МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

федеральное государственное бюджетное образовательное учреждение
высшего образования
«Тольяттинский государственный университет»

_____
(*наименование института*)
Кафедра ««Прикладная математика и информатика»
(*наименование кафедры*)

# ОТЧЕТ
# ПРОИЗВОДСТВЕННАЯ ПРАКТИКА (НИР) -1

(*наименование практики*)

**ОБУЧАЮЩЕГОСЯ:**

*(И.О. Фамилия)*

**НАПРАВЛЕНИЕ ПОДГОТОВКИ (СПЕЦИАЛЬНОСТЬ):** 09.04.03 Прикладная информатика, Информационные системы и технологии корпоративного управления



**ГРУППА:**

**РУКОВОДИТЕЛЬ ПРАКТИКИ:** _____

*(И.О. Фамилия)*

**ДАТА СДАЧИ ОТЧЕТА**_____

Руководитель практики от организации
(предприятия, учреждения, сообщества)

_____
(фамилия, имя, отчество, должность)

Тольятти 2019г.

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

федеральное государственное бюджетное образовательное учреждение
высшего образования
«Тольяттинский государственный университет»

Институт математики, физики и информационных технологий
(*наименование института*)
Кафедра ««Прикладная математика и информатика»
(*наименование кафедры*)

# АКТ о прохождении практики

**Данным актом подтверждается, что**

**ОБУЧАЮЩИЙСЯ: ДЕМОЧКИН ВАСИЛИЙ СЕРГЕЕВИЧ**
*(И.О. Фамилия)*

**НАПРАВЛЕНИЕ ПОДГОТОВКИ (СПЕЦИАЛЬНОСТЬ):** 09.04.03 Прикладная информатика, Информационные системы и технологии корпоративного управления



**ГРУППА:** ПИмд-1802а



Проходил производственную (НИР-1) практику
(*наименование практики*)

в _____
(*наименование организации*)

в период с 10.08.2019 по 30.11.2019 г.

Руководитель практики от кафедры:

_____
(фамилия, имя, отчество, должность)

ОЦЕНКА _____

_____
(подпись)

Руководитель практики от организации
(предприятия, учреждения, сообщества):

_____
(фамилия, имя, отчество, должность)

М.П. _____
(подпись)

Тольятти 219г.

**РЕФЕРАТ**

Отчет 42 с., 2 части, 7 рис., 2 табл., 48 источников, 1 приложение.

ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ, ОБУЧАЮЩАЯ СРЕДА, УЧРЕЖДЕНИЕ ДОПОЛНИТЕЛЬНОГО ОБРАЗОВАНИЯ, ИНФОРМАЦИОННО-ОБРАЗОВАТЕЛЬНАЯ СРЕДА, ПРОГРАММНО-МЕТОДИЧЕСКИЙ КОМПЛЕКС, ИНФОРМАТИЗАЦИЯ ОБРАЗОВАНИЯ.

Научно-исследовательская работа магистрантов (НИР) является важным средством повышения качества подготовки и воспитания специалистов, способных применять в практической деятельности достижения научно-технического прогресса.

Целью научно-исследовательской работы студентов является формирование у выпускника способности и готовности к выполнению профессиональных функций в научных и корпоративных организациях, в аналитических под-разделениях, компетенций в сфере научно-исследовательской и инновационной деятельности и др.; дальнейшее формирование профессиональной направленности личности студента, развитие практико-действенного компонента его мышления, формирование его готовности к профессиональной деятельности в исследовании, проектировании и внедрении информационных систем, становление системы профессиональных ценностей.



Задачи практики:

- обобщение и критический анализ результатов, полученных отечественными и зарубежными учеными, выявление и формулирование актуальных научных проблем;

- обоснование актуальности, теоретической и практической значимости темы научного исследования, разработка плана и программы проведения научного исследования;

- проведение самостоятельного исследования в соответствии с разработанной программой;

- разработка теоретических моделей исследуемых процессов, явлений и объектов;

- выбор методов и средств, разработка инструментария эмпирического исследования, сбор, обработка, анализ, оценка и интерпретация полученных результатов исследования;

- представление результатов проведенного исследования в виде научного отчета, статьи, доклада, магистерской диссертации в соответствии с существующими требованиями.

Методы, применяемые на эмпирическом уровне, - анализ научно-методической литературы, научное наблюдение, обобщение опыта преподавания, беседа, статистический анализ результатов работы.

В результате выполнения научно-исследовательской работы 1, были составлены: портфолио магистранта и индивидуальный план студента на все года обучения в магистратуре.



Портфолио применимо для систематизирования накапливаемого опыта, знаний, определения направления развития студента, облегчение консультирования со стороны более квалифицированных специалистов в конкретной сфере, а также для более объективной оценки своего профессионального уровня.

**СОДЕРЖАНИЕ**

## ОПРЕДЕЛЕНИЯ, ОБОЗНАЧЕНИЯ И СОКРАЩЕНИЯ

В настоящем отчете о НИР применяются следующие термины с соответствующими определениями, обозначениями и сокращениями:

НИР – научно-исследовательская работа;

ТГУ – Тольяттинский государственный университет;

# 1. ОСНОВНАЯ ЧАСТЬ

## 1.1 Практическое задание № 1

### Портфолио магистранта

| ФОТО |
|---|

ФИО: Демочкин Василий Сергеевич

Место работы:

Должность:

Контакты: тел.

e-mail: Vdemochk@yandex.ru



**Образование**

| Наименование квалификации | Наименование документа, подтверждающего квалификацию (диплом о высшем образовании, переподготовки, повышения квалификации и т.д.) | Наименование направления подготовки, программы переподготовки, повышения квалификации | Организация, где получена квалификация |
|---|---|---|---|
| | | | |
| | | | |
| | | | |

**Научные публикации**

| Наименование публикации | Форма работы (статья, монография, отчет, патент, пособие и т.д.) | Выходные данные | Объем в п.л. или с. | Соавторы |
|---|---|---|---|---|
| - | - | - | - | - |
| | | | | |

Сведения о получении именных стипендий _____-_____

Опыт работы, соответствующий направлению подготовки:

Академическая мобильность (документы, подтверждающие факт обучения за рубежом_____-_____

Владение иностранным языком (вид иностранного языка, уровень владения)
Немецкий, базовый уровень; английский, со словарем

Дополнительные сведения _____-_____

1.1 Практическое задание № 2

Составление индивидуального плана студента

федеральное государственное бюджетное образовательное учреждение
высшего образования
«Тольяттинский государственный университет»

**Институт математики, физики и информационных технологий**

Кафедра **«Прикладная математика и информатика»**

УТВЕРЖДАЮ
Заведующий кафедрой «Прикладная математика и информатика»
_____ А.В. Очеповский
«____»_____20__ г.



**ИНДИВИДУАЛЬНЫЙ ПЛАН СТУДЕНТА**

**20___ / 20___ уч. год**

**ДЕМОЧКИН ВАСИЛИЙ СЕРГЕЕВИЧ**
(фамилия, имя, отчество студента)

09.04.03 Прикладная информатика

Информационные системы и технологии корпоративного управления

Форма обучения заочная дистанционная Группа: ПИмд-1802а

Научный руководитель студента XXXXXXXXXXXXXXXX

Тема магистерской диссертации: XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX

**Руководитель магистерской программы**
к.тех.н., доцент,
зав. кафедрой «Прикладная математика и информатика» _____А.В. Очеповский

«___» _____ 20__г.

Тольятти 2019г.

## 1 семестр

### План учебной работы

| № п/п | Наименование учебных курсов, практик | Общая трудоемкость | | Форма контроля |
|---|---|---|---|---|
| | | ЗЕТ | Часов | |
| 1 | Философские проблемы науки и техники | 4 | 144 | Экзамен |
| 2 | Информационное общество и проблемы прикладной информатики | 6 | 216 | Экзамен |
| 3 | Методология и практика ИТ-консалдинга | 5 | 180 | Зачет |
| 4 | Английский язык 1 | 2 | 72 | Зачет |
| 6 | Корпоративные информационные системы | 6 | 216 | Экзамен, курсовая работа |
| 7 | Научно-исследовательская работа в семестре 1 | 3 | 108 ч. | Зачет |

### План научно-исследовательской работы (НИР) в 1 семестре

**Общая трудоемкость: 3 ЗЕТ, 108 часов**

| № п/п | Наименование планируемых работ, этапов выполнения магистерской диссертации | Форма отчетности | Планируемый срок | Отметки научного руководителя | | |
|---|---|---|---|---|---|---|
| | | | | о выполнении работ* | дата | подпись |
| 1 | Ознакомление с тематикой исследовательских работ по профилю магистерской программы | Индивидуальный план | | | | |
| 2 | Выбор темы и составление индивидуального плана работы студента | | | | | |
| 3 | Обоснование актуальности исследования, определение объекта и предмета исследования, формулировка целей и задач исследования. Выдвижение рабочей гипотезы исследования. | Проспект введения магистерской диссертации | | | | |
| 4 | Работа с научной литературой по теме исследования, составление библиографии. Подготовка реферата. | Реферат (материалы литературного обзора). | | | | |
| 5 | Сравнительный анализ альтернативных решений, уточнение постановки задачи и требований к работе. | Проспект аналитической части магистерской диссертации | | | | |

| | | | | | | |
|---|---|---|---|---|---|---|
| 6 | Уточнение требований к работе.<br><br>Предоставление отчета на научно-исследовательский семинар кафедры | Отчет о выполнении НИРС за семестр | | | | |

Студент _____ Научный руководитель _____
(подпись) (подпись)
«____» _____ 20___ г. «____» _____ 20___ г.
Отчет о выполнении плана заслушан на заседании кафедры
от «____» _____ 20____ г. Протокол № _____

**Заключение кафедры:**

Научный руководитель _____
(подпись)
«____» _____ 20___ г.

## 2 семестр

### План учебной работы

| № п/п | Наименование учебных курсов, практик | Общая трудоемкость | | Форма контроля |
|---|---|---|---|---|
| | | ЗЕТ | Часов | |
| 1 | Математическое моделирование | 5 | 180 | Экзамен |
| 2 | Безопасность корпоративных информационных систем | 4 | 144 | Зачет |
| 3 | Английский язык 2 | 3 | 108 | Зачет |
| 6 | Научно-исследовательская работа в семестре 2 | 3 | 108 ч. | Зачет с оценкой |
| 8 | Учебная практика | 3 | 108 ч. | Зачет |

### План научно-исследовательской работы (НИР) в 2 семестре

**Общая трудоемкость: 3 ЗЕТ, 108 часов**

| № п/п | Наименование планируемых работ, этапов выполнения магистерской диссертации | Форма отчетности | Планируемый срок | Отметки научного руководителя | | |
|---|---|---|---|---|---|---|
| | | | | о выполнении работ | дата | подпись |
| 1 | Выбор методов и подходов аналитического и математического аппаратов исследования | Проспект теоретической части магистерской диссертации | | | | |
| 2 | Проектирование структуры и компонентов программного продукта | Контекстная диаграмма и ее декомпозиция в 2-3-х уровнях | | | | |
| 3 | Обоснование выбора и описание основных средств реализации программного продукта | Проспект проектной части магистерской диссертации | | | | |
| 4 | Уточнение требований к работе.<br><br>Предоставление отчета на научно-исследовательский семинар кафедры | Отчет о выполнении НИРС за семестр | | | | |

Студент _____ Научный руководитель _____
(подпись) (подпись)
«____» _____ 20___ г. «____» _____ 20___ г.
Отчет о выполнении плана заслушан на заседании кафедры
от «____» _____ 20____ г. Протокол № _____

**Заключение кафедры:**

Научный руководитель _____
(подпись)
«____» _____ 20___ г.



**3 семестр**

## План учебной работы

| № п/п | Наименование учебных курсов, практик | Общая трудоемкость | | Форма контроля |
|---|---|---|---|---|
| | | ЗЕТ | Часов | |
| 1 | Математические и инструментальные методы поддержки принятия решений | 5 | 180 | Экзамен |
| 2 | Распределенные информационные системы | 6 | 216 | Экзамен |
| 3 | Методология и технология проектирования информационных систем | 6 | 216 | Курсовая работа<br><br>Экзамен |
| 5 | Научно-исследовательская работа в семестре 3 | 3 | 108 ч. | Зачет |
| 6 | Технологическая практика | 3 | 108 ч. | Зачет с оценкой |

## План научно-исследовательской работы (НИР) в 3 семестре

**Общая трудоемкость: 3 ЗЕТ, 108 часов**



| № п/п | Наименование планируемых работ, этапов выполнения магистерской диссертации | Форма отчетности | Планируемый срок | Отметки научного руководителя | | |
|---|---|---|---|---|---|---|
| | | | | о выполнении работ | дата | подпись |
| 1 | Разработка алгоритмов реализации проектируемого программного продукта | Функциональные и проектные спецификации | | | | |
| 2 | Реализация разработанных алгоритмов в программный продукт | Программный продукт | | | | |
| 3 | Тестирование и отладка программного продукта в образовательной среде | Результаты тестирования | | | | |
| 4 | Подготовка и оформление практической части<br><br>магистерской диссертации (реализация и использование программного продукта) | Проспект практической части<br><br>магистерской диссертации | | | | |
| | Подготовка доклада и выступление на конференции | Доклад (рукопись публикации) | | | | |
| | Подготовка научной публикации по теме | Копию опубликованно | | | | |

| | | | | | | |
|---|---|---|---|---|---|---|
| | исследования | й статьи и ее выходные данные | | | | |
| | Уточнение требований к работе.<br><br>Предоставление отчета на научно-исследовательский семинар кафедры | Отчет о выполнении НИРС за семестр | | | | |

Студент _____ Научный руководитель _____
(подпись) (подпись)
«____» _____ 20___ г. «____» _____ 20___ г.
Отчет о выполнении плана заслушан на заседании кафедры
от «____» _____ 20____ г. Протокол № _____

**Заключение кафедры:**

Научный руководитель _____
(подпись)
«____» _____ 20___ г.

## 4 семестр

## План учебной работы

### План учебной работы

| № п/п | Наименование учебных курсов, практик | Общая трудоемкость | | Форма контроля |
|---|---|---|---|---|
| | | ЗЕТ | Часов | |
| 1 | Математические модели в теории управления и исследования операций | 4 | 144 | Зачет |
| | Методологии создания и внедрения корпоративных информационных систем | 5 | 180 | Курсовая работа<br><br>Экзамен |
| | Многомерные статистические методы | 5 | 180 | Экзамен |
| | Педагогическая практика | 3 | 108 | Зачет с оценкой |
| 2 | Научно-исследовательская работа в семестре 4 | 6 | 216 | зачет |



**План научно-исследовательской работы (НИР) в 4 семестре**

**Общая трудоемкость: 6 ЗЕТ, 216 часов**

| № п/п | Наименование планируемых работ, этапов выполнения магистерекой диссертации | Форма отчетности | Планируемый срок | Отметки научного руководителя | | |
|---|---|---|---|---|---|---|
| | | | | о выполнении работ | дата | подпись |
| 1 | Проведение экспериментального исследования по теме диссертации | Результаты эксперимента | | | | |
| 2 | Обработка результатов исследований в соответствии с рабочей гипотезой | Таблицы и диаграммы | | | | |
| 3 | Подготовка и оформление доказательной базы диссертационного исследования согласно рабочей гипотезе | Проспект рекомендательной части магистерской диссертации | | | | |
| | Подготовка доклада и выступление на конференции | Доклад (рукопись публикации) | | | | |
| | Подготовка научной публикации по теме | Копию опубликованн | | | | |

| | | | | | | |
|---|---|---|---|---|---|---|
| | исследования | ой статьи и ее выходные данные | | | | |
| | Уточнение требований к работе.<br><br>Предоставление отчета на научно-исследовательский семинар кафедры | Отчет о выполнении НИРС за семестр | | | | |

Студент _____ Научный руководитель _____
(подпись) (подпись)
«____» _____ 20___ г. «____» _____ 20___ г.
Отчет о выполнении плана заслушан на заседании кафедры

от «____» _____ 20____ г. Протокол № _____

**Заключение кафедры:**

Научный руководитель _____
(подпись)
«____» _____ 20___ г.

## 5 семестр

## План учебной работы

### План учебной работы

| № п/п | Наименование учебных курсов, практик | Общая трудоемкость | | Форма контроля |
|---|---|---|---|---|
| | | ЗЕТ | Часов | |
| 1 | Преддипломная практика | 3 | 1084 | Зачет с оценкой |
| 2 | Научно-исследовательская работа в семестре 5 | 18 | 648 | зачет |

### План научно-исследовательской работы (НИР) в 5 семестре

**Общая трудоемкость: 18 ЗЕТ, 648 часов**

| № п/п | Наименование планируемых работ, этапов выполнения магистерской диссертации | Форма отчетности | Планируемый срок | Отметки научного руководителя | | |
|---|---|---|---|---|---|---|
| | | | | о выполнении работ | дата | подпись |
| 1 | Описание результатов исследований в соответствии с рабочей гипотезой | Диаграммы и сравнительные таблицы | | | | |
| 2 | Подготовка материалов для автореферата | Автореферат | | | | |
| 3 | Подготовка презентационного материала для выступления | Презентация | | | | |
| | Уточнение требований к работе.<br><br>Предоставление отчета на научно-исследовательский семинар кафедры | Отчет о выполнении НИРС за семестр | | | | |



Студент _____ (подпись) Научный руководитель _____ (подпись)

«____» _____ 20___ г. «____» _____ 20___ г.

Отчет о выполнении плана заслушан на заседании кафедры

от «____» _____ 20____ г. Протокол № _____

**Заключение кафедры:**

Научный руководитель _____
(подпись)
«____» _____ 20___ г.

**Итоговая государственная аттестация:**

| № п/п | Наименование | Сроки (с … по …) | Трудоемкость | |
|---|---|---|---|---|
| | | | ЗЕТ | Недель |
| | Оформление и защита диссертации | | 9 | 6 |
| | | | | |

Студент _____ (подпись)
«____» _____ 20___ г.

Научный руководитель _____ (подпись)
«____» _____ 20___ г.

Отчет о выполнении плана заслушан на заседании комиссии по предварительной защите магистерских диссертаций

от «____» _____ 20____ г. Протокол № _____



**Заключение комиссии по предзащите магистерских диссертаций о выполнении магистерской диссертации:**



Научный руководитель _____ (подпись)
«____» _____ 20___ г.

Тема магистерской диссертации _____
_____
_____
_____

утверждена распоряжением _____ (директора института)
№ _____ от «____» _____ 20___

## 1.3 Практическое задание № 3

Тема магистерской диссертации: «Разработка требований к средствам защиты информации в корпоративных системах на основе анализа рисков».

### Резюме (аннотация)

В данной реферативной работе исследована актуальность разработки требований к средствам защиты информации в корпоративных системах на основе анализа рисков.

Проблема информационной безопасности (ИБ) корпоративной системы обычно решается в двух плоскостях: во-первых, рассматриваются формальные критерии, которым должны соответствовать защищенные информационные технологии, а во-вторых, практический аспект - конкретный комплекс мер безопасности.



### Введение

Информационная безопасность - один из главных приоритетов современного бизнеса, поскольку нарушения в этой сфере приводят к гибельным последствиям для бизнеса любой компании.

В связи с применением высоких информационных технологий XXI века, с одной стороны, дает значительные преимущества в деятельности предприятий и организаций, а с другой - потенциально создает предпосылки для утечки, хищения, утраты, искажения, подделки, уничтожения, копирования и блокирования информации и, как следствие, это приводит к нанесению экономического, социального или других видов ущерба, т.е. проблема информационных рисков и нахождения путей снижения ущерба становится с каждым годом все острее.

Во многих странах, в том числе и в России, существуют национальные стандарты. Принят международный стандарт ISO 15408 «Общие критерии оценки безопасности информационных технологий», но это только формальные критерии.

Практические правила обеспечения безопасности в большинстве случаев рассматриваются лишь на концептуальном уровне. На практике сразу возникают вопросы.

- Где уязвимые места в информационной системе?
- Какие угрозы безопасности существуют, как оценить их серьезность?
- Какой остаточный уровень рисков допустим?
- Какой комплекс мер снизит риски до допустимого уровня?

На эти и другие вопросы, интересующие администраторов безопасности, ответа обычно не дается. Дело в том, что каждый из них сложен и требует специального исследования.



При изобилии средств защиты, позиционируемых производителем как средства защиты КИС при информационном обмене с Интернет, сегодня практически отсутствуют критерии их выбора, применимости и эффективности в конкретных информационных системах, особенно когда применяется набор средств различных производителей.

Объектом исследования являются информационные (автоматизированные) системы, внешний информационный обмен в которых значим с точки зрения обеспечения их деятельности, а также средства защиты информации, обеспечивающие защиту сервисов внешнего информационного обмена.

Предметом исследования является требования к средствам защиты информации в корпоративных системах на основе анализа рисков.

Целью работы является разработка требований к средствам защиты информации в корпоративных системах на основе анализа рисков.

Для достижения поставленной цели в работе решались следующие задачи:

- Выявление специфики систем внешнего информационного обмена с точки зрения защиты информации;

- Определение взаимосвязи угроз и уязвимостей, делающих возможной их реализацию;

- Классификация угроз в зависимости от значимости наносимого ими ущерба;

- Формализация задачи защиты систем внешнего информационного обмена с использованием модели рисков;

- Анализ требований, предъявляемых к отдельным средствам защиты информации;

- Разработка требований к средствам защиты информации в корпоративных системах на основе анализа рисков.

Методы исследования: для решения поставленных задач использовались методы количественного анализа и моделирования рисков, системного анализа.



## 1.Защита информации в корпоративных системах

Главной целью любой системы обеспечения информационной безопасности является обеспечение устойчивого функционирования предприятия, предотвращение угроз его безопасности, защита законных интересов предприятия от противоправных посягательств, недопущение хищения финансовых средств, разглашения, утраты, утечки, искажения и уничтожения служебной информации, обеспечение нормальной торговой и производственной деятельности всех подразделений предприятия.

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

В России, существуют национальные стандарты. Принят международный стандарт ISO 15408 “Общие критерии оценки безопасности информационных технологий”.

В конце 2000 г. принят стандарт ISO 17799, в основу которого положен BS 7799.

В соответствии с рекомендациями ведущих международных стандартов в области планирования информационной безопасности и управления ею политики безопасности должны содержать следующее:

- предмет, основные цели и задачи политики безопасности;

- условия применения политики безопасности и возможные ограничения;

- описание позиции руководства компании в отношении выполнения политики безопасности и организации режима информационной безопасности компании в целом;

- права и обязанности, а также степень ответственности сотрудников за выполнение политики безопасности компании;

- порядок действия в чрезвычайных ситуациях в случае нарушения политики безопасности.



В настоящее время большинством российских компаний определены следующие приоритетные задачи развития и совершенствования своей деятельности:

- минимизация рисков бизнеса путем защиты своих интересов в информационной сфере;

- обеспечение безопасного, доверенного и адекватного управления предприятием;

- планирование и поддержка непрерывности бизнеса;

- повышение качества деятельности по обеспечению информационной безопасности;

- снижение издержек и повышение эффективности инвестиций в информационную безопасность;

- повышение уровня доверия к компании со стороны акционеров, партнеров, уполномоченных государственных органов и др.

Современный рынок средств защиты информации можно условно разделить на две группы:

- средства защиты для государственных структур, позволяющие выполнить требования нормативно-правовых документов (федеральных законов, указов Президента РФ, постановлений Правительства РФ), а также требования нормативно-технических документов (государственных стандартов, руководящих документов Гостехкомиссии (ФСТЭК) России, силовых ведомств РФ;

- средства защиты для коммерческих компаний и структур, позволяющие выполнить требования и рекомендации федеральных законов, указов Президента РФ, постановлений Правительства РФ и некоторых международных стандартов.

Можно привести следующую краткую характеристику основных средств защиты информации:

1. Средства управления обновлениями



Внедрение средств управления обновлениями программных компонент автоматизированных систем. К таким относятся Microsoft Software Update Services, позволяет уменьшить объем интернет-трафика предприятия в целом, так как становится возможным организовать и контролировать необходимые обновления программных компонент автоматизированных систем предприятия с одной точки – выделенного внутреннего сервера.

2. Средства межсетевого экранирования

Межсетевые экраны используются как средства защиты от несанкционированного доступа периметра сети и основных критичных компонент автоматизированных систем.

3. Средства построения VPN

Средства построения виртуальных частных сетей (VPN) используются для организации защиты трафика данных, передаваемых по открытым каналам связи.

4. Средства контроля доступа

Данные средства осуществляют аутентификацию (точное опознание) подключающихся к автоматизированным системам (АС) пользователей и

процессов, авторизацию (наделение определенными полномочиями) пользователей и процессов, регламентируя доступ множества пользователей к приложениям и информационным ресурсам предприятия.

5. Средства обнаружения вторжений и аномалий

Средства обнаружения вторжений (Intrusion Detection Systems, IDS) позволяют с помощью некоторого регламента проверок контролировать состояние безопасности корпоративной сети в реальном масштабе времени.

6. Средства резервного копирования и архивирования

Средства резервного копирования и архивирования применяются для обеспечения целостности хранилищ в случаях аппаратных и программных сбоев, ошибочных действий администраторов и пользователей, а также отказов средств вычислительной техники.

7. Средства централизованного управления безопасностью

Средства централизованного управления информационной безопасностью позволяют эффективно создавать, проверять и поддерживать технические политики безопасности программных компонент автоматизированной системы.



8. Средства предотвращения вторжений на уровне серверов

Так как серверы компании обычно являются основной целью атак злоумышленников (на них обрабатывается основная часть конфиденциальной информации компании), то необходимо использовать средства предотвращения вторжений на уровне серверов.

9. Средства мониторинга безопасности.

Большое количество средств обеспечения информационной безопасности (межсетевые экраны, системы обнаружения вторжений, маршрутизаторы, средства создания виртуальных частных сетей, журналы безопасности серверов, системы аутентификации, средства антивирусной защиты и т.д.) генерирует огромное количество сообщений.

10. Средства контроля деятельности сотрудников в Интернете.

В настоящее время одной из серьезных проблем в работе отечественных служб безопасности является предотвращение попыток использования интернет-ресурсов компании в личных целях (загрузка видео, аудио, картинок, нелицензированного программного обеспечения).

11. Средства анализа содержимого почтовых сообщений

Средства анализа содержимого почтовых сообщений предназначены для обнаружения и предотвращения передачи конфиденциальной информации с помощью корпоративной электронной почты.

12. Средства анализа защищенности

Основной особенностью наиболее продаваемых и используемых коммерческих сканеров является возможность как минимум еженедельно обновлять базы данных уязвимостей путем взаимодействия с крупнейшими центрами по сбору новых уязвимостей и с ведущими производителями сетевого оборудования и программного обеспечения.



13. Средства защиты от спама

14. Средства защиты от атак класса «отказ в обслуживании»

В связи с тем, что атаки класса «отказ в обслуживании» приносят значительные убытки отечественным и западным компаниям, можно воспользоваться специальными средствами защиты.

15. Средства контроля целостности

Внесение некорректного изменения в конфигурацию сервера или маршрутизатора может привести к выходу из строя необходимого сервиса или целой сети.

16. Средства инфраструктуры открытых ключей.

Успешное выполнение перечисленных задач проблематично. Это связано с. возрастающей необходимостью повышения уровня информационной безопасности и недостаточной проработанностью политик информационной безопасности в отечественных компаниях.

## 2.Практические аспекты информационной безопасности в корпоративных системах

Практические правила обеспечения ИБ на всех этапах жизненного цикла информационной технологии должны носить комплексный характер и основываться на проверенных практикой приемах и методах.

При создании систем ИБ важно не упустить каких-либо существенных аспектов - в этом случае применяемой информационной технологии будет гарантирован некоторый минимальный (базовый) уровень ИБ.

Базовый уровень ИБ (рисунок 1) предполагает упрощенный подход к анализу рисков, при котором рассматривается стандартный набор распространенных угроз безопасности без оценки вероятностей этих угроз.

Для нейтрализации угроз применяется типовой комплекс контрмер, а вопросы эффективности защиты в расчет не берутся. Подобный подход приемлем, если ценность защищаемых ресурсов в данной организации не слишком высока.




Рисунок 1 - Разработка требований к ИБ

В ряде случаев базового уровня оказывается недостаточно. Для обеспечения повышенного уровня ИБ необходимо знать параметры, характеризующие степень безопасности информационной системы (технологии) и количественные оценки угроз безопасности, уязвимости, ценности информационных ресурсов. В том или ином виде рассматриваются ресурсы, характеристики рисков и уязвимости информационной системы. Как правило, проводится анализ по критерию стоимость/эффективность нескольких вариантов защиты.

Несмотря на существенную разницу в методологии обеспечения базового и повышенного уровней безопасности можно говорить о единой концепции ИБ.

Обеспечение базового уровня информационной безопасности в соответствии с ISO 17799 предполагает определенную последовательность действий (рисунок 2).

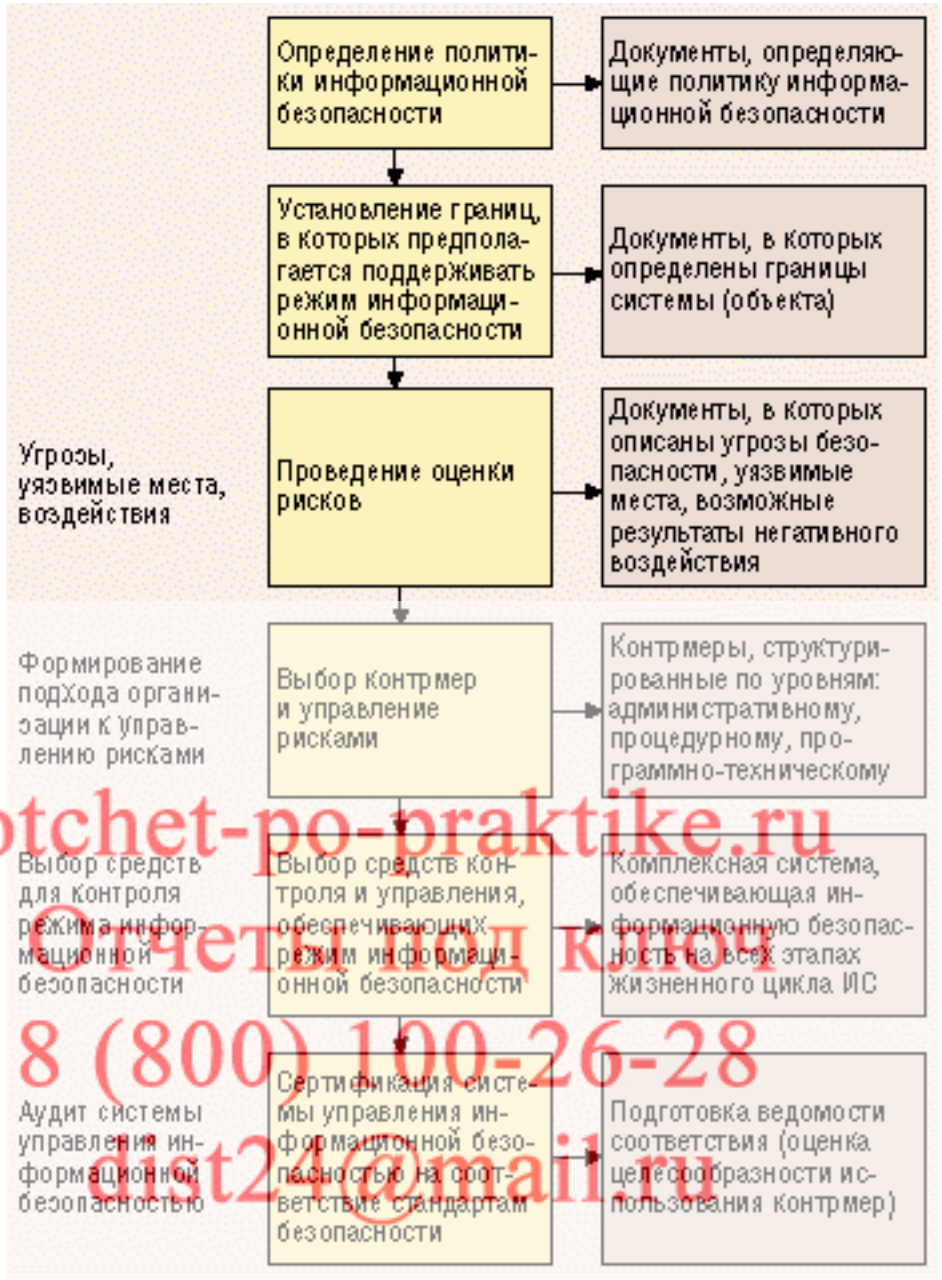




Рисунок 2 - Определение политики ИБ

Стратегия безопасности в практическом плане сводится к следующим шагам.

1. Определение необходимых руководящих документов и стандартов в области ИБ, а также основных положений политики ИБ, включая:

- управление доступом к средствам вычислительной техники (СВТ), программам и данным;

- антивирусную защиту;

- вопросы резервного копирования;

- проведение ремонтных и восстановительных работ;

- информирование об инцидентах в области ИБ.

2. Определение подходов к управлению рисками: является ли достаточным базовый уровень защищенности или нужно проводить полный вариант анализа рисков.

3. Структуризация контрмер по уровням.

4. Порядок сертификации на соответствие стандартам в области ИБ: график совещаний по тематике ИБ на уровне руководства, периодичность пересмотра положений политики ИБ, а также порядок обучения всех категорий пользователей информационной системы в этой области.

Задача оценки рисков:

На этом этапе ставится задача оценки рисков и обосновываются требования к методике их оценки.



К оценке рисков существуют различные подходы, выбор которых зависит от уровня требований к безопасности, характера угроз и эффективности потенциальных контрмер.



Минимальные требования к ИБ:

Минимальным требованиям соответствует базовый уровень ИБ, обычно реализуемый в типовых проектных решениях. В стандарте определен набор наиболее вероятных угроз, таких, как вирусы, сбои оборудования, несанкционированный доступ и т. д. Контрмеры для нейтрализации этих угроз должны быть приняты обязательно вне зависимости от вероятности их осуществления и уязвимости ресурсов. Таким образом, характеристики угроз на базовом уровне рассматривать не обязательно.

Повышенные требования к ИБ:

В случаях, когда нарушения режима ИБ чреваты тяжелыми последствиями, базового уровня требований становится недостаточно. Чтобы сформулировать дополнительные требования, необходимо:

- определить ценность ресурсов;

- к стандартному набору добавить список угроз, актуальных для исследуемой информационной системы;

- оценить вероятность угроз;

- определить уязвимость ресурсов.

Выбор контрмер и управление рисками:

Должна быть разработана стратегия управления рисками разных классов. Возможно несколько подходов.

1. Уменьшение риска. Например, грамотное управление паролями снижает вероятность несанкционированного доступа.

2. Уклонение от риска. Например, вынесение Web-сервера за пределы локальной сети организации позволяет избежать несанкционированного доступа в локальную сеть со стороны Web-клиентов.

3. Изменение характера риска. Если не удается уклониться от риска или эффективно его уменьшить, можно принять некоторые меры страховки:

- застраховать оборудование от пожара;

- заключить договора с поставщиками СВТ о сопровождении и компенсации ущерба в случае нештатной ситуации.

4. Принятие риска. Многие риски не могут быть уменьшены до пренебрежимо малой величины.



На практике, после того как бывает принят стандартный набор контрмер, ряд рисков уменьшается, но все же остается значимым. Поэтому необходимо знать остаточную величину риска.

Когда этап по определению принимаемых во внимание рисков завершен, должна быть предложена стратегия управления.

Выбор мер, обеспечивающих режим ИБ:

Комплекс предлагаемых мер должен быть построен в соответствии с выбранной стратегией управления рисками и структурирован по уровням (организационному, программно-техническому) и отдельным аспектам безопасности. Если проводится полный вариант анализа рисков, то эффективность комплекса контрмер оценивается для каждого риска.

Аудит системы управления ИБ:

При аудите проверяется, насколько выбранные контрмеры соответствуют декларированным в политике безопасности целям. В результате создается ведомость соответствия, в которой описывается анализ эффективности контрмер.

Обеспечение повышенных требований к ИБ:

Если к ИБ предъявляются повышенные требования, проводится так называемый полный вариант анализа рисков, в рамках которого в дополнение к базовым рассматриваются:

- модель бизнес-процессов с точки зрения ИБ;

- ресурсы организации и их ценность;

- составление полного списка угроз безопасности - потенциальные источники нежелательных событий, которые могут нанести ущерб ресурсам, и оценка их параметров;

- уязвимости - слабые места в защите, которые могут спровоцировать реализацию угрозы.

На основе собранных сведений оцениваются риски для информационной системы организации, для отдельных ее подсистем, баз данных и элементов данных.



Следующим шагом должен стать выбор контрмер, снижающих риски до приемлемых уровней.

## Заключение

Задача внешнего информационного обмена по значимости (а значит и по уровню требований к защите информационных ресурсов) сопоставима с другими задачами, решаемыми в корпоративных информационных системах. Задача анализа рисков в системах внешнего информационного обмена существенно упрощается за счет ограниченного набора сервисов в системах внешнего информационного обмена.

При проведении классификации можно выделить три класса угроз: угрозы первого типа, вероятность реализации которых не зависит от стоимости информационных ресурсов, угрозы второго типа, вероятность реализации которых растет с ростом значимости информационных ресурсов, угрозы третьего типа, имеющие вероятность реализации обратно пропорционально наносимому ущербу.

Связь между угрозами и возможным ущербом от их реализации позволяет создать достаточно простую, но адекватную модель количественного анализа рисков в системах внешнего информационного обмена.

## Список использованной литературы


1. Бетелин В.Б., Галатенко В.А., Кобзарь М.Т., Сидак А.А., Трифаленков И.А. Профили защиты на основе общих критериев. // Безопасность информационных технологий. М., 2003. - № 1. - 32 с.
2. Галатенко В.А., Трифаленков И.А. Информационная безопасность в Интранет: концепции и решения // Jetlnfo. М.: Джет Инфо Паблишер, 1996. -№23-24.-78 с.
3. Геннаднева Е.Г. Технико-экономические показатели задачи защиты информации // Безопасность информационных технологий. М., 1997. -№ 3. - С. 67-75.
4. Герасименко В.А. Защита информации в автоматизированных системах обработки данных. В 2 книгах: Книга 1. М.: Энергоатомиздат, 1994. - 400 с.
5. Калянов Г.Н. Консалтинг: от бизнес-стратегии к корпоративной информационно-управляющей системе. М.: Горячая линия-Телеком, 2004. -200 с.
6. Касперский Е.В. Основные классы угроз в компьютерном сообществе 2003 года, их причины и способы устранения // Jetlnfo. М.: Джет Инфо Паблишер, 2003. - №12. - 40 с.

7. Лукацкий А.В. Системы обнаружения атак // Сетевой. М., 2002. - №4. - С.5-16.
8. Медведовский И.Д., Семьянов П.В., Платонов В.В. Атака через «Internet», -СПб.: НПО Мир и семья, 1997. 95 с.
9. О противодействии распространению вредоносных программ (вирусов) и несанкционированных рекламных рассылок (спама). Меморандум Ассоциации Документальной электросвязи М., Ассоциация Документальной электросвязи, 2004. - 52 с.
10. Петренко С.А., Симонов С.В. Управление информационными рисками: экономическое оправдение безопасности. М.: АйТипресс, 2004. - 234 с.
11. Прикупец А.Л. Подход к оценке потерь фирмы от атак злоумышленника на ее данные в процессе передачи в распределенной базе данных. // Безопасность информационных технологий. М., 1998. - № 2. - С. 80-82
12. Руководящий документ. Концепция защиты средств вычислительной техники и автоматизированных систем от НСД к информации. Утв. Приказом Председателя Гостехкомиссии от 30.03.92. - М.: Гостехкомиссия России, 1992.- 9 с.
13. Слепов О.В., Отт А.Я. Контроль использования Интернет-ресурсов // Jetlnfo. М.: Джет Инфо Паблишер, 2005. - № 2. - 42 с.
14. Трифаленков И.А. Скрытые проблемы защиты СПД // Сети. М., 2001. - № 6. - С.9-26 с.
15. Трифаленков И.А. Критерии выбора средств защиты информации // 6-я Международная научно-практическая конференция «Защита информации в информационно-телекоммуникационных системах»: тезисы докладов. - Киев: Интерлинк, 2003. С.25-40.
16. Симонов С.В. Технологии и инструментарий управления рисками // Jetlnfo. -М.: Джет Инфо Паблишер, 2003. № 2. - 42 с.

## ЗАКЛЮЧЕНИЕ

Краткие выводы по результатам НИР или отдельных ее этапов

В ходе выполнения научно-исследовательской работы 1, были составлены: портфолио магистранта и индивидуальный план магистранта на все года обучения.

А также были подобраны и изучены учебная литература, справочники и нормативно-правовые документы по объекту исследования.

Оценка полноты решений поставленных задач.

В соответствии с учебно-методическим пособием о производственной практики «Научно-исследовательская работа» по направлению подготовки магистров, отчет по НИР 1 выполнен в полном объеме.

## СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ


1. Егоров А.Г. Правила оформления выпускных квалификационных работ по программам подготовки бакалавра и специалиста: учебно-методическое пособие / А.Г. Егоров, В.Г. Виткалов, Г.Н. Уполовникова, И.А. Живоглядова, Тольятти, 2012, - 135с.
2. Пудовкин А.П., Панасюк Ю.Н. Научно-исследовательская подготовка магистров техники и технологии: Методические указания. – Тамбов: Издательство ТГТУ, 2014. – 35 с.
3. Валиюллина А.А. Организация научно-исследовательской работы магистрантов: Методические указания. – Тюмень: РИО ФГБОУ ВПО «ТюмГАСУ», 2013. – 70 с.
4. Кузнецов И.Н. Научное исследование. Методика проведения и оформление: Учеб. пособие – М.: ИТК «Дашков и Ко», 2006. – 460 с.
5. Основы научных исследований : учебник для студ. учреждений высш. проф. образования / А.П.Болдин, В.А.Максимов. - М. : Издательский центр «Академия», 2012. - 336 с.
6. Черныш А.Я. Основы научных исследований: учебник / А.Я. Черныш, Е.Г. Анисимов, Н.П. Багмет, И.В. Глазунова, Т.Д. Михайленко. М.: Изд-во Российской таможенной академии, 2011. - 226 с.
7. ГОСТ 7.32-2001 "Межгосударственный стандарт. Система стандартов по информации, библиотечному и издательскому делу. Отчет о научно-исследовательской работе. Структура и правила оформления." (введен Постановлением Госстандарта России от 04.09.2001 N 367-ст) (ред. от 07.09.2005).