управления безопасностью вуза рассматривается как часть общей системы управления вузом, направленная на создание, обеспечение, управление, мониторинг, контроль, поддержание и улучшение комплексной безопасности вуза.

Для разработки архитектуры СОТУ (рисунок 1) использован подход, описанный в стандарте ИСО 27001.

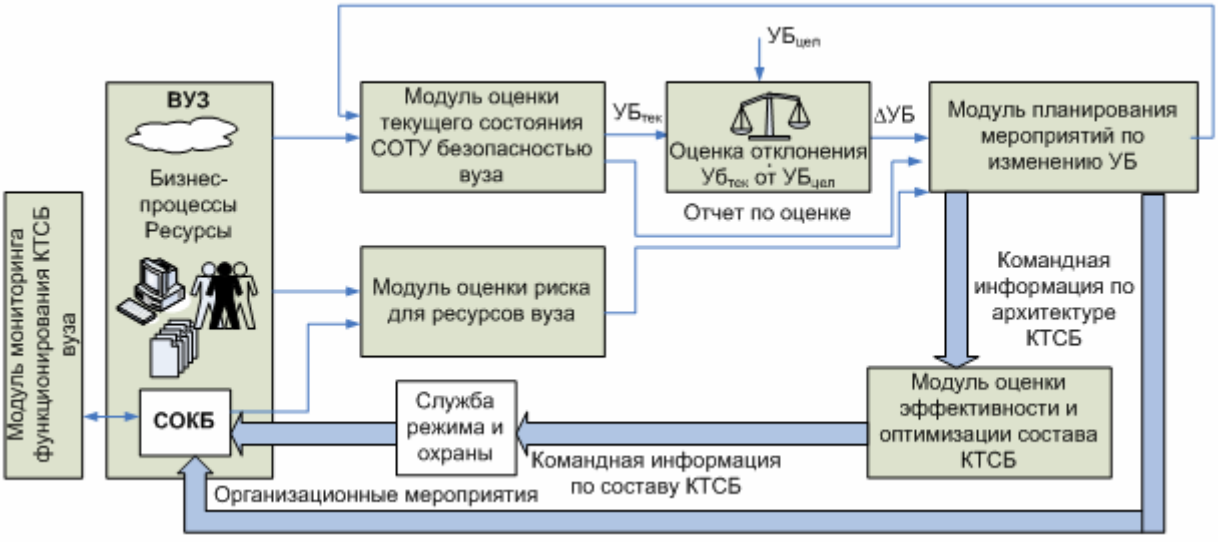

Рисунок 1 – Архитектура СОТУ

В соответствии с данным подходом, процесс обеспечения и управления комплексной безопасностью вуза должен осуществляться в рамках 4-хфазной модели жизненного цикла PDCA (Plan-Do-Check-Act): планируй (создание СОТУ); выполняй (внедрение и функционирование СОТУ); проверяй (мониторинг и проверка СОТУ); действуй (поддержание и улучшение СОТУ).

Функциональная модель процесса организационно-технического управления безопасностью вуза, построенная с применением IDEF-технологии, представлена на рисунке 2.

