Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Новосибирский государственный технический университет»

Кафедра защиты информации

“УТВЕРЖДАЮ”
ДЕКАН АВТФ
к.т.н. Рева И. Л.
“___”_____ _____ г.

РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ
Основы информационной безопасности

Образовательная программа: 09.03.02 Информационные системы и технологии, профиль: Информационные системы в промышленности и бизнесе

Курс: 4, семестр : 8

Факультет автоматики и вычислительной техники

		Семестр
№	**Вид деятельности**	**8**
1	Всего зачетных единиц (кредитов)	3
2	Всего часов	108
3	Всего занятий в контактной форме, час.	37
4	Лекции, час.	14
5	Практические занятия, час.	0
6	Лабораторные занятия, час.	14
7	из них в активной и интерактивной форме, час.	12
8	Аттестация, час.	2
9	Консультации, час.	7
10	Самостоятельная работа, час.	71
11	Виды самостоятельной работы (курсовой проект, курсовая работа, РГЗ, подготовка к контрольной работе)	РГЗ
12	Вид аттестации	Э

Новосибирск 2017

Рабочая программа составлена на основании федерального государственного образовательного стандарта высшего образования по направлению (специальности): 09.03.02 Информационные системы и технологии

ФГОС введен в действие приказом №219 от 12.03.2015 г. , дата утверждения: 30.03.2015 г.

Место дисциплины в структуре учебного плана: Блок 1, вариативная, по выбору студента

Рабочая программа разработана на основе компетентностной модели выпускника по направлению (специальности): 09.03.02 Информационные системы и технологии

Рабочая программа обсуждена на заседании кафедры

ЗИ, протокол заседания кафедры №6 от 20.06.2017

Утверждена на совете факультета автоматики и вычислительной техники, протокол № 6 от 21.06.2017

Программу разработал:

доцент, к.т.н. Рева И. Л.

Заведующий кафедрой:

с.н.с., к.т.н. Трушин В. А.

Ответственный за образовательную программу:

профессор Гужов В. И.

1. Внешние требования

Таблица 1.1

***Компетенция ФГОС*: ОПК.4 пониманием сущности и значения информации в развитии современного информационного общества, соблюдение основных требований к информационной безопасности, в том числе защите государственной тайны; *в части следующих результатов обучения*:**
з1. Знать основные требований к информационной безопасности, в том числе защите государственной тайны
у1. Уметь реализовывать документы в соответствии с требованиями к информационной безопасности
***Компетенция ФГОС*: ПК.31 способность обеспечивать безопасность и целостность данных информационных систем и технологий; *в части следующих результатов обучения*:**
з1. Знать правила обеспечения безопасности данных информационных систем и технологий
у2. Уметь обеспечивать безопасность данных

2. Требования НГТУ к результатам освоения дисциплины

Таблица 2.1

Результаты изучения дисциплины по уровням освоения (иметь представление, знать, уметь, владеть)	Формы организации занятий
Основы информационной безопасности	
ОПК.4.з1 Знать основные требований к информационной безопасности, в том числе защите государственной тайны	
1.источники и классификацию угроз информационной безопасности;	Лекции; Самостоятельная работа
2.классифицировать и оценивать угрозы информационной безопасности для объекта информатизации;	Лекции; Лабораторные работы; Самостоятельная работа
3.автоматизированную систему как объект информационного воздействия, критерии оценки ее защищенности и методы обеспечения ее информационной безопасности;	Лекции; Самостоятельная работа
4.требования информационной безопасности;	Лабораторные работы; Самостоятельная работа
5.организовать эксплуатацию автоматизированной системы с учетом требований информационной безопасности;	Лекции; Лабораторные работы; Самостоятельная работа
6.обеспечить эффективное применение информационно-технологических ресурсов автоматизированной системы с учетом требований информационной безопасности;	Лекции; Лабораторные работы; Самостоятельная работа
ОПК.4.у1 Уметь реализовывать документы в соответствии с требованиями к информационной безопасности	
7.основы организационного и правового обеспечения информационной безопасности, основные нормативные правовые акты в области обеспечения информационной безопасности и нормативные методические документы ФСБ России и ФСТЭК России в области защиты информации;	Лекции; Лабораторные работы; Самостоятельная работа
8.применять правовые акты и нормативные методические документы в области обеспечения информационной безопасности;	Лекции
9.разрабатывать проекты нормативных и методических материалов, регламентирующих работу по обеспечению информационной безопасности автоматизированных систем, а также положений, инструкций и других организационно-распорядительных документов в сфере профессиональной деятельности	Лекции; Лабораторные работы; Самостоятельная работа
ПК.31.з1 Знать правила обеспечения безопасности данных информационных систем и технологий	
10.Знать правила обеспечения безопасности данных информационных систем и технологий	Лабораторные работы
ПК.31.у2 Уметь обеспечивать безопасность данных	
11.Уметь обеспечивать безопасность данных	Лабораторные работы

3. Содержание и структура учебной дисциплины

Таблица 3.1

Темы лекций	Активные формы, час.	Часы	Ссылки на результаты обучения	Учебная деятельность
Семестр: 8				
Дидактическая единица: Ключевые аспекты и вопросы формирования информационной безопасности современного предприятия				
1. Предпосылки становления предметной области информационной безопасности. Ключевые вопросы информационной безопасности	1	2	2, 7, 8	
2. Концепция информационной безопасности Российской Федерации. Разработка корпоративной концепции информационной безопасности	0	1	1, 2	
Дидактическая единица: Защищенная информационная система. Уровни и структура ИБ				
3. Виды защищаемой информации. Модель угроз и модель информационной безопасности	0	2	6, 9	
4. Организационно-распорядительные документы в сфере информационной безопасности. Политика информационной безопасности	0	2	1, 2	
Дидактическая единица: Модели и стандарты в сфере ИБ и управления рисками ИБ				
5. Управление информационными рисками	1	2	2, 3, 5, 7, 9	
6. Стандартизация в сфере информационной безопасности	0	2	2, 5, 6, 8	
Дидактическая единица: Технологии и методы реализации ИБ. Комплексная защита информационной инфраструктуры				
7. Криптографические методы защиты информации	0	1	5, 9	
8. Криптографические методы защиты информации	1	2	1, 7	

Таблица 3.2

Темы лабораторных работ	Активные формы, час.	Часы	Ссылки на результаты обучения	Учебная деятельность
Семестр: 8				
Дидактическая единица: Ключевые аспекты и вопросы формирования информационной безопасности современного предприятия				
1. Правовые аспекты информационной безопасности. Международное и российское законодательство в сфере информационной безопасности	2	3	2, 4, 5, 7	Изучение правовых аспектов информационной безопасности. Международное и российское законодательство в сфере информационной безопасности
Дидактическая единица: Защищенная информационная система. Уровни и структура ИБ				

2. Понятие защищенной информационной системы. Программа информационной безопасности	2	3	10, 5, 6	Понятие защищенной информационной системы. Программа информационной безопасности
Дидактическая единица: Модели и стандарты в сфере ИБ и управления рисками ИБ				
3. Математические модели систем и процессов защиты информации. Сервисы ИБ и защита от инсайдеров	2	4	5, 6, 9	Математические модели систем и процессов защиты информации. Сервисы ИБ и защита от инсайдеров
Дидактическая единица: Технологии и методы реализации ИБ. Комплексная защита информационной инфраструктуры				
4. Комплексная защита информационной инфраструктуры и ресурсов. Оценка эффективности СЗИ	3	4	10, 11, 4, 6	Комплексная защита информационной инфраструктуры и ресурсов. Оценка эффективности СЗИ

4. Самостоятельная работа обучающегося

№	Виды самостоятельной работы	Ссылки на результаты обучения	Часы на выполнение	Часы на консультации
Семестр: 8				
1	РГЗ	2, 4, 5, 7, 9	18	2
: Иванов А. В. Техническая защита информации [Электронный ресурс] : электронный учебно-методический комплекс / А. В. Иванов, В. А. Трушин, И. Л. Рева ; Новосиб. гос. техн. ун-т. - Новосибирск, [2014]. - Режим доступа: http://elibrary.nstu.ru/source?bib_id=vtls000208799. - Загл. с экрана.				
2	Подготовка к занятиям	1, 3	19	2
: Иванов А. В. Техническая защита информации [Электронный ресурс] : электронный учебно-методический комплекс / А. В. Иванов, В. А. Трушин, И. Л. Рева ; Новосиб. гос. техн. ун-т. - Новосибирск, [2014]. - Режим доступа: http://elibrary.nstu.ru/source?bib_id=vtls000208799. - Загл. с экрана.				
3	Дополнительная учебная деятельность	3, 4, 6	14	0
: Линник С. Е. Противодействия атакам на популярные сетевые сервисы : учебно-методическое пособие / С. Е. Линник, И. Л. Рева ; Новосиб. гос. техн. ун-т. - Новосибирск, 2015. - 55, [1] с. : ил., табл.. - Режим доступа: http://elibrary.nstu.ru/source?bib_id=vtls000222748				
4	Подготовка к аттестации	1, 2, 3, 4, 6, 7	20	3
: Туманов С. А. Система защиты информации от несанкционированного доступа на основе "DallasLock 8.0" : учебно-методическое пособие / С. А. Туманов, И. Л. Рева ; Новосиб. гос. техн. ун-т. - Новосибирск, 2016. - 54, [1] с. : ил.. - Режим доступа: http://elibrary.nstu.ru/source?bib_id=vtls000227592 Иванов А. В. Техническая защита информации [Электронный ресурс] : электронный учебно-методический комплекс / А. В. Иванов, В. А. Трушин, И. Л. Рева ; Новосиб. гос. техн. ун-т. - Новосибирск, [2014]. - Режим доступа: http://elibrary.nstu.ru/source?bib_id=vtls000208799. - Загл. с экрана.				

5. Технология обучения

Для организации и контроля самостоятельной работы обучающихся, а также проведения консультаций применяются информационно-коммуникационные технологии (табл. 5.1).

Таблица 5.1

Деятельность	Информационно-коммуникационные технологии
Информирование	e-mail; Социальные сети
Консультирование	e-mail
Контроль	Портал НГТУ

Размещение учебных материалов	Портал НГТУ

6. Правила аттестации обучающихся по учебной дисциплине

Для аттестации обучающихся по дисциплине используется балльно-рейтинговая система (БРС), позволяющая выставлять оценки по традиционной шкале и 15-уровневой ECTS. Краткая информация о БРС приведена в табл. 6.1.

Таблица 6.1

Оцениваемые виды деятельности обучающихся	**Максимальный балл**
Семестр: 8	
Лабораторная:	30
РГЗ:	30
Экзамен:	40
Контролирующие материалы - список вопросов	

В таблице 6.2 представлено соответствие форм контроля заявляемым требованиям к результатам освоения дисциплины.

Таблица 6.2

Коды компетенций ФГОС	**Результаты обучения**	**Формы контроля**	
		Защита РГЗ	**Экзамен**
ОПК.4	з1. Знать основные требований к информационной безопасности, в том числе защите государственной тайны	+	+
	у1. Уметь реализовывать документы в соответствии с требованиями к информационной безопасности	+	+
ПК.31	з1. Знать правила обеспечения безопасности данных информационных систем и технологий	+	+
	у2. Уметь обеспечивать безопасность данных		+

Фонд оценочных средств по дисциплине представлен в приложении № 1 к рабочей программе.

7. Литература

Основная литература

1. Галатенко В. А. Основы информационной безопасности. Курс лекций : учебное пособие для вузов / В. А. Галатенко ; под ред. В. Б. Бетелина ; Интернет ун-т информ. технологий. - М., 2004. - 260 с. : ил.

2. Гунько А. В. Безопасность информационных ресурсов [Электронный ресурс] : учебно-методический комплекс / А. В. Гунько ; Новосиб. гос. техн. ун-т. - Новосибирск, [2012]. - Режим доступа: http://elibrary.nstu.ru/source?bib_id=vtls000176306. - Загл. с экрана.

3. Громов Ю. Ю. Информационная безопасность : учеб / Ю. Ю. Громов. - Москва, 2014

4. Расторгуев С. П. Основы информационной безопасности : [учебное пособие для вузов по специальностям "Компьютерная безопасность" и др.] / С П Расторгуев. - Москва, 2009. - 186, [1] с. : ил.

Дополнительная литература

1. Платонов В. В. Программно-аппаратные средства обеспечения информационной безопасности вычислительных сетей : [учебное пособие для вузов] / В. В. Платонов. - М., 2006. - 238, [1] с. : ил., табл.

2. Загоскин В. В. Организационная защита информации : учебное пособие [по специальностям: 075300 - Организация и технология защиты информации и др.] / В. В. Загоскин, А. П. Бацула ; Том. гос. ун-т систем упр. и радиоэлектроники (ТУСУР), Каф. радиоэлектроники и защиты информации. - Томск, 2005. - 145 с. : ил.

3. Маршаков Д. В. Экспертные системы информационной безопасности : учебное пособие / Д. В. Маршаков, В. А. Фатхи ; Дон. гос. техн. ун-т. - Ростов-на-Дону, 2015. - 222 с. : ил., табл.

Интернет-ресурсы

1. ЭБС НГТУ : http://elibrary.nstu.ru/

2. ЭБС «Издательство Лань» : https://e.lanbook.com/

3. ЭБС IPRbooks : http://www.iprbookshop.ru/

4. ЭБС "Znanium.com" : http://znanium.com/

5. :

8. Методическое и программное обеспечение

8.1 Методическое обеспечение

1. Иванов А. В. Техническая защита информации [Электронный ресурс] : электронный учебно-методический комплекс / А. В. Иванов, В. А. Трушин, И. Л. Рева ; