Министерство образования и науки Российской Федерации
Федеральное государственное автономное образовательное учреждение
высшего образования
**«НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ
ТОМСКИЙ ПОЛИТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ»**

Институт Физико-технический
Направление подготовки Ядерные физика и технологии
Кафедра Физико-энергетических установок

МАГИСТЕРСКАЯ ДИССЕРТАЦИЯ

Тема работы
Разработка алгоритмов оценки эффективности системы безопасности территориально – распределенного объекта

УДК 621.039.58:511.215

Студент

Группа	ФИО	Подпись	Дата
0АМ4В	Мерзляков Александр Александрович		

Руководитель

Должность	ФИО	Ученая степень, звание	Подпись	Дата
Старший преподаватель каф. ФЭУ ФТИ	Годовых А.В.			

КОНСУЛЬТАНТЫ:

По разделу «Финансовый менеджмент, ресурсоэффективность и ресурсосбережение»

Должность	ФИО	Ученая степень, звание	Подпись	Дата
Доцент каф. МЕН ИСГТ	Верховская М.В.	к.экон.н.		

По разделу «Социальная ответственность»

Должность	ФИО	Ученая степень, звание	Подпись	Дата
Ассистент каф. ПФ ФТИ	Гоголева Т.С.	к.ф.-м.н.		

ДОПУСТИТЬ К ЗАЩИТЕ:

Зав. кафедрой	ФИО	Ученая степень, звание	Подпись	Дата
ФЭУ	Долматов О.Ю.	к.ф.-м.н., доцент		

Томск – 2016 г.

ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОБУЧЕНИЯ ООП

Код результата	**Результат обучения**
	Профессиональные компетенции
Р1	Применять глубокие, математические, естественнонаучные, социально-экономические и профессиональные знания для теоретических и экспериментальных исследований в области использования ядерной энергии, ядерных материалов, систем учета, контроля и физической защиты ядерных материалов, технологий радиационной безопасности, медицинской физики и ядерной медицины, изотопных технологий и материалов в профессиональной деятельности.
Р2	Ставить и решать инновационные инженерно-физические задачи, реализовывать проекты в области использования ядерной энергии, ядерных материалов, систем учета, контроля и физической защиты ядерных материалов, технологий радиационной безопасности, медицинской физики и ядерной медицины, изотопных технологий и материалов.
Р3	Создавать теоретические, физические и математические модели, описывающие конденсированное состояние вещества, распространение и взаимодействие ионизирующих излучений с веществом и живой материей, физику кинетических явлений, процессы в реакторах, ускорителях, процессы и механизмы переноса радиоактивности в окружающей среде.
Р4	Разрабатывать новые алгоритмы и методы: расчета современных физических установок и устройств; исследования изотопных технологий и материалов; измерения характеристик полей ионизирующих излучений; оценки количественных характеристик ядерных материалов; измерения радиоактивности объектов окружающей среды; исследований в радиоэкологии, медицинской физике и ядерной медицине.
Р5	Оценивать перспективы развития ядерной отрасли, медицины, анализировать радиационные риски и сценарии потенциально возможных аварий, разрабатывать меры по снижению рисков и обеспечению ядерной и радиационной безопасности руководствуясь законами и нормативными документами, составлять экспертное заключение.
Р6	Проектировать и организовывать инновационный бизнес, разрабатывать и внедрять новые виды продукции и технологий, формировать эффективную стратегию и активную политику риск-менеджмента на предприятии, применять методы оценки качества и результативности труда персонала, применять знание основных положений патентного законодательства и авторского права Российской Федерации.
	Общекультурные компетенции
Р7	Демонстрировать глубокие знания социальных, этических и культурных аспектов инновационной профессиональной деятельности.
Р8	Самостоятельно учиться и непрерывно повышать квалификацию в течение всего периода профессиональной деятельности.
Р9	Активно владеть иностранным языком на уровне, позволяющем работать в иноязычной среде, разрабатывать документацию, презентовать результаты профессиональной деятельности.
Р10	Эффективно работать индивидуально и в коллективе, демонстрировать ответственность за результаты работы и готовность следовать корпоративной культуре организации.

Министерство образования и науки Российской Федерации
федеральное государственное автономное образовательное учреждение
высшего образования
**«НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ
ТОМСКИЙ ПОЛИТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ»**

Институт Физико-технический
Направление подготовки 14.04.02 Ядерная физика и технологии
Кафедра Физико-энергетические установки

УТВЕРЖДАЮ:
Зав. кафедрой
О. Ю. Долматов
(Подпись) (Дата) (Ф.И.О.)

ЗАДАНИЕ
на выполнение выпускной квалификационной работы

В форме:

Магистерской диссертации

Студенту:

Группа	**ФИО**
0АМ4В	Мерзлякову Александру Александровичу

Тема работы:

Разработка алгоритмов оценки эффективности системы безопасности территориально – распределенного объекта	
Утверждена приказом директора (дата, номер)	26.02.2016 № 1618/с

Срок сдачи студентом выполненной работы:	20.06.2016

ТЕХНИЧЕСКОЕ ЗАДАНИЕ:

Исходные данные к работе	Методология оценки эффективности системы безопасности территориально – распределенного объекта должна предусматривать: – наличие исходных данных необходимых для формирования требований к построению основных типов систем безопасности; – представление основных опасных событий и угроз в отношении территориально-распределенного объекта/

Перечень подлежащих исследованию, проектированию и разработке вопросов	– сбор исходных данных для формирования требований к построению основных типов систем безопасности, принципов организации, функционирования и структурных компонентов систем безопасности; – формирование перечня угроз в отношении объекта исходя из его характерных параметров; – разработка/адаптация полученных методик и их применение для оценки эффективности системы безопасности выбранного объекта.
Перечень графического материала	Схема базовой части модели совокупности угроз безопасности в отношении территориально – распределенного объекта – обязательный чертёж

Консультанты по разделам выпускной квалификационной работы

Раздел	Консультант
Финансовый менеджмент, ресурсоэффективность и ресурсосбережение	М. В. Верховская
Социальная ответственность	Т. С. Гоголева
Иностранный язык	Я. В. Ермакова

Названия разделов, которые должны быть написаны на русском и иностранном языках:

Введение
Методическая основа построения систем безопасности
Методы проведения оценки эффективности системы безопасности территориально распределенного объекта
Разработка методики оценки эффективности объекта по основным мерам защиты
Оценка коммерческого потенциала и перспективности проведения исследования с позиции ресурсоэффективности и ресурсосбережения
Безопасность использования и анализа данных при помощи электронной вычислительной машины
Заключение

Дата выдачи задания на выполнение выпускной квалификационной работы по линейному графику	01.02.2016

Задание выдал руководитель:

Должность	ФИО	Ученая степень, звание	Подпись	Дата
ст. преподаватель	А. В. Годовых			01.02.2016

Задание принял к исполнению студент:

Группа	ФИО	Подпись	Дата
0АМ4В	Мерзляков Александр Александрович		01.02.2016

ЗАДАНИЕ ДЛЯ РАЗДЕЛА
«ФИНАНСОВЫЙ МЕНЕДЖМЕНТ, РЕСУРСОЭФФЕКТИВНОСТЬ И РЕСУРСОСБЕРЕЖЕНИЕ»

Студенту:

Группа	ФИО
0АМ4В	Мерзлякову Александру Александровичу

Институт	Физико-технический	Кафедра	ФЭУ
Уровень образования	Магистратура	**Направление/специальность**	14.04.02 Ядерные физика и технологии/ Ядерные реакторы и энергетические установки

Исходные данные к разделу «Финансовый менеджмент, ресурсоэффективность и ресурсосбережение»:	
1. *Стоимость ресурсов научного исследования (НИ): материально-технических, энергетических, финансовых, информационных и человеческих*	Работа с информацией, представленной в российских и иностранных научных публикациях, аналитических материалах, статистических бюллетенях и изданиях, нормативно-правовых документах
2. *Нормы и нормативы расходования ресурсов*	
3. *Используемая система налогообложения, ставки налогов, отчислений, дисконтирования и кредитования*	
Перечень вопросов, подлежащих исследованию, проектированию и разработке:	
1. *Оценка коммерческого потенциала, перспективности и альтернатив проведения НИ с позиции ресурсоэффективности и ресурсосбережения*	Оценочная карта конкурентных технических решений
2. *Планирование и формирование бюджета научных исследований*	Иерархическая структура работ SWOT-анализ Календарный план-график реализации проекта
3. *Оценка ресурсной, финансовой, социальной, бюджетной эффективности научного исследования*	Определение ресурсоэффективности проекта

Перечень графического материала *(с точным указанием обязательных чертежей)*

1. *Оценочная карта конкурентных технических решений*
2. *Матрица SWOT*
3. *Иерархическая структура работ*
4. *Календарный план проекта*
5. *Бюджет проекта*
6. *Определение ресурсоэффективности проекта*

Дата выдачи задания для раздела по линейному графику	

Задание выдал консультант:

Должность	ФИО	Ученая степень, звание	Подпись	Дата
Доцент каф. МЕН ИСГТ	Верховская М.В.	к.экон.н.		

Задание принял к исполнению студент:

Группа	ФИО	Подпись	Дата
0АМ4В	Мерзляков Александр Александрович		

ЗАДАНИЕ ДЛЯ РАЗДЕЛА
«СОЦИАЛЬНАЯ ОТВЕТСТВЕННОСТЬ»

Студенту:

Группа	ФИО
0АМ4В	Мерзлякову Александру Александровичу

Институт	Физико-технический	Кафедра	ФЭУ
Уровень образования	Магистратура	**Направление/специальность**	14.04.02 Ядерные физика и технологии/ Ядерные реакторы и энергетические установки

Исходные данные к разделу «Социальная ответственность»:	
1. *Описание рабочего места (рабочей зоны) на предмет возникновения:*	– вредных факторов производственной среды (микроклимат, освещение, шумы, электромагнитные поля, ионизирующее излучение); – опасных факторов производственной среды (электрической, пожарной и взрывной природы).
2. *Знакомство и отбор законодательных и нормативных документов по теме*	электробезопасность, пожаробезопасность, требования при работе на ПЭВМ
Перечень вопросов, подлежащих исследованию, проектированию и разработке:	
1. *Анализ выявленных вредных факторов проектируемой производственной среды в следующей последовательности:*	– воздействие на организм человека; – приведение допустимых норм; – предлагаемые средства защиты.
2. *Анализ выявленных опасных факторов проектируемой произведённой среды в следующей последовательности:*	– электробезопасность (в т.ч. статическое электричество, средства защиты); – пожаровзрывобезопасность (причины, профилактические мероприятия, первичные средства пожаротушения).

Дата выдачи задания для раздела по линейному графику	

Задание выдал консультант:

Должность	ФИО	Ученая степень, звание	Подпись	Дата
Ассистент каф. ПФ ФТИ	Гоголева Т.С.	к.ф.-м.н.		

Задание принял к исполнению студент:

Группа	ФИО	Подпись	Дата
0АМ4В	Мерзляков Александр Александрович		

Реферат

Выпускная квалификационная работа содержит 101 страницу, 3 рисунка, 14 таблиц, 35 источников, 3 приложения, 1 лист графического материала.

Ключевые слова: территориально – распределенный объект, оценка эффективности системы безопасности объекта, модель угроз безопасности, перечень угроз, структурные компоненты.

Объектом исследования являются объекты относящиеся к категории территориально – распределенных.

Цель работы – разработка алгоритмов оценки эффективности системы безопасности территориально – распределенного объекта.

В процессе исследования проводились мероприятия по изучению основных типов систем безопасности, принципов организации, функционирования и структурных компонентов систем безопасности, формирование перечня угроз в отношении объекта, разработка методологии построения модели угроз безопасности для ТРО.

В результате исследования получена методологический подход к построению модели угроз безопасности для территориально – распределенного объекта.

Область применения: объекты относящиеся к категории территориально – распределенных с многофункциональным целевым назначением.

Значимость работы: предлагаемый методологический подход позволяет проводить анализ возможных угроз в отношении территориально – распределенного объекта, способов их идентификации, тем самым повысив надежность системы безопасности ТРО.

Список используемых сокращений:

Территориально – распределенный объект; ТРО

Объект исследования; ОИ

Система безопасности; СБ

Интегрированная система безопасности; ИСБ

Показатель исхода операции; ПИО

Предварительный анализ опасностей; ПАО

Опасные вещества и материалы; ОВМ

Комплексная система обеспечения безопасности; КСОБ

Нормативно-справочная информация; НСИ

Оглавление

Введение

Основа эффективного обеспечения безопасности любого объекта – создание достоверной модели угроз безопасности, содержащей ранжированные по выбранным показателям угрозы безопасности и их источники, а также определяющей возможные последствия от реализации этих угроз – вред, ущерб. В общем случае модель угроз безопасности – информационная модель, содержащая совокупность сведений, характеризующих состояние безопасности объекта при возникновении определённых опасных событий, процессов, явлений, а также отношений объекта с внешним миром. По способу представления эти модели относятся, как правило, к вербальным информационным моделям, формирующимся в описательном виде в результате логических умозаключений и сопоставительного анализа при структуризации и определении взаимосвязи основных компонентов – в нашем случае источников угроз безопасности и объектов в части обеспечения их безопасности. Эти факторы требуют специфического подхода к методологии построения модели угроз безопасности, к выработке логики проведения сопоставительного анализа и формирования последующих утверждений. С точки зрения обеспечения безопасности, наиболее сложными являются территориально-распределённые объекты (системы) с многофункциональным целевым предназначением. К сожалению, целостной и связной методологии построения моделей угроз для подобного рода сложных объектов в настоящее время не сложилось.

Для достижения безопасности следует осуществлять всесторонний анализ потенциальных угроз, помогающий разработать эффективные средства защиты и минимизировать возможные риски.

Комплексная безопасность предприятия – это система выявления, предупреждения и пресечения посягательств на законные права предприятия, его имущество, интеллектуальную собственность, производственную дисциплину, научные достижения и охраняемую информацию.

Концепция системы безопасности объекта определяет цели и задачи системы безопасности, принципы ее организации, функционирования, правовые основы, виды угроз безопасности и ресурсы, подлежащие защите, а также основные направления разработки системы безопасности, включая правовую, организационную и инженерно-техническую защиту.

Целью данной работы является разработка алгоритмов оценки эффективности системы безопасности территориально – распределенного объекта.

Для достижения поставленной цели необходимо выполнить следующие задачи:

– сбор исходных данных для формирования требований к построению основных типов систем безопасности, принципов организации, функционирования и структурных компонентов систем безопасности;

– формирование перечня угроз в отношении объекта исходя из его характерных параметров;

– разработка/адаптация полученных методик и их применение для оценки эффективности системы безопасности выбранного объекта.

1 Методическая основа построения систем безопасности

1.1 Система безопасности объекта

Основная цель системы комплексной безопасности – обеспечить для предприятия возможность успешно осуществлять деятельность в условиях нестабильности внутренней и внешней среды организации, своевременно распознавать и предотвращать все возможные угрозы, охранять здоровье и жизнь работников.

Под безопасностью объекта понимается состояние защищенности интересов владельцев, руководства и клиентов предприятия, материальных ценностей и информационных ресурсов от внутренних и внешних угроз.

Таким образом, концепция безопасности объекта – это научно-обоснованная система взглядов на определение основных направлений, условий и порядка практического решения задач защиты, общий замысел обеспечения безопасности объекта от прогнозируемых угроз. Цели системы безопасности:

– обеспечение устойчивого функционирования предприятия и предотвращение угроз его безопасности;

– защита законных интересов организации от противоправных посягательств;

– недопущение хищения финансовых и материально-технических средств, уничтожения имущества и ценностей;

– недопущение разглашения, утраты, утечки, искажения и уничтожения служебной информации;

– предотвращение нарушения работы технических средств, средств обеспечения производственной деятельности, включая и средства информатизации.

– охрана жизни и здоровья персонала.

Задачи системы безопасности:

– прогнозирование, своевременное выявление и устранение угроз безопасности персоналу и ресурсам объекта исследования (ОИ);

– причин и условий, способствующих нанесению финансового, материального и морального ущерба, нарушению его нормального функционирования и развитию;

– создание механизма и условий оперативного реагирования на угрозы безопасности и проявление негативных тенденций в функционировании ОИ;

– создание условий для максимально возможного возмещения и локализации наносимого ущерба неправомерным действиям физических и юридических лиц, ослабление негативного влияния последствий нарушения безопасности на достижение стратегических целей ОИ. Основными составляющими обеспечения безопасности объектов являются:

– система физической защиты (безопасности) материальных объектов и финансовых ресурсов;

– система безопасности инфокоммуникационных ресурсов.

Система обеспечения безопасности инфокоммуникационных ресурсов должна предусматривать комплекс организационных, технических, программных и криптографических средств и мер по защите информации в процессе традиционного документооборота при работе исполнителей с конфиденциальными документами и сведениями, при обработке информации в автоматизированных системах различного уровня и назначения, при передаче по каналам связи.

Система физической безопасности материальных объектов должна предусматривать:

– систему охраны (инженерно-технических и организационных мер);

– систему регулирования доступа;

– систему мер (режима) сохранности и контроль вероятных каналов утечки информации;

– систему мер возврата материальных ценностей (или компенсации).

1.2 Структурные компоненты архитектуры систем безопасности

Основными структурными компонентами архитектуры безопасности являются базовые программно-аппаратные и программно-методические комплексы, которые проектным путем объединяются в «индивидуальную» систему безопасности для конкретных условий применения на одном или нескольких объектах и на разных уровнях их управления.

Функционально полный набор компонент систем комплексной безопасности является основой создания системы мониторинга безопасности, инфраструктуры государства, регионов, муниципальных образований и поселений, корпораций и отдельных предприятий. Создание распределенной сети центров мониторинга безопасности территории (общественной, экологогической, противопожарной, антитеррористической, промышленной и др.), работающих на основе согласованных регламентов взаимодействия, стандартов открытых систем и протоколов обмена данными.

1.3 The hazards facing operators of critical infrastructures

The hazards facing operators of critical infrastructures can be broken down into hazards relating to natural events, hazards relating to human error or technical failure and hazards relating to terrorism or criminal acts. In this connection it is to be noted that an entire facility or security-critical parts of a facility may also be affected

by events outside of the actual facility, in neighbouring operational areas or traffic facilities to which a special threat potential applies (domino effect). Possible impacts in this respect include the spread of fire from neighbouring facilities, flying debris after an explosion in neighbouring facilities, the failure of supplies after catastrophic events outside of the facility, etc. Events occurring within a short time of each other, such as a second, delayed explosion or several incidents occurring around the same time at different locations, may also entail an exponential effect by preventing rescue or restoration measures or causing resources to be concentrated in the wrong place, for example (diversionary measures).

The following overview is intended to illustrate the complexity and heterogeneity of the risk factors which require to be considered. It does not purport to be an exhaustive synopsis:

- risk factor: People:
  - inadequate security consciousness;
  - inadequately qualified personnel;
  - human error ;
  - criminal behaviour (sabotage, terrorist attacks).
  - risk factor: Organisation:
  - concentration of vital resources;
  - outsourcing of infrastructures which are critical to the company.
- risk factor: Nature/environment:
  - natural disasters;
  - epidemics.
- risk factor: IT:
  - complexity of systems;
  - increasing IT-dependency;
  - extensive, worldwide networking of IT systems;

- short IT innovation cycles;
- standardisation of technology and components;
- networking/interdependencies of critical infrastructures;
- internet as nerve system of critical infrastructures (connection to IT security).

1.3.1 Hazards through natural events

Extreme weather situations. According to information from the insurance industry, a large proportion of elementary damage in Germany results from extreme atmospheric events. These include events such as high water (incl. rising of the groundwater level), flooding, storm tides, snow, ice, droughts and storms. Particular hazards apply during flooding as a result of the massive erosive impact of water on roads, bridges, dams etc. and from flotsam. The danger of drinking water contamination and attendant substantial health risks is increased by leaking harmful substances and refuse which are carried off in the floods. Rising groundwater levels may also cause flooding in more distant areas.

Hurricanes and hail may result from heavy thunderstorms and give rise to additional dangers. Air movements at a velocity of 75 km/h and over are defined as storms, while air movements of 120 km/h and over qualify as hurricanes. In addition to direct damage caused by wind pressure and subsequent gusts, storms and hurricanes can give rise to additional hazards resulting from debris and dirt which are entrained by the violently rotating funnel of a hurricane. Storms play a predominant role in terms of both frequency and the percentage share of damage caused to the economy.

In isolated cases, hailstones can measure over 10 cm and weigh more than a kilogram. Apart from causing damage to property and crops, hailstones can also inflict serious injury. Hailstones can also block water run-offs, resulting in flooding.

Earthquakes. The level of danger resulting from earthquakes inevitably rises according to the intensity of the earthquake. Depending on geological parameters such as soil characteristics, however, weaker earthquakes can also cause extensive damage to buildings and infrastructures. Secondary damage such as fires and tidal waves may also require consideration.

Conflagrations can be caused naturally by lightning, by spontaneous combustion or by wilful or negligent arson in combination with prolonged dry periods. The primary threat is to wooded areas, agricultural land and heathland.

Mass movements. Mass movements are caused by geophysical events (e.g. earthquakes, weathering), meteorological influences (e.g. heavy precipitation, flooding, snow and ice melts) and by anthropogenic influences (e.g. building measures, shock, deforestation). Examples of mass movements are avalanches, mudflows, hillside landslides and liquefaction of the soil. Apart from direct damage, mass movements can also give rise to indirect hazards, by creating tidal waves in lakes or reservoirs or damming up rivers which subsequently burst free.

Epidemics. The term «epidemic» refers to the occurrence of an infectious disease among humans or animals at high incidence within a short period of time over a broad geographic area. An increased risk of epidemics results from the global movement of goods, global tourism, intensive livestock farming, floods and droughts, for example. A pandemic is an epidemic which spreads throughout several countries or even worldwide.

1.3.2 Hazards through human and technical failure

Fires. A fire may spread out of control as a result of human error, technical failure, arson , lightning, the release of hazardous substances or following explosions. Fires are classified according to their size as small-scale, medium-scale (e.g. fires in buildings) and large-scale fires (e.g. fires at industrial enterprises, large-scale plants, warehouses).

Release of hazardous substances. Hazardous substances include all substances of an atomic, biological, chemical or radiological nature which can have a harmful effect on the environment or humans and/or may lead to explosions and fires. The properties of hazardous substances vary greatly, ranging from irritating through highly inflammable to explosive, environmentally hazardous, chronically harmful and toxic. The hazardous substances used at a company can be identified by means of an individual register of hazardous substances.

Explosions. An explosion is caused by a sudden expansion in the volume of gases due to the release of energy, leading to a blast wave and possibly also involving the generation of heat. Explosions result from human error, technical failure, wilful acts, lightning or the release of hazardous substances. Other physical impacts from inside and outside Physical impacts from inside and outside can be caused by accidents such as traffic or industrial accidents and plane crashes. Apart from destroying facilities, accidents can also lead to fires and explosions, to the release of hazardous substances and to other forms of damage.

1.3.3 Hazards through terrorism and criminal acts

Hazards relating to terrorism or criminal acts which are identified in the analysis of a company's general risk situation can be assigned to specific graduated risk categories. The respective levels here provide an overview of potential perpetrators, their possible or typical practices, their aims and motives and their degree of criminal energy. These risk levels enable a clear overview of which risks require to be considered.

While the assumptions within a risk category are based on empirical criminological knowledge, they must not apply precisely to every single case. Obviously, the question as to possible perpetrators and their mode of action cannot be answered with complete certainty. On the basis of experience acquired in safeguarding plants and facilities, however, it is possible to carry out rough

classification in a table defining the given levels of risk according to perpetrator groups, their typical motives and possible modes of behaviour. Acts of negligence are not included in this assessment, as they fall under hazards relating to human error and technical failure.

The extent to which potential perpetrators are actually able to cause serious damage and where such damage is possible and probable must be examined in the course of risk assessment, taking into account the points of danger identified in the company's environment. The risk categories contain a number of assumptions which are intended to enable allocation to the determined threat level. These assumptions primarily concern:

- possible background circumstances relating to the offence;
- possible motives and typical modes of action;
- resources which are likely to be employed;
- the level of criminal energy to be expected.

Interference options can also be identified as a means of differentiation, establishing a link between perpetrators, their motivations and the options for action offered by the nature of the infrastructures concerned. The following interference options are conceivable in principle.

Deliberate maloperation. This option covers all intentional actions whereby a malfunction could be triggered by simple means, without the use of any tools or resources. Such actions could include, for example: switching facilities on/off, opening/closing closures in piping systems (valves/gates), turning handwheels and actuating levers in the course of a process. Deliberate maloperation can be carried out by a companyís own personnel or by persons from outside the company.

Manipulation. Manipulation involves deliberately altering or adjusting parts of a system with the aim of inducing a critical status in the plant concerned. Possible examples here include programming control systems incorrectly, maladjusting measuring facilities, suppressing process signals, fault signals or alarms or shutting

down protective systems. Insiders with a precise knowledge of the facilities are the primary suspects here.

Vehicle accident. Hazardous substances could be released or important parts of facilities could be damaged or destroyed as a result of road or rail traffic accidents. Examples here include leaking drums resulting from fork-lift accidents, derailing of tank wagons, destruction of facilities by lorry impact.

Interference using simple tools. This category covers intentional interference, usually of a spontaneous nature, in important parts of facilities, using the tools and resources which are available at every plant. Examples here include smashing glass parts of a plant, clamping moving parts of a plant or adding prohibited substances or materials to the process. Company employees are the primary suspects here.

Interference using heavy tools. The planned violent destruction of parts of a plant is assumed for the purposes of this interference option. Possible tools employed in such attacks include crowbars, electric drills, flame cutters, bolt cutters or sledgehammers. Examples of such attacks include breaking open doors and subsequently destroying facilities, smashing up measurement and control facilities and smashing open containers and piping systems, resulting in large-scale leakages. Instead of a specific attack, vandalism may also occur, e.g. out of anger following a failed break-in.

Arson using simple resources. Simple resources cover ignition with matches, lighters or cigarette ends. This interference option thus only applies when sufficient quantities of combustible, highly inflammable materials are available. Examples here include igniting combustible liquids from a process, setting fire to storage locations to release hazardous substances, setting fire to peripheral rooms or facilities with subsequent impacts on important plant components.

Arson using fire-promoting resources. This category concerns fire attacks carried out with the aid of quickly and intensively burning materials. Examples of such attacks include pouring out and igniting combustible fluids (e.g. petrol),

throwing so-called «Molotov cocktails» (e.g. through windows) or installing professional incendiary compounds with timing or remote ignition devices. Such attacks can also be carried out from outside (throwing distance) and require a pronounced level of criminal energy. Use of explosives Home-made, commercial or military explosives could be used here. Possible forms of attack include setting off a home-made «fire-extinguisher bomb» inside sensitive parts of a facility or, more probably, at the periphery of a building, blowing up containers and piping systems, blowing away load-bearing components to cause containers to collapse, destroying plant components. This type of attack generally involves a radical political background and is carried out by perpetrators from outside the company.

Bombardment. Forms of bombardment can range from the simple use of air guns or catapults (steel balls) to the use of heavy weapons - e.g. anti-aircraft missiles - by terrorist perpetrators. Possible methods of interference here include causing leaks in outdoor containers or in pipelines, inducing an explosion. Bombardment is possible above all from outside the outer fencing of an operational area or industrial estate, whereby facilities installed in the vicinity of the fence are at a greater risk.

Plane crash. Both the kinetic energy of crashing aircraft and the explosive impact of the fuel or any explosives on board require to be considered here. An aircraft can also be used as a means of transport to propagate ABCR substances. Attacks leading to plane crashes may take place from outside, e.g. by rocket attack, remote ignition of explosives, remote manipulation of the on-board electronics, failure/abuse of air traffic control centres, or from inside by taking over/interfering with the control system or by igniting explosives (suicide attackers).

Depending on the availability of corresponding agents and resources, there is a broad range of conceivable possibilities requiring special discussion. Possible forms of deployment range from the intentional spreading of diseases (mailing of anthrax pathogens) or epidemics (introduction of highly infectious pathogens into supply systems or the air we breathe) through the use of so-called «dirty bombs» aimed at

causing sustained public disquiet to the use of poison gas at traffic junctions, for example.

Combined effects. A broad spectrum of possibilities is conceivable here, too, from the above-mentioned dirty bombs as a combination of explosive impact and radioactive contamination through the destruction of a production plant combined with the propagation of harmful substances to individual publicity grabbing actions with far-reaching consequences for corporate activities or public utilities.

1.4 Endangered areas in companies

Critical infrastructures, as well as individual production or service areas within a facility, are subject to different levels of risk from natural events, human error, technical failure, terrorism or criminal acts. At company level, additional risks can arise as a result of job cutting, the centralization and automation of control and monitoring processes, shifts in areas of responsibility resulting from outsourcing or the inadequate implementation of required measures as a result of cost pressure.

Areas especially endangered through natural events. Areas at special risk from extreme weather conditions Storm tides and flash floods can lead to the destruction of entire buildings and plants. Areas at particular risk include networks, buildings, production, extracting and processing plants and non-electronic data records. Slowly draining floods lead primarily to damage in lower-lying areas of buildings (basement, ground floor). As damage resulting from the effects of water generally leads to network failures, information and communication technology, the (internal) power supply, supply networks and other networks are at particular risk. Outside of flooded areas, such damage can be caused by rising groundwater levels.

All buildings and facilities are exposed to storms, irrespective of their location. At particular risk, however, are buildings and facilities in exposed locations (mountains, hills, mountain ridges, snow paths) and buildings and facilities whose

design exposes them to storms. Storms, as well as droughts or extreme frost, can also lead to supply shortages which threaten the continuation of normal operations.

Areas at special risk from earthquakes. Earthquakes can damage or destroy buildings and entire complexes and lead to failures and breakdowns in all areas. The risk of even minor tremors causing damage in the area of IT and in vibration-sensitive areas of production, extraction and processing cannot be ruled out.

Areas at special risk from conflagrations. Conflagrations can cause damage in all areas in which buildings or facilities are located. Conflagrations can additionally lead to entire areas or traffic routes being closed off, as a result of which facilities become difficult or impossible to access.

Areas at special risk from mass movements. Mass movements can damage or destroy buildings and facilities as a whole or block access to such buildings and facilities. Mass movements outside of a facility involving effects on external networks can also lead to supply shortages which threaten the continuation of normal operations.

Areas at special risk from epidemics. Epidemics can lead to unavailability or shortages with regard to the specialist personnel which is required to operate facilities. Production operations, computer centres and control centres would be particularly seriously affected by such circumstances. In addition, the closing-off of areas during human and livestock epidemics may render it difficult or impossible to access facilities.

1.4.1 Areas especially endangered through human and technical failure

Areas at special risk from fires. Fires can act on facilities and buildings from within and from outside. They can destroy or damage all areas, or they may prevent further use due to the effects of smoke. Even small fires in exposed parts of facilities (e.g. IT) may lead to failure of the entire facility.

Areas at special risk from hazardous substances. In addition to the primary risks of harm to the operating personnel and damage to the area surrounding the facility concerned, the release of hazardous substances may also induce explosions and fires. The further use of contaminated technical facilities, including IT equipment, may be impossible or restricted.

Areas at special risk from explosions. Explosions can impact on facilities and buildings from within and from outside. They may damage or destroy all areas and induce chain reactions. The primary destruction results from the blast wave; the initial explosion is often followed by fires. Even small fires in sensitive areas (IT, power) may lead to failure of the entire facility.

Areas at special risk from other physical impacts from inside and outside. Physical impacts from inside and outside may impair the functional effectiveness of facilities or buildings and damage or destroy entire complexes. This can lead to breakdowns and failures in all areas. Physical impacts in the area of external networks can lead to internal supply shortages and production losses.

1.4.2 Areas especially endangered through terrorism and criminal acts

The graduated risk categories indicating conceivable threats initially apply to the entire company. However, individual complexes within the overall company are also comprised of units or plant components which differ in terms of risk potential, design, form of usage, technical configuration and, above all, vulnerability to interference and malfunctions. Points of special vulnerability generally also exist within plant components. Where appropriate, these are to be ascertained by means of a separate systematic examination. By way of analogy to the security report which is to be drawn up in accordance of the Ordinance on Major Incidents, both the actual risk potentials and the facilities operated to supply and control the facilities and the materials transport systems, etc. are also of importance with regard to installation protection.

Consequently, it is generally expedient to break down the operational area into a number of sub-areas of different types and risk categories. A complete analysis of all potential weak points combined with the diverse scope of conceivable forms of attack or impact would result in an unmanageable number of different variants. It would thus appear expedient to group together areas and parts of facilities in a more generalised manner. It may be useful, for example, to consider a continuous complex as a whole, without considering in greater detail which individual components and parts are vulnerable and what precise impact a potential attack on one or other of the facility's components might have. The complex concerned is then classified as security-critical and secured as a whole in such a manner as to cover all the individual components. Classification of security areas In the case of supply systems which are deployed throughout the operational area, sub-segments concerning threatened installations should ideally be established and the examination process should not be extended unnecessarily to include comprehensive complete networks. At the same time, a view extending beyond the company's perimeters remains important, with regard to both special risks in the area of the up- and down-stream value chain and geographic interactions with neighbouring hazardous area.

It may be expedient to group together hazardous areas as follows, for example:

- Production, extraction and processing plants;
- Control centres, IT systems;
- (Unmanned) external facilities;
- Service lines;
- All kinds of power supply systems;
- All kinds of emergency power units.

1.5 Generalising recommendations for baseline protection

The aim is to present baseline protection requirements for different hazards, which are to be regarded as representing the minimum level of protection required for stationary facilities in the area of critical infrastructures. A multi-stage process based on the approach described in section 1 is appropriate here, covering identification of the given risks and the development and implementation of various protection measures. Baseline protection defining minimum required level of proection

Firstly, the locations of the facilities are to be examined. This includes risk assessment with regard to natural events, events resulting from technical failure and human error, and terrorist attacks and criminal acts. Risk assessments regarding dangers from natural events can be carried out on the basis of plans (flooding plans, earthquake maps, regional development plans, risk maps) which can be Risk assessment obtained from the competent authorities. With regard to dangers relating to human error and technical failure, due compliance with relevant rules and technical regulations (e.g. fire protection, Ordinance on Hazardous Substances, occupational health and safety, training) is to be verified. Regarding terrorist threats, operators of critical infrastructures can:

- undertake systematic assessments of critical areas of the company and facilities in cooperation with the authorities which are responsible for internal security in order to establish whether they may constitute a key target in principle, in view of which the possibility of the impairment, interference with or destruction of the facility concerned exists (danger analysis);

- examine in cooperation with the authorities responsible for averting dangers outside of the company what concrete consequences are to be expected as a result of the possible impairment, interference with or destruction of the given facility, and whether these might lead to a serious danger (hazard analysis);

– assess contrasting and common requirements pertaining to protection from interference by unauthorised persons, from natural hazards and from human error and technical failure.

Danger analysis and hazard analysis are to be accorded equal priority in analysing protection requirements. It should be decided in each individual case which of these steps is to be undertaken first. For the purposes of this concept it is suggested to begin with a general danger analysis and then to determine the concrete consequences of these dangers for the company by means of a hazard analysis. The required level of protection can subsequently be discussed on the basis of this analysis process and duly defined.

The analysis and the resultant measures should be documented. This documentation is of a particularly confidential nature, however, and should only be accessible to a limited group of employees even within the company. Documents which are available to the personnel as a whole and to the public should, however, verify that the operator has undertaken the necessary measures to secure the relevant area of the company and the facilities. The analysis is furthermore to be repeated at regular intervals and/or integrated into the company's risk management process, in order to enable the identification of new dangers, to carry out any reassessment which may be necessary, to adapt the protection requirements accordingly and thus to ensure that the basic protection remains up to date.

1.5.1 Consideration of dependencies and interaction

In addition to direct dangers pertaining to natural events, human error and technical failure or terrorism and criminal acts, critical infrastructures are also exposed to indirect dangers. These require to be considered in carrying out a comprehensive analysis of protection requirements. Firstly, the so-called domino effects are to be identified. These occur when external events, e.g. in neighbouring

operational areas, in the surrounding area or in the traffic area, impact on the facility. By way of example, natural events occurring some distance away, such as floods, mass movements or earthquakes, can affect the functional effectiveness of the facility as a result of backwater or blocked access and delivery routes. Malfunctions in surrounding facilities, particularly such facilities as are subject to a special risk of danger, may damage the facility as a result of an encroaching fire or flying debris after an explosion. The failure of supply facilities such as energy and water supply systems or of services from suppliers is also possible as a result of catastrophic events outside of the facility.

Events occurring within a short time of each other, such as several incidents occurring around the same time at different locations or a second, delayed explosion may also entail an exponential effect by preventing rescue or restoration measures or causing resources to be concentrated in the wrong place, for example (diversionary measures). Beyond this, additional damage (secondary damage) may result from the impairment of critical infrastructures, such as supply bottlenecks and shortages linked to disruptions to the transport system following a power failure. Such secondary damage is also to be considered in analysing the protection requirements, in order to enable an adequate assessment of the effects of the complete or localised failure of critical infrastructures on areas both within and outside of the facility.

1.5.2 Special consideration of terrorism and criminal acts

Previously drawn up danger and hazard analyses and security concepts should be examined to ascertain whether they also accord due consideration to such dangers which, according to the danger analysis, may result from interference by unauthorised persons, even if these dangers have been largely ruled out in the form of malfunctions, natural risks or accidents. If the hazard analysis has established that a serious danger may exist for special objects of protection, it is to be examined to what

extent the facilities may appear particularly «attractive» for terrorist attacks or criminal acts. To this end, a systematic analysis is to be carried out, focusing in particular on the following aspects which have already been mentioned in section 1:

– general risk assessment;

– geographic location of the operational area and the facilities;

– importance of the facilities to up- and down-stream production processes and services;

– symbolic character of the enterprise and/or facilities;

– interdependencies, i.e. interaction with other infrastructures;

– type, typology and cooperative relationships of the risk management structures implemented by the operator;

– structural nature of the cooperation between public facilities and operators.

Operators will be required to obtain some of the information necessary for this purpose from the authorities responsible for internal security. The involvement of these authorities is generally recommendable at this stage. The general security situation describes dangers such as generally apply to operational areas, where appropriate with regional differences. An initial indicator of relevant criminality is provided by police crime statistics and publications by insurance agencies. The security situation with regard to politically motivated offences is defined by ongoing appraisals by the authorities on the basis of their operations relating to judicial police activities and the protection of the constitution. Regional aspects can also be allocated a stronger focus on the basis of this information.

The scope, severity and nature of previously recorded offences in an operational area can provide an indication of the level of danger. A period of around

five years can be reviewed for this purpose. The following information should be contained in such a review:

- general information on recorded minor offences, such as simple theft;
- number of previously committed break-ins or serious cases of theft;
- identification of organised criminality in the operational area;
- number of previously perpetrated acts of sabotage, including unresolved cases involving a substantial suspicion of sabotage;
- number of previous bomb threats or other threatening acts.
- number of previous arson attacks or attacks with explosives, including suspected cases.

1.5.3 Definition of protection aim

To enable the stipulation and operationalisation of protection objectives and to establish such objectives as an inherent part of corporate policy, it is recommendable to define them as part of a security management system. In the past, management systems have proven an effective instrument for the systematic handling and examination of corporate processes and procedures, as long as they were able to ensure a successful synthesis of top-down approaches (hierarchic, centralised), bottom-up approaches (discursive, decentralised) and an open-minded approach (innovative, networked). The systematic integration of various security-relevant processes, including both mutual integration and integration with value creation strategies, is particularly crucial in the context of corporate security. Many of these measures are already in use or can be introduced comparatively quickly. If they have not already done so, operators should appraise the effectiveness of existing measures and take any necessary action on the basis of their findings.

The quality and extent of personnel and technical resources for the company's internal and/or external security service (e.g. plant security) are of particular importance in this context, appurtenant requirements are defined. Particular emphasis is also to be attached to networking and harmonising elements of security management which are often largely autonomous, such as IT security, installation protection and personnel security. When the operational area under review belongs to a larger enterprise (corporate division, subsidiary, majority-owned company, etc.), the level of threat and danger facing the enterprise as a whole must additionally be considered. This applies above all with regard to politically motivated crimes. Past experience shows that this danger generally increases according to the size and (global) significance of the enterprise as a whole. In this connection it should also be established whether increased risks apply as a result of certain distribution links. This could be the case if business links exist with politically instable countries, for example. As export-oriented operational areas generally supply goods all over the world, an increased risk applies above all when particularly prominent links exist with such countries. Key protection objectives to secure facilities and installations which are assessed as being security-critical can be described as follows:

- the boundaries of operational areas are to be secured by technical and organisational measures such that unauthorised persons are unable to enter into these areas without the use of force or malicious deceit and such as to ensure that any forced entry will be detected within a reasonable time;

- jutsiders should be identifiable;

- the facilities themselves are to be secured such that no unauthorised interference can be carried out without internal knowledge and/or technical resources;

- financial resources should be deployed according to lists of priorities (integrated security management).

– industrial estates impose special requirements with regard to security measures on account of the large number of legally and organisationally independent operators alone. As a rule, the vulnerability of dangerous facilities can only be minimised through jointly defined protection objectives and measures. Suitable measures are most expediently selected by means of a systematic security analysis.

1.5.4 Measures to achieve the protection aims

Objectives should be defined for the protection of facilities and installations which are assessed as being securitycritical. In view of specific threat situations (terrorism), it is also necessary to hinder the entry of unauthorised persons into operational facilities of critical infrastructures which are not directly subject to the Ordinance on Major Incidents. Effective measures here include monitored fencing, the organisation of gate checks, patrols, video surveillance, etc. The risk of terrorist attacks on operational areas/facilities is to be considered with due regard to the probability of such attacks on the one hand and the potential consequences on the other. Security measures which have been commonly employed to date continue to offer substantial protection.

The measures to achieve the security objectives for the internal and external protection of facilities include the following, for example:

– particularly sensitive areas should not be built in regions which are subject to a risk of flooding and earthquakes. If they are already located in such regions, relocation to non-endangered regions should be considered; as a minimum precaution, special measures should be undertaken to afford protection from flooding and earthquakes (e.g. raising of IT facilities and power distribution installations, cushioning against vibration, diking);

– all facilities and particularly sensitive parts of facilities should be made more robust, in order to reduce or avoid consequences of storm tides, flash floods, earthquakes, of physical forces and of explosions. Adequate reserve resistance capacities are to be incorporated into the lower storeys (pressure compensation). Particularly sensitive areas should furthermore be located inside the facilities;

– locating facilities and installations requiring protection such that accessing them requires a certain distance to be covered and takes a certain time is a key aspect in preventing terrorist attacks and sabotage. Barriers and obstacles can hinder or prevent access to sensitive areas (access zones, access controls, plant security, gates, fencing, patrols, bollards, concrete elements, elevations);

– concealed areas can be monitored with electronic security systems (video surveillance, motion detectors, noise sensors, thermal imaging cameras, night vision devices);

– the importance of gates to security generally extends beyond controlling access. In this context, the question as to security for the gates themselves arises. If, for example, the main gate is the sole point for receiving alarm and fault messages (frequently after the normal service hours of the operating area concerned), it must not be possible to prevent the relay of these messages to support centres by interfering with the communication facilities or threatening the security staff at the gate. This is to be ensured via appropriate protection measures. It is also of central importance that the gate / security centre be continuously manned;

– an understanding of security considerations for the operating area is to be instilled in the personnel, who are also to be involved in security processes through team training, seminars, etc.

In most cases, the measures to secure the site as a whole serve to provide basic protection; they provide an initial barrier to ward off unauthorised persons. Special individual protection is additionally required for all points of danger.

«Classical» measures to secure facilities and installations play a major role here. Securing individual danger areas usually represents the most important preventive measure, as the ìexternalî measures which apply to the entire operational area rarely afford complete and adequate protection.

External protection measures will not affect any risk of wilful action on the part of employees, for example. Similarly, 100 per cent control of access to the operational area or installations is practically impossible. On the other hand, there is scope for substantially more effective controls at individual points of the operational area.

2 Методы проведения оценки эффективности системы безопасности территориально – распределенного объекта

2.1 Принципы организации и функционирования системы безопасности

Организация и функционирование системы безопасности предприятия должны строиться на основе таких принципов, как:

- комплексность – руководство объекта должно оценивать все возможные угрозы;
- своевременность – все, что делается для обеспечения безопасности, должно быть направлено в первую очередь на предупреждение возможных угроз, а также на разработку эффективных мер предупреждения посягательств на интересы компании;
- непрерывность – защитные меры должны применяться постоянно;
- законность – система безопасности должна строиться на основе действующего законодательства с использованием всех дозволенных методов обнаружения и пресечения правонарушений;
- плановость – деятельность по осуществлению безопасности должна строиться на основе специально разработанных планов работы всех подразделений предприятия и его отдельных сотрудников;
- целесообразность – необходимо сопоставлять размер возможного ущерба и затраты на обеспечение безопасности (критерий «эффективность – затраты»);
- совершенствование – меры и средства защиты необходимо изменять и дополнять, отслеживать появление новых технических средств и нормативно-технических требований;
- единство и централизация управления – система безопасности должна работать самостоятельно по единым, утвержденным в организации

принципам, а руководитель компании должен владеть ситуацией и принимать решения.

К защищаемым объектам предприятия относятся:

– финансовые средства, материальные ценности (здания, сооружения, хранилища, техническое оборудование, транспорт и иные средства);

– информационные ресурсы (информация с ограниченным доступом, составляющая коммерческую тайну, иная конфиденциальная информация, предоставленная в виде документов и массивов независимо от формы и вида их представления).

Каждому объекту защиты соответствует некоторые виды угроз безопасности. Целью угроз является нанесение серьезного материального ущерба и срыв на длительное время нормального функционирования. Основная угроза материальным ценностям - хищение, повреждение, уничтожение. В отношении зданий и помещений угрозы проявляются в виде:

– пожаров, поджогов, затоплений;

– технологических аварий и повреждений;

– повреждения входных дверей, решеток, ограждений, личных и служебных транспортных средств.

2.2 Оценка эффективности системы безопасности

Для оценки эффективности интегрированной системы безопасности (ИСБ) существуют методы, на основе которых можно сравнивать конкурирующие варианты ИСБ. Эффективность системы безопасности характеризует вероятность выполнения системой своей основной целевой функции по обеспечению защиты объекта от угроз, источниками которых являются умышленные противоправные (несанкционированные) действия физических лиц (нарушителей).

Для решения подобных задач необходимо учитывать принципы грамотного и эффективного использования денежных средств. Для разработки системы безопасности выбранного объекта необходимо основополагаться на следующих принципах:

– необходимости применяемых мер;

– правовой основе;

– организованной службе охраны;

– оптимальном количестве применяемых технических средств защиты.

Существующие модели возможно классифицировать не только по уровню сложности их построения, но и к функциональным, структурным составляющим. Далее приведены основные составляющие показатели свойств систем:

– общесистемные свойства (управляемость, динамичность, наблюдаемость, целостность, устойчивость, и т.д.);

– структурный состав системы (сложность, организация, связность, масштабность, пространственное распределение, централизованность и т.д);

– функциональные свойства системы (мобильность, ресурсоемкость, производительность, активность, результативность, оперативность, быстродействие, работоспособность, экономичность и т.д.).

При данном анализе показатели качества можно отнести к области обще структурных свойств систем. Свойства же, которые характеризуют процесс функционирования системы, можно назвать операционными свойствами, так как искусственно созданные системы применяются для исполнения конкретных операций. В общем случае оценка операционных свойств проводится как оценка двух аспектов:

– результата операций;

– обеспечение полученных результатов (алгоритмов).

Качественная характеристика результата операции и алгоритм, обеспечения полученных результатов, рассчитываются по показателям качества операции, к которым относят ресурсоемкость, оперативность и результативность. Результативность методики проведения операции характеризуются полученным эффектом, ради которого функционирует система. Ресурсоемкость оценивается ресурсами всех типов (человеческими, материально-техническими, финансовыми, информационными и т.д.), применяемыми для обеспечения целевого эффекта. Оперативность определяется расчетом затраченного времени, необходимого для достижения поставленной цели.

Оценка выполнения операции учитывает, что операция проводится для достижения поставленной цели – исхода операции. Под исходом операции понимается состояние системы и внешней среды, образующаяся на период ее завершения. Для качественной и количественной оценки выполнения операции вводится понятие показателя исхода операции (ПИО), составляющие части которого образуют показатели его отдельных свойств, отражающие Оперативность, ресурсоемкость и результативность операции.

Метод оценки выполнения алгоритма функционирования системы по своей сути является одной из ведущих методов при оценке эффективности. Основой такого утверждения является теоретический постулат, подтвержденный на практике: существование правильного «алгоритма» эксплуатации системы безопасности увеличивает уверенность в получении необходимых результатов. Данный метод оценки особенно важен для организационно-технических систем, а также систем, в которых результаты операции обозначаются в режиме реального времени.

В общем результате оперативность, ресурсоемкость и результативность порождают свойство – эффективность процесса. Данное свойство проявляется при функционировании системы безопасности и зависит как от свойств самой

системы и от свойств внешней среды. Для большинства операций процедура оценки эффективности решений носит характер прогнозирования.

Выбор критерия эффективности – центральный, самый ответственный момент исследования системы. Считается, что гораздо лучше найти неоптимальное решение выбранному критерию, чем наоборот – оптимальное решение при неправильно выбранном критерии. Процесс выбора критерия эффективности, как и процесс определения цели, является в значительной мере субъективным, творческим, требующим в каждом отдельном случае индивидуального подхода. Наибольшей сложностью отличается выбор критерия эффективности решений в операциях, реализуемых иерархическими системами.

В зависимости от типа систем и внешних воздействий операции могут быть детерминированными, вероятностными или неопределенными. В соответствии с этим выделяют три группы показателей и критериев эффективности функционирования систем:

– в условиях определенности, если ПИО отражают один строго определенный исход детерминированной операции;

– в условиях риска, если ПИО являются дискретными или непрерывными случайными величинами с известными законами распределения в вероятностной операции;

– в условиях неопределенности, если ПИО являются случайными величинами, законы распределения которых неизвестны.

Основной проблемой оценки эффективности вероятностных операций является неясность способа определения требуемых вероятностей. Это связано с отсутствием достаточной статистики. Известно что применение методов классической теории вероятностей допустимо при повторяемости опытов и одинаковости условий. Эти требования в сложных системах выполняются не всегда. Наибольшие трудности возникают при оценке эффективности систем в условиях неопределенности. Для решения этой задачи разработано несколько

подходов. Порядок оценки эффективности систем в неопределенных операциях составляет один из разделов теории принятия решений. Выбор показателей для конкретной системы связан с анализом большого объема плохо структурированной информации, и поэтому в системном анализе сформулированы требования, следование которым позволяет обосновать применимость показателей в данной задаче оценки. Общими требованиями к показателям исхода операции являются:

- соответствие ПИО цели операции;
- полнота;
- измеримость;
- ясность физического смысла;
- неизбыточность;
- чувствительность.

Система считается эффективной, если выполняются следующие требования:

- в заданных условиях эксплуатации полностью и в установленные сроки выполняет стоящие перед ней задачи (техническая эффективность);
- затраты на создание и эксплуатацию системы не превышают положительного эффекта от ее использования (экономическая эффективность).

Вероятностные методы включают такие параметры как вероятности реализации угроз; обнаружения угроз; ложных тревог; пресечения несанкционированных действий и др. Указанные параметры могут быть получены на основе статистических данных и экспертных оценок.

Дополнительную сложность указанных методов создает то, что практически отсутствует статистический материал по вероятностям реализации угроз, вероятностным характеристикам оборудования обеспечения безопасности, а экспертные оценки представляются достаточно субъективными. Комбинированные методы, учитывающие как экономические, так и вероятностные характеристики, позволяют определить максимальный

относительный предотвращенный ущерб от реализации всех угроз с учетом случайного характера их появления. Надежность системы можно рассчитать по формулам, которые позволяют определить эффективность тех или иных методов задержки нарушителя. Указанные критерии могут быть применены как к системе безопасности в целом, так и к отдельным подсистемам, поскольку систему безопасности, как сложную иерархическую систему, можно декомпозировать. Однако, естественно, окончательный и более полный вывод можно сделать только на основе анализа эффективности функционирования всех подсистем не по отдельности, а во взаимодействии.

Комплексный подход к разработке системы безопасности подразумевает также и комплексный подход к оценке на создание и эксплуатации системы (анализ объекта, проектирование, поставка оборудования, монтаж, пуско-наладка, обучение персонала, обслуживание, расширение, модернизация). Очевидно, что в общем случае должны учитываться различные стороны эффективности. Все мероприятия по обеспечению безопасности можно разделить на 5 категорий:

– прогнозирование возможных угроз;

– организация деятельности по предупреждению возможных угроз (превентивные меры);

– выявление, анализ и оценка возникших реальных угроз безопасности;

– принятие решений и организация деятельности по реагированию на возникшие угрозы и их ликвидация;

– постоянное совершенствование системы обеспечения безопасности предприятия.

По всем выявленным угрозам следует оценить возможные потери от реализации каждой угрозы. Для построения системы безопасности на предприятии необходимо для начала определить, какие функции будут на нее возложены, что будет являться потенциально опасным объектом, и провести

анализ степени их защищенности. Затем следует рассчитать силы и средства, которые необходимы для обеспечения безопасности: количество людских, материально-технических ресурсов и оптимальные затраты на их содержание.

2.3 Методы оценки рисков

Существуют множество методов оценки возможных рисков в отношении объекта безопасности. Методики, используемые в данном случае, могут быть смешанными, качественными, количественными. Степень изучения и характеристика анализа зависит от доступности проверенных данных и необходимости принятие решений организацией. Некоторые методы и степень глубины анализа могут быть установлены в соответствии с обязательными правилами. При качественной оценке определяются последствия, вероятность и уровень риска по шкале «низкий», «средний» и «высокий». Оценка вероятности последствий может быть объединена в сравнительную характеристику уровня риска, в данном случае проводится оценка в сравнении с качественными критериями. В смешанных методах используют числовую шкалу оценки последствий, вероятности и их сочетания для определения уровня риска по соответствующей формуле. Шкалы могут быть линейными, логарифмическими или могут быть построены по другим принципам. Используемые формулы соответственно могут быть различными. При количественном анализе оценивают практическую значимость и стоимость последствий, их вероятности и получают значение уровня риска в определенных единицах, установленных при разработке области применения менеджмента риска. Полный количественный анализ не всегда может быть возможен или желателен из-за недостаточной информации об анализируемой системе, видах деятельности организации, недостатка данных, влияния человеческого фактора и т. п. или потому, что такой анализ не требуется, или трудозатраты на количественный анализ слишком велики[11]. В данной главе

были отобраны наиболее эффективные и простые в методах анализа, методики оценки риска.

Анализ дерева событий. Анализ дерева событий является графическим методом представления взаимоисключающих последовательностей событий, следующих за появлением исходного события, в соответствии с функционированием и не функционированием систем, разработанных для смягчения последствий опасного события. Метод анализа дерева событий может быть применен для качественной и/или количественной оценки. Последовательность событий легко представить в виде дерева событий и поэтому с помощью данного метода легко установить ухудшающие или смягчающие последствия события, принимая во внимание дополнительные системы, функции или барьеры.

Метод анализа дерева событий может быть использован для моделирования, вычисления и ранжирования (с точки зрения риска) различных сценариев инцидента после возникновения начального события. Метод анализа дерева событий может быть применен на всех стадиях жизненного цикла продукции или процесса. Данный метод может быть использован на качественном уровне при мозговом штурме, определении сценариев и последовательностей событий, которые могут возникнуть после начального события, и при определении воздействия на результат различных видов обработки риска, барьеров или средств управления, предназначенных для снижения нежелательных последствий.

Предварительный анализ опасностей. Предварительный анализ опасностей (ПАО) является простым индуктивным методом анализа, цель которого состоит в идентификации опасностей, опасных ситуаций и событий, которые могут нарушить работу или нанести вред данному виду деятельности, оборудованию или системе. ПАО обычно выполняют на ранних стадиях разработки проекта в условиях недостатка информации о деталях проекта или рабочих процессов. ПАО часто предшествует дальнейшим исследованиям или

направлен на получение информации для разработки требований к проектируемой системе. Предварительный анализ опасностей также может быть полезен при анализе существующих систем, направленном на ранжирование опасностей и риска для последующего анализа риска. Входные данные включают в себя:

– информацию об оцениваемой системе;

– доступные и относящиеся к делу детали проекта системы.

Процесс выполнения метода заключается в построении переченя опасностей, общих опасных ситуаций и риска формируют на основе следующей информации:

– данные об используемых и изготавливаемых материалах, их химической или иной активности;

– перечень используемого оборудования;

– сведения о рабочей среде;

– схема расположения оборудования;

– сведения о взаимодействии компонентов системы и т. д.

2.4 Методика описания ТРО и анализ необходимости в защите объекта

Вначале необходимо проанализировать местонахождение объекта критической инфраструктуры. При проведении описания (категорирования) объекта необходимо рассмотреть следующие исходные данные:

– сведения о размещении объекта, рельефе окружающей местности, природно-климатических условиях, удаленности объекта от других потенциально опасных объектов, населенных пунктов, густонаселенных районов местности, жилых и административных зданий, мест массового скопления людей, автомобильных магистралей, железнодорожных путей или станций, аэродромов и аэропортов, морских или речных портов и т.д.;

– сведения о размещении и специфике потенциально опасных производств объекта, местах использования и хранения опасных веществ и материалов (ОВМ), объемах их запасов;

– возможные условия возникновения и развития чрезвычайных ситуаций, в том числе выбросов в окружающую среду вредных веществ;

– категории, присвоенные объекту по гражданской обороне, химической опасности, режиму секретности;

– категории, присвоенные зданиям и сооружениям объекта по взрывопожароопасности;

– характеристики систем контроля безопасности промышленного производства, сведения об объемах и содержании организационных, технических и иных мероприятий по предупреждению чрезвычайных ситуаций;

– сведения о состоянии системы физической защиты и охраны объекта, имевших места случаях ее нарушения, попытках проникновения на объект посторонних лиц, несанкционированных действиях, направленных на повреждение или разрушение элементов производственно-технологического процесса.

Также необходимо прогнозирование рисков, исходящих от стихийных явлений, человеческих просчетов или технических сбоев, а также от терроризма или преступных деяний. Для прогнозирования рисков, исходящих от стихийных явлений, можно истребовать имеющиеся у соответствующих органов планы (карты зон затоплений, карты сейсмического районирования, схемы территориального планирования, карты вероятных зон риска). В целях определения угроз, исходящих от человеческих просчетов или технических сбоев необходимо проверить соблюдение соответствующих предписаний и технических правил (например, по противопожарной защите, Постановление о порядке обращения с опасными веществами, по охране труда, проведение обучения безопасным методам и приемам работы).

С учетом угроз, прогнозирование рисков исходящих от терроризма, инфраструктурные организации могут при сотрудничестве с органами, курирующими вопросы внутренней безопасности, систематически контролировать критические зоны предприятия и установки с целью выяснения, могут ли они в принципе представлять собой приоритетную цель, и существует ли в результате возможность сбоев в эксплуатации сооружения либо его полного или частичного разрушения (анализ уязвимости) при сотрудничестве с органами, курирующими вопросы предотвращения опасности за пределами предприятия, выяснить, какие конкретные последствия надо ожидать в результате сбоев в эксплуатации сооружения либо его полного или частичного разрушения, и могут ли эти последствия привести к серьезной опасности (анализ опасности) определить расхождения и совпадения, существующие между соответствующими требованиями по защите от несанкционированных действий со стороны посторонних лиц, по защите от стихийных явлений, а также по защите от человеческих просчетов или технических сбоев.

Анализ уязвимости и анализ опасности являются равнозначными элементами анализа потребности в защите. Последовательность осуществления

этих шагов следует определять для каждого отдельного случая. В рамках настоящей Концепции предлагается сначала провести общий анализ уязвимости, а потом путем проведения анализа опасности выявить конкретные последствия для предприятия, вытекающие из существующих угроз, чтобы на этой основе согласовать и определить необходимый уровень защиты.

Факт проведения анализа и следующие из него меры должны получать документальное подтверждение. Но эта документация особенно нуждается в конфиденциальности, и поэтому она должна быть доступной ограниченному кругу лиц из числа сотрудников предприятия. Однако из документов, доступных всему персоналу и общественности, должно логично следовать, что инфраструктурная организация приняла необходимые меры для обеспечения безопасности соответствующего участка предприятия и соответствующих установок. В целях выявления возникших новых уязвимых мест или в случае необходимости – в целях требующейся переоценки ситуации, адаптации потребности в защите и тем самым актуализации основных мер защиты предприятия, кроме того, необходимо регулярно повторять этот анализ или же интегрировать его в процесс риск-менеджмента предприятия.

4 Финансовый менеджмент, ресурсоэффективность и ресурсосбережение

Целью данного раздела является проектирование и создание конкурентоспособных разработок и технологий, отвечающих предъявляемым требованиям в области ресурсоэффективности и ресурсосбережения.

Достижение цели обеспечивается решением следующих задач:

– разработка общей экономической идеи проекта, формирование концепции проекта;

– организация работ по научно-исследовательскому проекту;

– определение возможных альтернатив проведения научных исследований;

– планирование научно-исследовательских работ;

– оценки коммерческого потенциала и перспективности проведения научных исследований с позиции ресурсоэффективности и ресурсосбережения;

– определение ресурсной (ресурсосберегающей), финансовой, бюджетной, социальной и экономической эффективности исследования.

В данной диссертационной работе проведена разработка методики оценки эффективности системы безопасности территориально – распределенного объекта. Проведено изучение основных типов систем безопасности, принципов организации, функционирования и их структурных компонентов. Сформирован перечень угроз в отношении ТРО.

4.1 Потенциальные потребители результатов исследования

Результатом исследования является создание методики оценки эффективности системы безопасности территориально – распределенного объекта.

Целевым рынком данного исследования будут являться объекты относящиеся к категории территориально – распределенных, государственные корпорации по атомной энергетике, атомная и смежные отрасли научной промышленности.

Сегментировать рынок услуг по разработке методики оценки эффективности системы безопасности территориально – распределенного объекта можно по степени потребности её использования. Результаты сегментирования представлены в рисунке 2.1.

		Методика оценки		
		Атомная промышленность	Научная отрасль	Объекты относящиеся к категории ТРО
Потребность	Сильная			
	Слабая			

Рисунок 2 – Карта сегментирования рынка услуг по использованию оптимальной методики измерения

4.1.1 Анализ конкурентных технических решений

Детальный анализ конкурирующих разработок, существующих на рынке, необходимо проводить систематически, поскольку рынки пребывают в постоянном движении. Такой анализ помогает вносить коррективы в научное исследование, чтобы успешнее противостоять своим соперникам. Важно реалистично оценить сильные и слабые стороны разработок конкурентов.

С этой целью может быть использована вся имеющаяся информация о конкурентных разработках: технические характеристики разработки, конкурентоспособность разработки, уровень завершенности научного исследования (наличие макета, прототипа и т.п.), бюджет разработки, уровень проникновения на рынок, финансовое положение конкурентов, тенденции его изменения и т.д.

Анализ конкурентных технических решений с позиции ресурсоэффективности и ресурсосбережения позволяет провести оценку сравнительной эффективности научной разработки и определить направления для ее будущего повышения.

Позиция разработки и конкурентов оценивается по каждому показателю экспертным путем по пятибалльной шкале, где 1 – наиболее слабая позиция, а 5 – наиболее сильная. Веса показателей, определяемые экспертным путем, в сумме должны составлять 1.

Анализ конкурентных технических решений определяется по формуле:

$$К = \sum B_i \cdot Б_i \,, \qquad (1)$$

где $К$ – конкурентоспособность научной разработки или конкурента;

B_i – вес показателя (в долях единицы);

$Б_i$ – балл i-го показателя.

Таблица 2 – Оценочная карта для сравнения конкурентных технических решений (разработок)

Критерии оценки	Вес критерия	Баллы			Конкурентоспособность		
		$Б_ф$	$Б_{к1}$	$Б_{к2}$	$К_ф$	$К_{к1}$	$К_{к2}$
1	2	3	4	5	6	7	8
Технические критерии оценки ресурсоэффективности							
1. Повышение производительности труда пользователя	0,1	5	4	4	0,5	0,4	0,4
2. Удобство в эксплуатации	0,1	5	4	3	0,5	0,4	0,3
3. Энергоэкономичность	0,04	5	3	3	0,2	0,12	0,12
4. Надежность	0,05	5	4	4	0,25	0,2	0,2
5. Уровень шума	0,01	5	5	5	0,05	0,05	0,05
6. Безопасность	0,06	5	5	5	0,3	0,3	0,3
7. Потребность в материальных ресурсах	0,04	4	4	4	0,16	0,16	0,16
8. Функциональная мощность	0,05	5	4	3	0,25	0,2	0,15
9. Помехоустойчивость	0,07	5	3	3	0,35	0,21	0,21
10. Простота эксплуатации	0,1	5	4	4	0,5	0,4	0,4
Экономические критерии оценки эффективности							
1. Конкурентоспособность метода	0,03	5	4	4	0,15	0,12	0,12
2. Уровень проникновения на рынок	0,05	5	4	3	0,25	0,2	0,15
3. Предполагаемый срок эксплуатации	0,2	5	4	4	1	0,8	0,8
4. Послепродажное обслуживание	0,1	5	3	3	0,5	0,3	0,3
Итого	1				4,96	3,86	3,66

На основании представленного выше анализа можно сделать вывод, что разработанная в данной диссертационной работе методика является оптимальной для использования в практических целях. По результатам проведенного анализа можно сделать вывод, что предлагаемый аналитический комплекс является наиболее оптимальным техническим решением поставленной задачи – оценка эффективности системы безопасности

территориально – распределенного объекта. Самый широкий набор функциональных возможностей в совокупности с минимальными энергозатратами и простотой эксплуатации делает предлагаемы продукт безусловным лидером среди конкурентных решений. Ценовая политика и отсутствие необходимости в специализированном оборудовании делает комплекс доступным для широкого использования.

4.1.2 SWOT-анализ

SWOT – Strengths (сильные стороны), Weaknesses (слабые стороны), Opportunities (возможности) и Threats (угрозы) – представляет собой комплексный анализ научно-исследовательского проекта. SWOT-анализ применяют для исследования внешней и внутренней среды проекта.

Сильные стороны – это факторы, характеризующие конкурентоспособную сторону научно-исследовательского проекта. Сильные стороны свидетельствуют о том, что у проекта есть отличительное преимущество или особые ресурсы, являющиеся особенными с точки зрения конкуренции.

Слабые стороны – это недостаток, упущение или ограниченность научно-исследовательского проекта, которые препятствуют достижению его целей. Это то, что плохо получается в рамках проекта или где он располагает недостаточными возможностями или ресурсами по сравнению с конкурентами.

Возможности включают в себя любую предпочтительную ситуацию в настоящем или будущем, возникающую в условиях окружающей среды проекта, например, тенденцию, изменение или предполагаемую потребность, которая поддерживает спрос на результаты проекта и позволяет руководству проекта улучшить свою конкурентную позицию.

Угроза представляет собой любую нежелательную ситуацию, тенденцию или изменение в условиях окружающей среды проекта, которые

имеют разрушительный или угрожающий характер для его конкурентоспособности в настоящем или будущем.

В таблице 3 представлена интерактивная матрица проекта, в которой показано соотношение сильных сторон с возможностями, что позволяет более подробно рассмотреть перспективы разработки.

Таблица 3 – Интерактивная матрица проекта

Возможности проекта	Сильные стороны проекта				
	С1	С2	С3	С4	С5
В1	+	+	+	+	+
В2	+	+	+	+	+
В3	+	+	–	+	+
В4	+	+	+	+	+
В5	+	+	+	+	+

В матрице пересечения сильных сторон и возможностей имеется определенный результат: «плюс» – сильное соответствие сильной стороны и возможности, «минус» – слабое соотношение.

В результате была составлена итоговая матрица SWOT-анализа, представленная в таблице 4.

Таблица 4 – SWOT-анализ

	Сильные стороны проекта: С1. Актуальность выбранной темы. С2. Применение современного оборудования. С3. Бюджетное финансирование С4. Наличие достоверных результатов. С5. Возможность применения полученной методики.	Слабые стороны проекта: Сл1. Узкое сфера внедрения методики. Сл2. Сложность в проведении анализа. Сл3.Недостаток квалифицированных кадров для обучения. Сл4. Необходимость финансирования. Сл5.Высокая стоимость оборудования.

Продолжение таблицы 4 – SWOT-анализ

Возможности: В1. Использование для исследований инфраструктуры НИ ТПУ. В2. Разработка метода оценки рисков. В3. Возможность создания алгоритма оценки территориально-распределенного объекта. В4. Поддержка развития систем безопасности стороны государства. В5. Дополнительный спрос на результаты исследования.	Результаты анализа интерактивной матрицы проекта полей «Сильные стороны и возможности»: 1. Полное обеспечение условий проведения анализа. 2. Появление дополнительного спроса и финансирования, обеспеченных актуальностью тематики.	Результаты анализа интерактивной матрицы проекта полей «Слабые стороны и возможности»: 1. Привлечение профильных специалистов для оценки эффективности территориально – распределенного объекта. 2. Крупные затраты на оборудование и функционирование.
Угрозы: У1 Недостаток квалифицированных кадров для реализации проекта. У2 Недостаток квалифицированных кадров на базе университета. У3 Неустойчивая экономическая ситуация в стране. У4 Недостаток аудиторного фонда на базе университета. У5 Изменение потребностей атомной отрасли в специалистах.	Результаты анализа интерактивной матрицы проекта полей «Сильные стороны и угрозы»: 1. Актуальность темы и широта распространения исследований на данную тематику.	Результаты анализа интерактивной матрицы проекта полей «Слабые стороны и угрозы»: 1. Невозможность быстрого реагирование на изменение рынка потребностей в методике оценки. 2. Недостаток финансирования со стороны государства для проведения оценки эффективности.

Таким образом, выполнив SWOT-анализ можно сделать вывод, что на данный момент преимущества разработанной методики измерений значительно преобладают над её недостатками. Все имеющиеся несовершенства можно легко устранить, воспользовавшись перечисленными выше возможностями.

4.2 Планирование управления научно-техническим проектом

4.2.1 Иерархическая структура работ проекта

Иерархическая структура работ (ИСР) – детализация укрупненной структуры работ. В процессе создания ИСР структурируется и определяется содержание всего проекта.

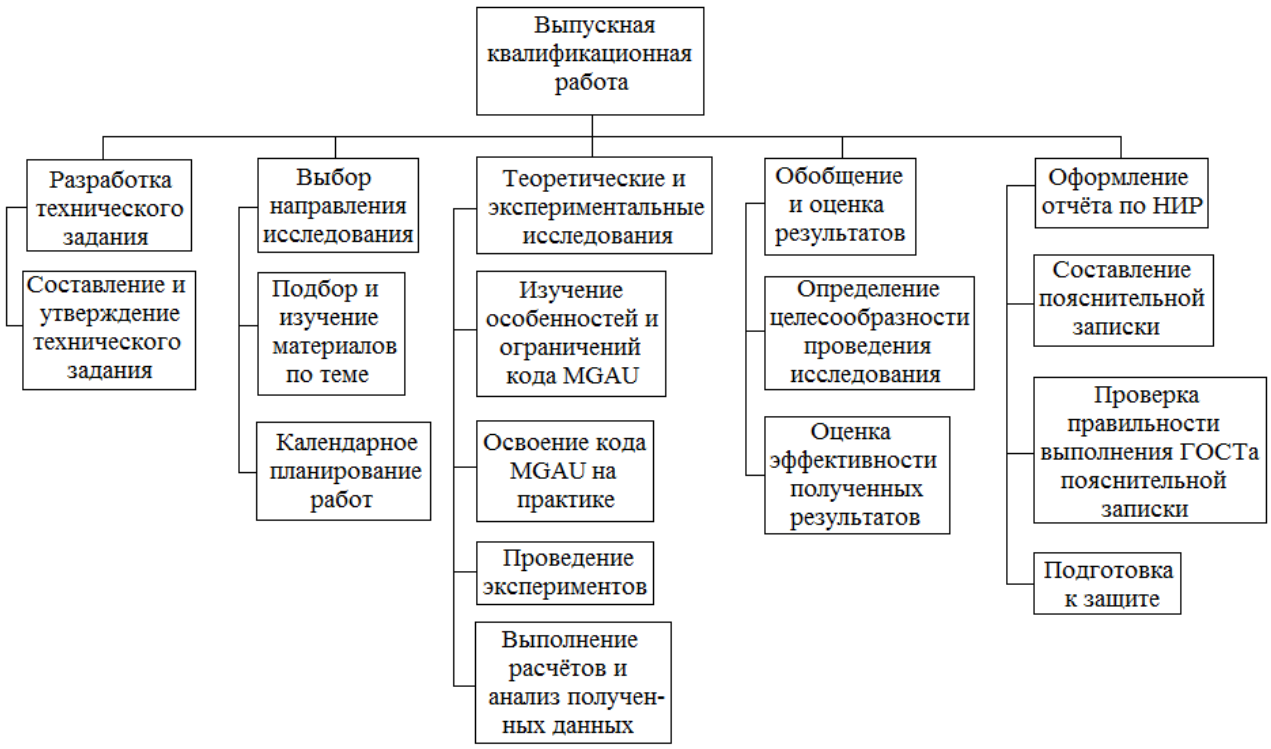

Рисунок 3 – Иерархическая структура работ

4.2.2 Контрольные события проекта

Ключевые события исследовательского проекта, их даты и результаты приведены в таблице 5.

Таблица 5 – Контрольные события проекта

№	Контрольное событие	Дата	Результат (подтверждающий документ)
1	Разработка технического задания на НИР	1.02.2016	Приказ по ФТИ
2	Составление и утверждение технического задания	3.02.2016	Задание на выполнение исследования
3	Выбор направления исследований	5.02.2016	
4	Подбор и изучение материалов по теме	10.02.2016	Отчёт
5	Календарное планирование работ	12.02.2016	План работ
6	Изучение особенностей построения систем безопасности	13.02.2016	Отчёт
7	Освоение методики построения алгоритмов оценки систем безопасности	14.02.2016	Отчёт
8	Проведение экспериментов	15.02.2016-30.03.2016	Отчёт
9	Выполнение расчётов и анализ полученных данных	28.03.2016	Отчёт
10	Обобщение и оценка результатов	30.03.2016	Отчёт
11	Составление пояснительной записки	14.02.2016-25.04.2016	Пояснительная записка
12	Проверка правильности выполнения ГОСТа пояснительной записки	26.04.2016	
13	Подготовка к защите	27.04.2016-25.05.2016	

4.2.3 План проекта

В рамках планирования исследовательского проекта построен календарный план-график с помощью диаграммы Ганта. Линейный график представлен в таблице 6.

Таблица 6 – Календарный план проекта

Код работы	Название	Длительность, дни	Дата начала работ	Дата окончания работ	Состав участников
1	Разработка технического задания	2	1.02.2016	3.02.2016	Руководитель
2	Составление и утверждение технического задания	2	3.02.2016	5.02.2016	Руководитель
3	Выбор направления исследований	5	5.02.2016	10.02.2016	Руководитель, студент
4	Подбор и изучение материалов по теме	2	10.02.2016	12.02.2016	Студент
5	Календарное планирование работ	1	12.02.2016	13.02.2016	Руководитель, студент
6	Изучение особенностей построения систем безопасности	1	13.02.2016	14.02.2016	Студент
7	Освоение методики построения алгоритмов оценки систем безопасности	1	14.02.2016	14.02.2016	Студент
8	Проведение анализа уязвимости в отношении ТРО	45	15.02.2016	30.03.2016	Студент
9	Анализ полученных данных	2	28.03.2016	30.03.2016	Студент
10	Обобщение и оценка результатов	1	30.03.2016	30.03.2016	Руководитель, студент

Продолжение таблицы 6 – Календарный план проекта

Код работы	Название	Длительность, дни	Дата начала работ	Дата окончания работ	Состав участников
11	Составление пояснительной записки	72	14.02.2016	25.04.2016	Студент
12	Проверка правильности выполнения ГОСТа пояснительной записки	1	26.04.2016	27.04.2016	Руководитель, студент
13	Подготовка к защите	29	27.04.2016	25.05.2016	Студент

Таблица 7 – Календарный план-график проведения научного исследования.

№ работ	Вид работ	Исполнители	$T_к$, кал.дн.	Продолжительность выполнения работ													
				Февраль			Март			Апрель			Май			Июнь	
				1	2	3	1	2	3	1	2	3	1	2	3	1	2
1	Разработка технического задания	Руководитель	2														
2	Составление и утверждение технического задания	Руководитель	2														
3	Выбор направления исследований	Руководитель, студент	5														
4	Подбор и изучение материалов по теме	Студент	2														
5	Календарное планирование работ	Руководитель, студент	1														
6	Изучение особенностей построения систем безопасности	Студент	1														
7	Освоение методики построения алгоритмов оценки систем безопасности	Студент	1														

Продолжение таблицы 7 – Календарный план-график проведения научного исследования.

8	Проведение анализа уязвимости в отношении ТРО	Студент	45	
9	Анализ полученных данных	Студент	2	
10	Обобщение и оценка результатов	Руководитель, студент	1	
11	Составление пояснительной записки	Студент	72	
12	Проверка правильности выполнения ГОСТа пояснительной записки	Руководитель, студент	1	
13	Подготовка к защите	Студент	29	

4.3 Бюджет научного исследования

При планировании бюджета исследования должно быть обеспечено полное и достоверное отражение всех видов расходов, связанных с его выполнением. В процессе формирования бюджета используется следующая группировка затрат по статьям:

- материальные затраты;
- затраты на специальное оборудование для научных (экспериментальных) работ;
- основная заработная плата исполнителей темы;
- дополнительная заработная плата исполнителей темы;
- отчисления во внебюджетные фонды (страховые отчисления).

4.3.1 Расчёт материальных затрат

Расчет материальных затрат осуществляется по следующей формуле:

$$З_{\text{м}} = (1 + k_{\text{Т}}) \cdot \sum_{i=1}^{m} Ц_i \cdot N_{\text{расх}i}, \quad (2)$$

где m – количество видов материальных ресурсов, потребляемых при выполнении научного исследования;

$N_{\text{расх}i}$ – количество материальных ресурсов i-го вида, планируемых к использованию при выполнении научного исследования (шт., кг, м, м^2 и т.д.);

$Ц_i$ – цена приобретения единицы i-го вида потребляемых материальных ресурсов (руб./шт., руб./кг, руб./м, руб./м^2 и т.д.);

Основными затратами в данной диссертационной работе являются затраты на электроэнергию и приобретение канцелярских товаров. Результаты расчётов по затратам на материалы приведены в таблице 8.

Затраты на электроэнергию рассчитываются по формуле:

$C = Ц_{\text{эл}} \cdot P \cdot F_{\text{об}} = 2{,}05 \cdot 3{,}6 \cdot 26 + 2{,}05 \cdot 0{,}5 \cdot 400 = 601,$

где $Ц_{\text{эл}}$ – тариф на промышленную электроэнергию (2,05 руб. за 1 кВт·ч);

P – мощность оборудования, кВт;

$F_{\text{об}}$ – время использования оборудования, ч.

В итоге затраты на электроэнергию составили 601, рубль.

Таблица 8 – Материальные затраты

Наименование	Марка, размер	Количество	Цена за единицу, руб.	Сумма, руб.
Электроэнергия	–	293,6 кВт·ч	2,05	601
Бумага	SvetoCopy	200	0,38	76
Печать на листе А4	–	200	1,5	300
Ручка	Pilot fine 0.7 мм	1	111	111
Доступ в интернет	–	4 месяца	350	1400
Всего за материалы				2488
Транспортно-заготовительные расходы				0
Итого по статье $С_{\text{м}}$				2488

4.3.2 Основная заработная плата исполнителей темы

Статья включает основную заработную плату работников, непосредственно занятых выполнением проекта, (включая премии, доплаты) и дополнительную заработную плату.

$$З_{зп} = З_{осн} + З_{доп}, \quad (3)$$

где $З_{осн}$ – основная заработная плата;

$З_{доп}$ – дополнительная заработная плата.

Основная заработная плата ($З_{осн}$) руководителя рассчитывается по следующей формуле:

$$З_{осн} = З_{дн} \cdot Т_{раб}, \quad (4)$$

где $З_{осн}$ – основная заработная плата одного работника;

$Т_{раб}$ – продолжительность работ, выполняемых научно-техническим работником, раб.дн.

$З_{дн}$ – среднедневная заработная плата работника, руб.

Среднедневная заработная плата рассчитывается по формуле

$$З_{дн} = (З_{м} \cdot М) / F_{д}, \quad (5)$$

где $З_{м}$ – месячный должностной оклад работника, руб.;

– при отпуске в 24 раб. дня М =11,2 месяца, 5-дневная неделя;

– при отпуске в 48 раб. дней М=10,4 месяца, 6-дневная неделя;

$F_{д}$ – действительный годовой фонд рабочего времени научно-технического персонала, раб. дн. (таблица 9).

Таблица 9 – Баланс рабочего времени

Показатели рабочего времени	Руководитель	Студент
Календарное число дней	365	365
Количество нерабочих дней: – выходные дни; – праздничные дни	 52 14	 104 14
Потери рабочего времени: – отпуск; – невыходы по болезни	 48 7	 24 –
Действительный годовой фонд рабочего времени	244	223

Студент во время прохождения преддипломной практики получает стипендию, равную 5670 руб/месяц. Среднедневная стипендия (оплата) составляет:

$$З_{дн} = (5670 \cdot 11{,}2) / 223 = 284{,}7 \text{ руб/день.}$$

Основной заработок студента за время преддипломной практики составляет:

$$З_{осн} = 284{,}7 \cdot 45 = 12811{,}5 \text{ руб.}$$

Основная заработная плата научного руководителя рассчитывается на основании отраслевой оплаты труда. Отраслевая система оплаты труда в ТПУ предполагает следующий состав заработной платы:

– оклад – определяется предприятием. В ТПУ оклады распределены в соответствии с занимаемыми должностями, например, ассистент, ст. преподаватель, доцент, профессор.

– стимулирующие выплаты – устанавливаются руководителем подразделений за эффективный труд, выполнение дополнительных обязанностей и т.д.

– иные выплаты: районный коэффициент.

Руководителем данной диссертационной работы является сотрудник с должностью доцента. Оклад доцента со степенью кандидата наук в НИ ТПУ составляет 23265 рублей.

Надбавки к заработной плате составляют 10000 рублей (надбавки учёного совета), также районный коэффициент по Томску равен 1,3.

Основная заработная плата научного руководителя:

$$З_{осн} = 23265 \cdot 1{,}3 + 10000 = 40244{,}5 \text{ руб / месяц.}$$

Среднедневная заработная плата научного руководителя:

$$З_{дн} = (40244{,}5 \cdot 10{,}4) / 244 = 1714{,}3 \text{ руб / день.}$$

4.3.3 Дополнительная заработная плата исполнителей темы

Затраты по дополнительной заработной плате исполнителей темы учитывают величину предусмотренных Трудовым кодексом РФ доплат за отклонение от нормальных условий труда, а также выплат, связанных с обеспечением гарантий и компенсаций.

Дополнительная заработная плата рассчитывается исходя из 10-15 % от основной заработной платы работников, непосредственно участвующих в выполнении темы:

$$З_{доп} = k_{доп} \cdot З_{осн}, \quad (6)$$

где $З_{доп}$ – дополнительная заработная плата, руб.;

$k_{доп}$ – коэффициент дополнительной заработной платы;

$З_{осн}$ – основная заработная плата, руб.

Примем коэффициент дополнительной заработной платы равным 0,15 для научного руководителя и 0,1 для студента. Результаты расчёта основной и дополнительной заработной платы исполнителей научного исследования представлены в таблице 10.

Таблица 10 – Заработная плата исполнителей исследовательской работы

Заработная плата, руб.	Руководитель	Студент
Основная зарплата	40244,5	12811,5
Дополнительная зарплата	6036,7	1281,15
Зарплата исполнителя	46281,2	14092,65
Итого по статье $С_{зп}$	60373,85	

4.3.4 Отчисления во внебюджетные фонды

Размер отчислений во внебюджетные фонды составляет 27,1 % от суммы затрат на оплату труда работников, непосредственно занятых выполнением исследовательской работы.

Величина отчислений во внебюджетные фонды определяется исходя из следующей формулы:

$$C_{\text{внеб}} = k_{\text{внеб}} \cdot (З_{\text{осн}} + З_{\text{доп}}), \quad (7)$$

где $k_{\text{внеб}}$ – коэффициент отчислений на уплату во внебюджетные фонды (пенсионный фонд, фонд обязательного медицинского страхования и пр.).

Величина отчислений во внебюджетные фонды составляет:

$$C_{\text{внеб}} = 0{,}271 \cdot (40244{,}5 + 6036{,}7) = 12542{,}21 \text{ руб.}$$

4.3.7 Накладные расходы

В эту статью включаются затраты на управление и хозяйственное обслуживание, которые могут быть отнесены непосредственно конкретной тему. Кроме того, сюда относятся расходы по содержанию, эксплуатации и ремонту оборудования, производственного инструмента и инвентаря, зданий, сооружений и др.

Расчет накладных расходов ведется по следующей формуле:

$$C_{\text{накл}} = k_{\text{накл}} \cdot (З_{\text{осн}} + З_{\text{доп}}), \quad (8)$$

где $k_{\text{накл}}$ – коэффициент накладных расходов.

Накладные расходы в ТПУ составляют 25-35 % от суммы основной и дополнительной зарплаты работников, участвующих в выполнении темы. Примем $k_{\text{накл}}$ = 30 %.

Накладные расходы составляют:

$$C_{\text{накл}} = 0{,}3 \cdot (40244{,}5 + 6036{,}7) = 13884{,}36 \text{ руб.}$$

4.3.8 Формирование бюджета затрат исследовательского проекта

Рассчитанная величина затрат диссертационной работы является основой для формирования бюджета затрат проекта, который при формировании договора с заказчиком защищается научной организацией в качестве нижнего предела затрат на разработку научно-технической продукции.

Определение бюджета затрат на научно-исследовательский проект по каждому варианту исполнения приведен в таблице 11.

Таблица 11 – Расчёт бюджета затрат диссертационной работы

Наименование статьи	Сумма, руб
1. Материальные затраты исследования	2488
2. Затраты на специальное оборудование	9863
3. Затраты по основной заработной плате исполнителей темы	53056
4. Затраты по дополнительной заработной плате исполнителей темы	7317,9
5. Отчисления во внебюджетные фонды	12542,2
6. Накладные расходы	13884,4
Бюджет затрат исследования	99151,5

4.4 Организационная структура проекта

Организационная структура проекта представляет собой временное структурное образование, создаваемое для достижения поставленных целей и задач проекта и включающее в себя всех участников процесса выполнения работ на каждом этапе.

Данной исследовательской работе соответствует функциональная структура организации. То есть организация рабочего процесса выстроена иерархически: у каждого участника проекта есть непосредственный руководитель, сотрудники разделены по областям специализации, каждой группой руководит компетентный специалист (функциональный руководитель).

Организационная структура научного проекта представлена на рисунке 3.

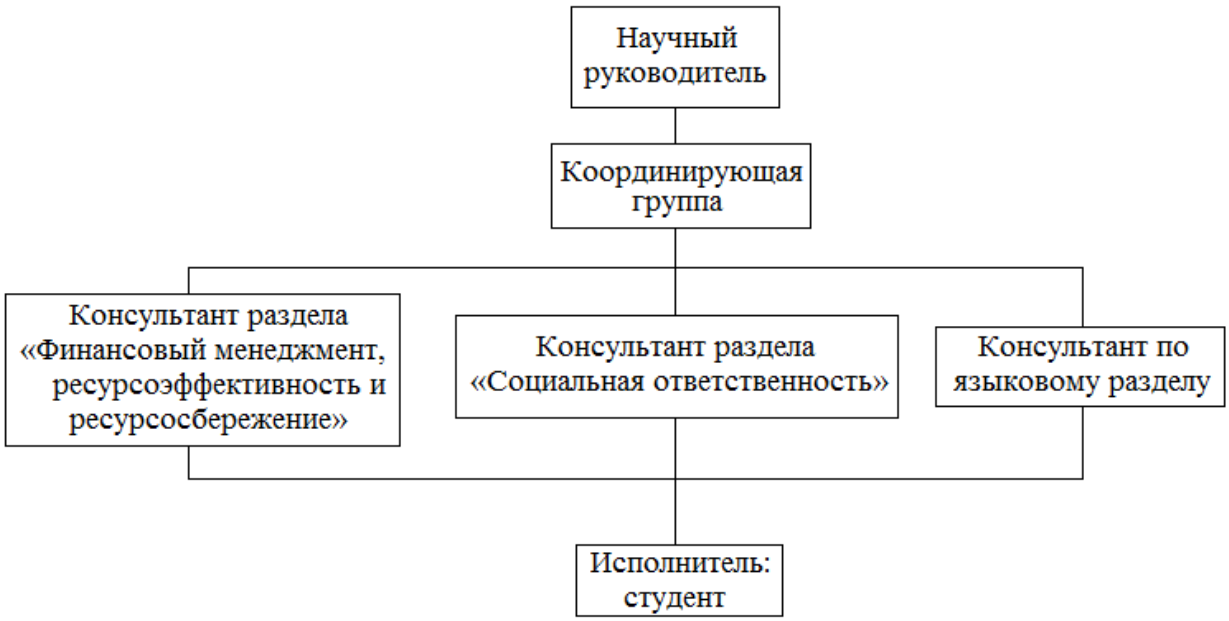

Рисунок 3 – Организационная структура научного проекта

4.5 Матрица ответственности

Степень ответственности каждого члена команды за принятые полномочия регламентируется матрицей ответственности. Матрица ответственности данного проекта представлена в таблице 2.5.

Таблица 12 – Матрица ответственности

Этапы проекта	Научный руководитель	Консультант раздела «Финансовый менеджмент»	Консультант раздела «Соцответственность»	Консультант по языковому разделу	Студент
Разработка технического задания	О				
Составление и утверждение технического задания	О				
Выбор направления исследований	О				И
Подбор и изучение материалов по теме	С				И
Календарное планирование работ	О				И
Изучение особенностей подготовки образцов	С				И
Освоение методики построения алгоритмов оценки систем безопасности	С				И
Проведение анализа уязвимости в отношении ТРО	О				И
Выполнение анализа полученных данных	О				И
Выполнение оценки ресурсоэффективности и ресурсосбережения		С			И
Выполнение раздела по социальной ответственности			С		И
Выполнение перевода части работы на английский язык				С	И
Обобщение и оценка результатов	С				И
Составление пояснительной записки	С				И
Проверка правильности выполнения ГОСТа пояснительной записки	С				И
Подготовка к защите	О				И

Степень участия в проекте характеризуется следующим образом:

– ответственный (О) – лицо, отвечающее за реализацию этапа проекта и контролирующее его ход;

– исполнитель (И) – лицо (лица), выполняющие работы в рамках этапа проекта. Утверждающее лицо (У) – лицо, осуществляющее утверждение результатов этапа проекта (если этап предусматривает утверждение);

– согласующее лицо (С) – лицо, осуществляющее анализ результатов проекта и участвующее в принятии решения о соответствии результатов этапа требованиям.

4.6 Определение ресурсной (ресурсосберегающей), финансовой, бюджетной, социальной и экономической эффективности исследования

Определение эффективности происходит на основе расчета интегрального показателя эффективности научного исследования. Его нахождение связано с определением двух средневзвешенных величин: финансовой эффективности и ресурсэффективности.

Интегральный показатель финансовой эффективности научного исследования получают в ходе оценки бюджета затрат трех (или более) вариантов исполнения научного исследования (см. табл. 2.6). Для этого наибольший интегральный показатель реализации технической задачи принимается за базу расчета (как знаменатель), с которым соотносится финансовые значения по всем вариантам исполнения.

Интегральный финансовый показатель разработки определяется:

$$I_{финр}^{исп.i} = \frac{Ф_{pi}}{Ф_{\max}}, \quad (9)$$

где $I_{финр}^{испi}$ – интегральный финансовый показатель разработки;

$Ф_{pi}$ – стоимость i-го варианта исполнения;

$Ф_{\max}$ – максимальная стоимость исполнения научно-исследовательского проекта (в т.ч. аналоги).

Полученная величина интегрального финансового показателя разработки отражает соответствующее численное увеличение бюджета затрат

разработки в разах (значение больше единицы), либо соответствующее численное удешевление стоимости разработки в разах (значение меньше единицы, но больше нуля).

Так как разработка имеет одно исполнение, то

$$I^{p}_{финр} = \frac{Ф_{p}}{Ф_{\max}} = \frac{99151,5}{99151,5} = 1;$$

Для аналогов соответственно:

$$I^{a1}_{фина1} = \frac{Ф_{a1}}{Ф_{\max}} = \frac{145500,2}{99151,5} = 1,47; \quad I^{a1}_{фина1} = \frac{Ф_{a1}}{Ф_{\max}} = \frac{161260,3}{99151,5} = 1,63$$

Интегральный показатель ресурсоэффективности вариантов исполнения объекта исследования можно определить следующим образом:

$$I_{pi} = \sum a_i \cdot b_i \,, \tag{10}$$

где I_{pi} – интегральный показатель ресурсоэффективности для i-го варианта исполнения разработки;

a_i – весовой коэффициент *i*-го варианта исполнения разработки;

b_i^a, b_i^p – бальная оценка *i*-го варианта исполнения разработки, устанавливается экспертным путем по выбранной шкале оценивания;

n – число параметров сравнения.

Расчёт интегрального показателя ресурсоэффективности представлен ниже.

Таблица 13 – Сравнительная оценка характеристик вариантов исполнения проекта

ПО / Критерии	Весовой коэффициент параметра	Текущий проект	Аналог 1	Аналог 2
1.Способствует росту производительности труда пользователя	0,25	5	3	3
2. Удобство в эксплуатации (соответствует требованиям потребителей)	0,2	5	3	3
3. Помехоустойчивость	0,05	5	3	2
4. Энергосбережение	0,2	5	2	2
5. Надёжность	0,15	5	4	3
6. Материалоёмкость	0,15	5	4	4
ИТОГО	1	5	3,1	2,9

$I_{тп} = 5 \cdot 0,25 + 5 \cdot 0,2 + 5 \cdot 0,05 + 5 \cdot 0,2 + 5 \cdot 0,15 + 5 \cdot 0,15 = 5;$

Аналог 1 $= 3 \cdot 0,25 + 3 \cdot 0,2 + 3 \cdot 0,05 + 2 \cdot 0,2 + 4 \cdot 0,15 + 4 \cdot 0,15 = 3,1;$

Аналог 2 $= 3 \cdot 0,25 + 3 \cdot 0,2 + 2 \cdot 0,05 + 2 \cdot 0,2 + 3 \cdot 0,15 + 4 \cdot 0,15 = 2,9.$

Интегральный показатель эффективности вариантов исполнения разработки ($I^{p}_{финр}$) и аналога ($I^{ai}_{финаi}$) определяется на основании интегрального показателя ресурсоэффективности и интегрального финансового показателя по формуле:

$$I^{p}_{финр} = \frac{I^{p}_{m}}{I^{p}_{финр}};\ I^{ai}_{финаi} = \frac{I^{ai}_{m}}{I^{ai}_{финаi}}; \qquad (11)$$

В результате:

$$I^{p}_{финр} = \frac{I^{p}_{m}}{I^{p}_{финр}} = \frac{5}{1} = 5;\ I^{a1}_{фина1} = \frac{I^{a1}_{m}}{I^{a1}_{фина1}} = \frac{3,1}{1,05} = 2,95;\ I^{a2}_{фина2} = \frac{I^{a2}_{m}}{I^{a2}_{фина2}} = \frac{2,9}{1,16} = 2,5.$$

Сравнение интегрального показателя эффективности текущего проекта и аналогов позволит определить сравнительную эффективность проекта.

Сравнительная эффективность проекта:

$$Э_{ср} = \frac{I^{p}_{финр}}{I^{ai}_{финаi}} \qquad (12)$$

Результат вычисления сравнительной эффективности проекта и сравнительная эффективность анализа представлены в таблице 14.

Таблица 14 – Сравнительная эффективность разработки

	Показатели	Аналог 1	Аналог 2	Разработка
	Интегральный финансовый показатель разработки	1,16	1,29	1
	Интегральный показатель ресурсоэффективности разработки	3,1	2,9	5
	Интегральный показатель эффективности	2,95	2,5	5
	Сравнительная эффективность вариантов исполнения	1,69	2	1

Таким образом, основываясь на определении ресурсосберегающей, финансовой, бюджетной, социальной и экономической эффективности исследования, проведя необходимый сравнительный анализ, можно сделать вывод о превосходстве выполненной разработки над аналогами.

Список публикаций

1 Мерзляков, А. А., Годовых А.В.. Вопросы построения системы безопасности ВУЗ на основе RFID-технологий [Электронный ресурс]/ Мерзляков Александр// VI Школа-конференция молодых атомщиков Сибири : сборник тезисов докладов, 14-16 октября 2015 г., г. Томск / – Томск: Изд-во СТИ НИЯУ МИФИ, 2015. – [С. 123]. — Заглавие с титульного экрана. – Свободный доступ из сети Интернет. – Adobe Reader.

2 Мерзляков, А. А. Годовых А.В. Использование RFID технологий в системе контроля и управления доступом в высших учебных заведениях [Электронный ресурс] / Мерзляков Александр // Физико-технические проблемы в науке, промышленности и медицине: сборник тезисов докладов VII Международной научно-практической конференции, г. Томск, 3-6 июня 2015 г. / – Томск: Изд-во ТПУ, 2015. – [С. 273-274]. –Заглавие с титульного экрана. – Свободный доступ из сети Интернет. – Adobe Reader.

3 Мерзляков, А. А. Годовых А.В. Комплексная безопасность территориально – распределенного объекта [Электронный ресурс] / Мерзляков Александр // Физико-технические проблемы в науке, промышленности и медицине: сборник тезисов докладов VIII Международной научно-практической конференции, г. Томск, 1-3 июня 2016 г. / – Томск: Изд-во ТПУ, 2016. – Заглавие с титульного экрана. – Свободный доступ из сети Интернет. – Adobe Reader.