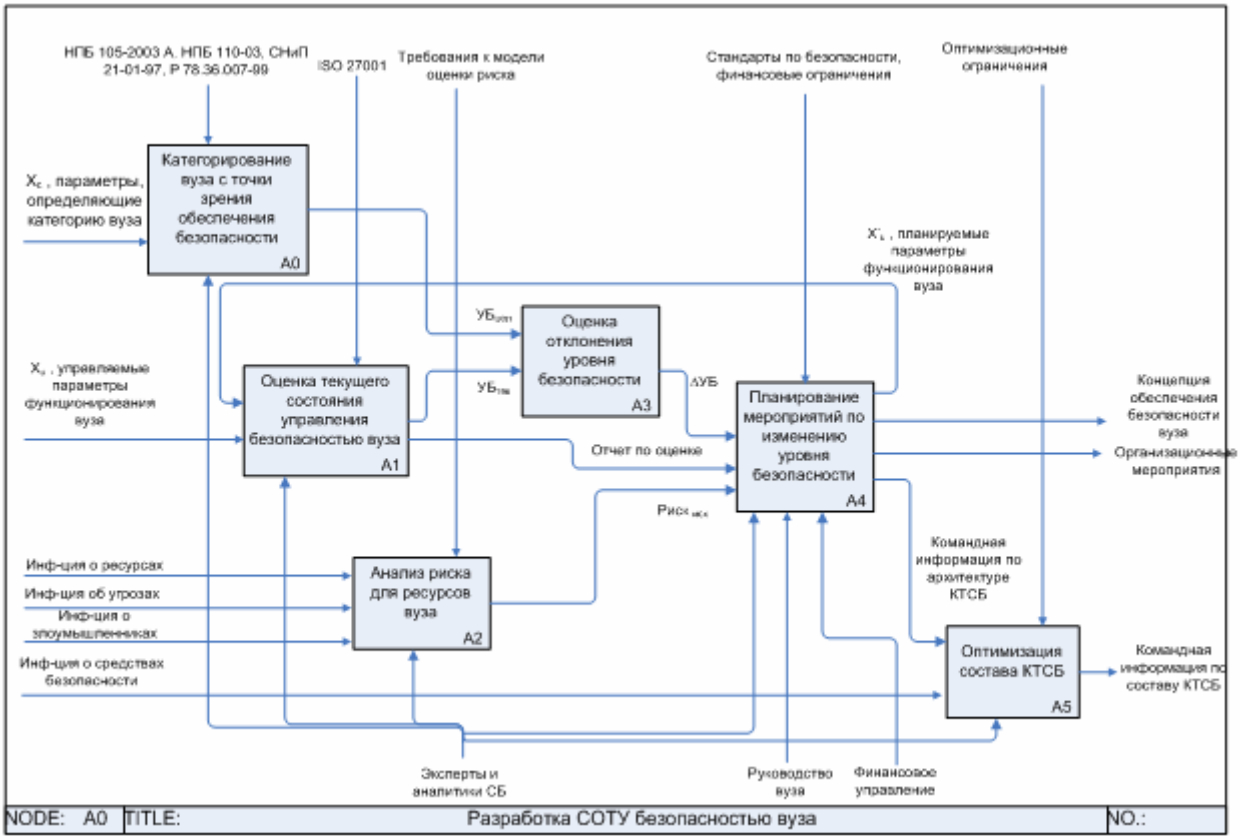

Рисунок 2 – Функциональная модель процесса организационно-технического управления безопасностью вуза

Первым шагом при оценке текущего состояния СОТУ безопасностью вуза является определение категории вуза. От категории вуза зависит целевой рейтинг (уровень) безопасности $УБ_{цел}$, который должна обеспечить разрабатываемая СОТУ.

Категорию обеспечения безопасности вуза в целом предлагается определять с использованием кортежа параметров:

$$X_c = \{Q, T, S, P\}, \quad (1)$$

где Q – численность контингента вуза (персонал, преподаватели, обучающиеся); T – территориальная распределенность вуза; S – тип вуза по предоставляемым обществу образовательных и научных продуктов (дистанционный, классический, исследовательский); P – процентное соотношение количества поме-

щений первой и второй категорий и количества помещений третьей и четвертой категорий.

Предлагаемое количество категорий вуза составляет четыре: низкая, средняя, высокая, очень высокая категории. Так как диапазон приведенных параметров может иметь довольно размытые границы (нельзя конкретно сказать, когда, к примеру, численность контингента является средней или высокой), то для определения категории защиты вуза предложено воспользоваться аппаратом нечетких множеств.

Чем выше категория вуза, тем более высокий рейтинг он должен иметь, то есть

$$УБ_{цел} = f(K), \quad (2)$$

где $УБ_{цел}$ – целевой уровень обеспечения безопасности вуза; K – категория вуза.

В простейшем случае функция f имеет вид простого отображения множества категорий на множество возможных уровней безопасности.

По аналогии с отраслевым стандартом Банка России СТО БР ИББС-1.0-2006, уровень безопасности вуза предлагается определять с помощью методики экспертной оценки текущего состояния СОТУ безопасностью вуза. Количество уровней обеспечения безопасности определяется количеством категорий вуза и ограничено пятью – с нулевого по четвертый. Нулевой уровень характеризует полное отсутствие каких-либо процессов управления безопасностью в рамках деятельности вуза. Четвертый уровень присваивается при наличии разработанной и эффективно функционирующей СОТУ безопасностью вуза.

Для оценки уровня обеспечения безопасности используются групповые и частные показатели безопасности. Частные показатели безопасности объединены в совокупности, соответствующие групповым показателям безопасности, которые отражают области обеспечения безопасности вуза, процессы управления безопасностью и принципы безопасного функционирования вуза. Оценки EV_{M_i} групповых показателей формируются в виде совокупности оценок $EV_{M_{i.j}}$ частных показателей, входящих в состав группового показателя M_i. Отвечая на вопросы частных показателей разработанных анкет, эксперты формируют оценки групповых показателей M_i (рисунок 3). Оценка EV1 определяет текущий уровень обеспечения безопасности вуза и вычисляется следующим образом:

$$EV1 = \sum EV_{M_i}, i = 1,...,9, \quad (3)$$

где EV_{M_i} – оценки групповых показателей.

Подобным же образом формируется оценка EV2, определяющая состояние процессов управления безопасностью вуза (групповые показатели с 10 по 19). Итоговая оценка $УБ_{тек}$ определяет уровень обеспечения безопасности вуза, а также состояние СОТУ, и вычисляется на основе оценок EV1 и EV2 (отображены на рисунке 3 прямоугольниками).

Горизонтальные линии соответствуют целевым (заданным) уровням безопасности.

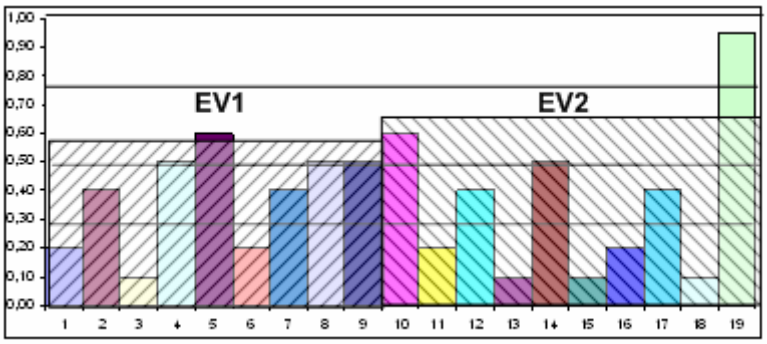

Рисунок 3 – Диаграмма отображения оценок соответствия уровня обеспечения безопасности вуза и итоговой оценки рейтинга

После качественного определения текущего состояния СОТУ безопасностью вуза необходимо количественно оценить риск, которому подвергаются ресурсы вуза: материальные, информационные, людские. Для того чтобы учесть отношения между ресурсами, а также различные свойства отдельных ресурсов, была построена концептуальная (общесистемная) модель вуза М в виде онтологии, которая включает в себя классы ресурсов, отношения между ними (классификации, принадлежности), свойства индивидов. Возможность задания отношений между классами онтологии позволила добавить в нее также классы угроз и типов злоумышленника.

Предлагаемый подход к оценке риска основан на модели системы «с полным перекрытием», только рассматриваются совокупности нескольких видов ресурсов – составные ресурсы-помещения.

При анализе риска ресурсам вуза рассматриваются различные модели злоумышленника: террорист, опытный вор, случайный посетитель, студент, сотрудник. Обозначим множество типов злоумышленника как $D=\{d_k\}$. Вероятность столкновения с определенным типом злоумышленника определяется распределением вероятностей $P(d_k)=\{ p_{d_k} \}$. Злоумышленник определенного типа при воздействии на ресурсы может реализовывать одну из угроз множества $Q_k=\{q_i\}$. Вероятность выбора злоумышленником той или иной угрозы определяется распределением вероятностей $P^k(q_i)=\{ p_i^k \}$. Риск от воздействия i-й угрозы, характерной для злоумышленника d_k, на определенный ресурс-помещение L_j будет рассчитываться следующим образом:

$$r_{ij}^k = p_i^k \cdot P_{\text{пр}}^{\text{j}} \cdot C_{L_j}, \qquad (4)$$

где p_i^k – вероятность реализации k-м типом злоумышленника угрозы q_i; $P_{\text{пр}}^{\text{j}}$ – вероятность его проникновения в j-е помещение; C_{L_j} – суммарная стоимость ресурсов помещения L_j.

Риск от совокупности угроз, реализуемых k-м типом злоумышленника в отношении j-го помещения, рассчитывается по формуле

$$r_j^k = \sum_i r_{ij}^k . \qquad (5)$$

Для нахождения вероятности проникновения в помещение использован аппарат марковских цепей. Строится модель проникновения злоумышленника в элементы охраняемого пространства (помещения), представляющая собой орграф $G_0(A,C)$. Преобразуя матрицу смежности графа $G_0(A,C)$ в матрицу переходных вероятностей, соответствующих вероятностям событий перехода злоумышленника, получим модель его поведения в дискретном времени.

Риск для ресурсов *j*-го помещения от столкновения с различными типами злоумышленников будет равен:

$$r_j = \sum_{k=1}^{5} r_j^k \cdot p_{d_k} . \qquad (6)$$

Вероятность столкновения с k-м типом злоумышленника p_{d_k} задается экспертно. Для того чтобы найти суммарный риск от действий злоумышленников всех типов ($R_{зл}$), используется формула

$$R_{зл} = \sum_{j=1}^{m} r_j . \qquad (7)$$

где m – общее количество защищаемых помещений. В работе приведен пример расчета исходного риска для ресурсов нескольких помещений вуза.

В третьей главе рассматривается процесс планирования организационно-технического управления безопасностью, приводится его функциональная модель. Результатами оценки текущего состояния СОТУ безопасностью вуза являются значения групповых показателей М1,…,М19. При отклонении значения текущего уровня безопасности $УБ_{тек}$ от желаемого значения $УБ_{цел}$ необходимо для каждой из групп показателей разработать соответствующие мероприятия, повышающие значение соответствующего группового показателя и УБ в целом. Предлагается алгоритм определения состава мероприятий по совершенствованию СОТУ, которые должны документально закрепляться в «Концепции обеспечения безопасности вуза».

В соответствии с определенной ранее категорией вуза предлагается применять соответствующую архитектуру (состав подсистем) КТСБ. Формирование структуры КТСБ (мест установки средств безопасности) предлагается проводить исходя из обеспечения устанавливаемого ограничения для значения риска.

Одной из главных целей разработки СОТУ безопасностью вуза является планирование архитектуры и состава КТСБ вуза. Следовательно, эффективность СОТУ, как степень соответствия системы своему целевому назначению, определяется эффективностью разработанной КТСБ. В качестве количественной меры соответствия КТСБ своему предназначению (обеспечение безопасности ресурсов вуза) предложено использовать значение относительного риска $\overline{R}$, который отражает меру снижения потенциального ущерба ресурсам вуза при использовании средств КТСБ по отношению к исходному значению риска.

Помимо злоумышленных действий, существует такая угроза, как пожар. Ущерб для ресурсов *j*-го помещения от возникновения пожара оценивается по формуле:

$$r_j^{пож} = p_j^{пож} \cdot C_{L_j}, \quad (8)$$

где $p_j^{пож}$ – вероятность возникновения пожара в *j*-м помещении.

Потенциальный ущерб от пожара и исходный риск для ресурсов вуза рассчитываются следующим образом:

$$R_{пож} = \sum_{j=1}^{m} r_j^{пож}, \; R_{общ}^{исх} = R_{зл} + R_{пож}. \quad (9)$$

При анализе риска с учетом установленных средств безопасности рассматривается последовательность преодоления рубежей, представленных на рисунке 4. Вероятность реализации угрозы зависит от того как три периметральных рубежа осуществляют задержку распространения угрозы с вероятностью задержки ($P_{зад}$), а на открытых пространствах между периметральными рубежами реализуется вероятность обнаружения ($P_{обн}$).

Тогда в общем случае (при возникновении угрозы за пределами объекта) вероятность успешной реализации угрозы в отношении *j*-го помещения будет равна

$$P_{реал}^j = \prod_{v=1}^{3}(1 - P_{обнv}^j)\prod_{z=1}^{3}(1 - P_{задz}^j), \quad (10)$$

где $P_{обнv}^j$ – вероятность обнаружения угрозы в *v*-м объеме; $P_{задz}^j$ – вероятность задержки распространения угрозы *z*-м периметральным рубежом.

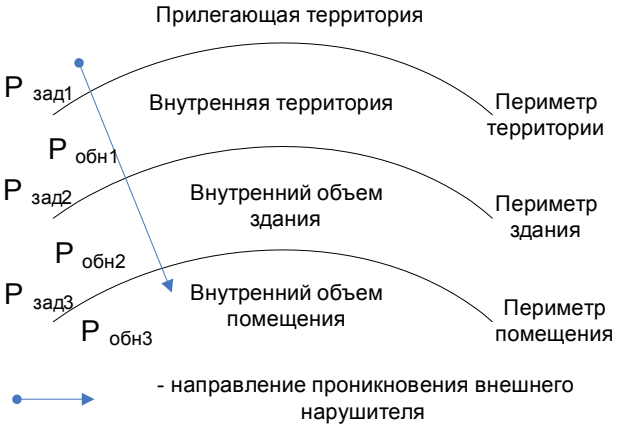

Рисунок 4 – Последовательность преодоления рубежей

Следует отметить, что для внутреннего нарушителя имеет смысл рассматривать только задержку на периметре помещения ($P_{зад3}$) и обнаружение во внутреннем объеме ($P_{обн3}$).

Для определения вероятности реализации внешним нарушителем угрозы строятся структурно-надежностные схемы, как показано на рисунке 5.

Для схемы, представленной на рисунке 5, функция обнаружения будет выполняться с вероятностью

$$P_{обн} = (1-(1-P_{обн1}^{СРО})\cdot(1-P_{обн1}^{СТН}))\cdot(1-(1-P_{обн2}^{СРО})\cdot(1-P_{обн2}^{СТН}))\cdot(1-(1-P_{обн2}^{СРО})\times \times(1-P_{обн2}^{СТН})\cdot(1-P_{обн2}^{СТН})). \quad (11)$$

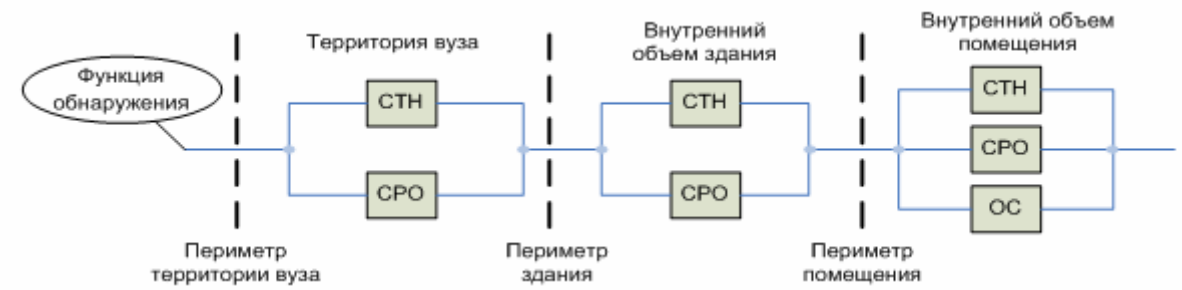

Рисунок 5 – Структурно-надежностные схемы выполнения функций КТСБ: СТН – система телевизионного наблюдения, СРО – служба режима и охраны, ОС – охранная сигнализация

«Эффект резервирования» функций безопасности позволяет повысить вероятность того, что угроза будет в итоге парирована.

Значение потенциального ущерба от злоумышленных действий, при наличии средств обнаружения и задержки, определяется следующим образом:

$$R'_{\text{зл}} = \sum_{j=1}^{m} r'_j , \tag{12}$$

где $r'_j = P_{реал}^{j} \cdot r_j$ – значение риска для j-го помещения с учетом наличия средств обнаружения и задержки, r_j – исходное значение риска для j-го помещения.

Потенциальный ущерб от пожара с учетом технических средств равен

$$R'_{пож} = \sum_{j=1}^{m} r'^{пож}_{j} , \tag{13}$$

где $r'^{пож}_{j} = (1 - P^{пож}_{обнj}) \cdot r^{пож}_{j}$ – ущерб для ресурсов j-го помещения от возникновения пожара, при наличии пожарной сигнализации, $P^{пож}_{обнj}$ – вероятность обнаружения пожара в j-м помещении.

Тогда общий риск для ресурсов вуза, с учетом наличия средств безопасности, будет равен

$$R'_{общ} = R'_{\text{зл}} + R'_{пож} . \tag{14}$$

В качестве показателя эффективности применения КТСБ используется показатель относительного риска, рассчитываемый по формуле:

$$\overline{R} = \frac{R'_{общ}}{R^{исх}_{общ}} . \tag{15}$$

На современном рынке средств безопасности в настоящее время сотни фирм предлагают свою продукцию покупателю. Выбор конкретных средств безопасности, устанавливаемых на объекте, в условиях подобного разнообразия затруднен. Необходимо учесть весь спектр технических характеристик каждого элемента каждой подсистемы КТСБ, а также сравнить средства по характеристикам и цене. Все подсистемы КТСБ в принципе имеют одинаковую структуру, оценить которую можно, используя *показатель технического качества*, который зависит от совокупности технических характеристик элементов подсис-

тем. Поскольку эти структуры похожи, то и алгоритм подсчета данного показателя будет универсален для всех подсистем. В главе рассмотрено нахождение подобного показателя на примере системы охранно-пожарной сигнализации (ОПС). Показатель технического качества *i*-го элемента представлен в виде функции от технических и надежностных характеристик устройства: $K^i_{кач} = f(d^i_1, d^i_2, ..., d^i_n)$, где d^i_j – *j*-ая нормированная характеристика *i*-го устройства системы, $j = \overline{1, n}$. В качестве функции *f* может быть использована линейная «свертка» характеристик d^i_j вида

$$K^i_{кач} = \sum_{j=1}^{n} w_j d^i_j , \qquad (16)$$

где w_j – вес *j*-й характеристики, показывающий ее важность (значимость) для итогового значения показателя технического качества.

Для вычисления показателя качества функционирования системы необходимо:

1) произвести свертку технических и надежностных характеристик элементов в одну функцию – показатель качества $K^i_{кач}$ для выбранного типа датчиков (формула (16));

2) произвести свертку показателей качества $K^i_{кач}$ в одну функцию – обобщенный (агрегированный) показатель качества $K_{кач}$ системы ОПС

$$K_{кач} = \prod_{i=1}^{m} K^i_{кач} \text{ или } K_{кач} = \sum_{i=1}^{m} w_i K^{\text{i}}_{\text{кач}} . \qquad (17)$$

Оптимизация заключается в достижении наивыгоднейшего (максимального) значения критерия эффективности (показателя качества). При этом следует учитывать не только показатели технического качества совокупности технических средств, но и стоимость проектного решения. А это два показателя, находящихся в обратной зависимости друг к другу. Чем выше качество предлагаемого решения, тем больше будет и его стоимость. Возможны две постановки задачи оптимального выбора оборудования КТСБ:

1. Максимизация показателя качества системы безопасности (*K*), при ограниченном объеме выделенных для этой цели финансовых средств ($C_{\text{доп}}$): $K \to \max$, при $\sum_k C_k \le C_{доп}$.

2. Минимизация объема выделенных на создание системы безопасности финансовых средств, при достижении заданного уровня качества системы безопасности ($K_{\text{доп}}$): $\sum_k C_k \to \min$, при $K \ge K_{доп}$.

Значения $C_{\text{доп}}$ и $K_{\text{доп}}$ задаются экспертно специалистами по безопасности.

Для нахождения оптимального варианта возможно применение различных методов математического программирования (например, градиентных методов), а также методов стохастического поиска. В работе предложено использование для поставленной цели генетических алгоритмов (ГА). По своей сути,

ГА представляют собой метод параллельного поиска глобального экстремума, основанный на использовании в процессе поиска сразу нескольких, закодированных в хромосомы точек (кандидатов на решения), которые образуют развивающуюся по определенным случайным законам популяцию.

С использованием ГА разработан алгоритм оптимизации проектных решений и проведена его проверка на примере выбора комплекса технических средств для ОПС стандартного учебного кабинета университета. Система ОПС кабинета университета включает в себя 5 типов датчиков. Оптимизация заключается в выборе необходимого состава датчиков таким образом, чтобы выполнялось условие первой постановки задачи оптимизации.

Для начала технические характеристики датчиков приводятся к нормированному виду. Далее находится значение функции $K^{i}_{кач}$ для *i*-го датчика ОПС, которое вычисляется по формуле (16). Для получения значения общего качества функционирования системы применяется формула (17). В качестве функции пригодности для ГА используется целевая функция $P(x)=K_{кач}$. Для программной реализации генетического алгоритма был использован набор инструментов GAOT (Genetic Algorithm Optimization Toolbox) пакета Matlab 7.0.

Генетический алгоритм из множества вариантов комплектации системы (на каждое установочное место претендовали 5–6 датчиков различных производителей) нашел оптимальный состав при ограничении средств $C_{доп}$ = 2500 руб.

В четвертой главе рассматривается разработанный исследовательский прототип СППР СОТУ безопасностью вуза. С использованием программно реализованного модуля «Методика оценки текущего состояния СОТУ безопасностью вуза» в качестве примера была проведена оценка $УБ_{тек}$ для УГАТУ. Целевой уровень безопасности в соответствии с категорией вуза был определен как высокий. По результатам оценки предложены мероприятия по повышению уровня безопасности, ставшие основой для принятия «Концепции обеспечения безопасности УГАТУ». Время, затрачиваемое на анализ и предоставление полного отчета по СОТУ безопасностью вуза, при этом, снижается (по результатам экспертного оценивания) в 4–6 раз.

Для оценки применимости предложенного подхода к анализу риска был реализован программный прототип, который позволил применить предложенные для анализа риска при наличии средств безопасности формулы, а также показал, что предлагаемый показатель относительного риска может быть использован в качестве показателя эффективности функционирования СОТУ безопасности вуза.

Для программной реализации примера оптимизации комплекта ОПС для учебного кабинета университета был разработан программный прототип, позволивший сравнить два метода оптимизации – метод ветвей и границ (МВГ) и ГА. При программной реализации примера, МВГ показал превосходство по временным затратам над генетическим алгоритмом. Это связано с тем, что оптимизация состояла всего из 7776 переборов, а такого количества тестов для применения генетических алгоритмов недостаточно. Для ГА выигрыш в скоро-

сти оптимизации достигается за счёт отсеивания заведомо убыточных комбинаций параметров, а при малом количестве вариантов генетические алгоритмы не могут определить, какие «родители» дадут плохое «потомство». При увеличении же количества элементов, входящих в комплект (n), а также числа рассматриваемых альтернатив для каждого типа элемента (m), рост количества перебираемых вариантов значителен, т.к. имеет вид степенной зависимости m^n, что обусловливает резкий рост времени полного перебора вариантов с использованием МВГ и генетические алгоритмы показывают свои преимущества (рисунок 6).

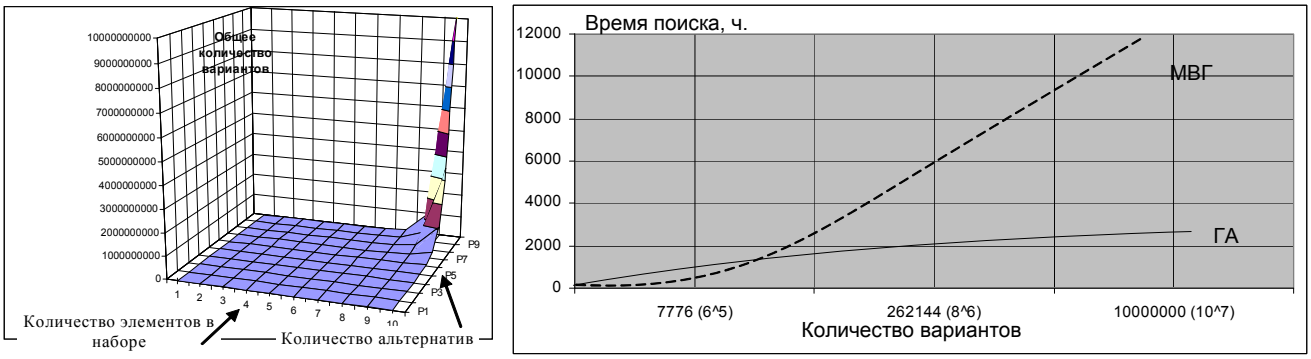

Рисунок 6 – Рост временных затрат для МВГ и ГА с ростом размерности задачи

ОСНОВНЫЕ РЕЗУЛЬТАТЫ И ВЫВОДЫ

Проведенный в работе анализ состояния проблемы управления безопасностью вуза показал практически полное отсутствие методических разработок в данной области. Однако то, что вузы относятся к объектам социальной значимости и являются специфичными по многим признакам объектами, определило необходимость разработки методического и алгоритмического обеспечения управления их безопасностью. Таким образом, основными результатами диссертационной работы являются:

1. На основе принципов интегрированного описания процессов IDEF0, с учетом требований стандарта ISO 27001, построены модели бизнес-процессов по созданию СОТУ безопасностью вуза, разработана ее структура. Текущее состояние СОТУ безопасностью вуза предложено оценивать с использованием разработанной «Методики оценки текущего состояния СОТУ безопасностью вуза». Данная методика позволяет оценивать как текущий уровень обеспечения безопасности вуза, так и состояние управления безопасностью вуза.
2. Предложена модель анализа риска, основанная на модели системы с полным перекрытием каналов воздействия угроз и использовании марковских моделей. Данная модель учитывает возможность столкновения с различными типами злоумышленников, а также различные распределения вероятности выбора данными злоумышленниками угроз. При оценке риска с учетом влияния средств обеспечения безопасности предложено рассматривать рубежи задержки распространения и обнаружения угроз с соответствующими характеристиками.

В качестве количественной меры эффективности функционирования СОТУ безопасностью вуза предложено использовать значение относительного риска $\overline{R}$, отражающего меру снижения потенциального ущерба ресурсам вуза при использовании средств КТСБ по отношению к исходному значению риска. Разработан подход к оценке данного показателя и его компонент.

3. Предложен подход к оптимизации состава комплекса технических средств безопасности, основанный на оптимизации показателя технического качества системы с использованием генетического алгоритма. Рассмотрен пример применения ГА для поиска оптимального состава средств ОПС учебного кабинета вуза. Проведено сравнение ГА с методом ветвей и границ. При программной реализации примера, метод ветвей и границ показал превосходство по временным затратам над генетическим алгоритмом. Однако было показано, что генетические алгоритмы позволяют получить значительный выигрыш по времени при росте количества рассматриваемых вариантов, числа рассматриваемых альтернатив и мест их установки.

4. Разработанный исследовательский прототип СППР по организационно-техническому управлению безопасностью вуза объединяет модули «Оценки текущего состояния СОТУ безопасностью вуза», «Оценки риска ресурсам», «Оптимизации состава КТСБ», реализованные по отдельности и доступные через единый интерфейс СППР СОТУ. Прототип подтвердил применимость предложенных методик и подходов, в частности, с помощью модуля «Оценки текущего состояния СОТУ безопасностью вуза» была проведена оценка текущего уровня безопасности УГАТУ. По результатам оценки сформирован комплекс мероприятий, ставший основой «Концепции обеспечения безопасности УГАТУ». Применение указанного модуля позволяет снизить временные затраты на данные работы в 4–6 раз.

ОСНОВНЫЕ ПУБЛИКАЦИИ ПО ТЕМЕ ДИССЕРТАЦИИ

В рецензируемых журналах из списка ВАК

1. Разработка методологических основ создания и внедрения комплексной системы безопасности вуза / В. И. Васильев, Т. А. Иванова // Вестник УГАТУ: научн. журн. Уфимск. гос. авиац. техн. ун–та. 2006. № 2 (18). С. 40–42.

В других изданиях

2. Алгоритм проектирования оптимальной структуры комплексной системы безопасности на основе анализа риска / В.И. Васильев, Т.А. Иванова // Информационная безопасность : матер. 7-й Междунар. науч.–практ. конф. Таганрог : Изд-во ТРТУ, 2005. С. 270–274.

3. Проектирование комплексных систем защиты информации на основе анализа риска / В.И. Васильев, Т.А. Иванова // Компьютерные науки и информационные технологии : тр. 7-й Междунар. конф. (CSIT’2005). Уфа : Изд-во УГАТУ, 2005. Т. 2. С. 200–206 (На англ. яз.).

4. Концепция обеспечения комплексной безопасности высшего учебного заведения / В.И. Васильев, С.Н. Зарипов, Т.А. Иванова, Т.З. Хисамутдинов // Проблемы техники и технологии телекоммуникаций : матер. VI Междунар. науч.–техн. конф. Уфа : Изд-во УГАТУ, 2005. С.189–192.

5. Методологические проблемы проектирования комплексной системы безопасности вуза / М.Б. Гузаиров, В.И. Васильев, С.Н. Зарипов, Т.А. Иванова // Мавлютовские чтения : рос. науч.–техн. конф. : сб. тр. Уфа : УГАТУ, 2006. Т. 1. С. 70–76.

6. К вопросу о выборе критериев эффективности комплексных систем безопасности / В.И. Васильев, Т.А. Иванова, А.А. Бакиров // Информационная безопасность : матер. 8-й Междунар. науч.–практ. конф. Таганрог : Изд-во ТРТУ, 2006. Ч. 1. С. 76–79.

7. Проектирование комплексных систем безопасности высших учебных заведений (основные принципы) / Т.А. Иванова // Компьютерные науки и информационные технологии : тр. 8-й Междунар. конф. (CSIT'2006). Карлсруэ, Германия, 2006. Т. 2. С. 177–179 (На англ. яз.).

8. Особенности проектирования комплексной системы безопасности вуза / Т.А. Иванова // XXXII Гагаринские чтения : науч. тр. Междунар. молодёжн. науч. конф. М. : МАТИ, 2006. Т. 8. С. 16–18.

9. Применение генетических алгоритмов для оптимизации состава технических средств безопасности / Ю.Г. Строкина, Т.А. Иванова, Л.М. Исхакова // Компьютерные науки и информационные технологии : тр. 9-й Междунар. конф. (CSIT'2007). Уфа–Красноусольск, 2007. С. 168–172 (На англ. яз.).

10. Комплексная система безопасности вуза, оценка эффективности ее функционирования / Т.А. Иванова // Интеллектуальные системы обработки информации и управления. Т. 1. Информатика, управление и компьютерные науки: сб. ст. 2-й рег. зимн. шк.–сем. аспирантов и молодых ученых. Уфа : Технология, 2007. С. 178–183.

11. Организационное и техническое обеспечение комплексной системы безопасности высшего учебного заведения / Т.А. Иванова // Актуальные проблемы в науке и технике. Т. 1. Информатика, управление и компьютерные науки : сб. ст. 3-й Всерос. зимн. шк.–сем. аспирантов и молодых ученых. Уфа : Диалог, 2008. С. 308–314.

12. Методика расчета экономической эффективности проекта создания КСБ вуза / Т.А. Иванова, С.Н. Зарипов, В.Ю. Васильев // Актуальные проблемы в науке и технике. Т. 1. Информатика, управление и компьютерные науки : сб. ст. 4-й Всерос. зимн. шк.–сем. аспирантов и молодых ученых. Уфа : Диалог, 2009. С. 227–231.

Диссертант Т.А. Иванова

ИВАНОВА Татьяна Александровна

МЕТОДИЧЕСКОЕ И АЛГОРИТМИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ОРГАНИЗАЦИОННО-ТЕХНИЧЕСКОГО УПРАВЛЕНИЯ КОМПЛЕКСНОЙ БЕЗОПАСНОСТЬЮ ВЫСШЕГО УЧЕБНОГО ЗАВЕДЕНИЯ

Специальность 05.13.10 –
Управление в социальных и экономических системах

А В Т О Р Е Ф Е Р А Т
диссертации на соискание ученой степени
кандидата технических наук

Подписано к печати 28.09.2009. Формат 60х84 1/16.
Бумага офсетная. Печать плоская. Гарнитура Таймс.
Усл. печ. л. 1,0. Усл. кр. – отт. 1,0. Уч. – изд. л. 0,9.
Тираж 100 экз. Заказ № 467

ГОУ ВПО Уфимский государственный авиационный технический университет
Центр оперативной полиграфии
450000, Уфа-центр, ул. К.Маркса, 12.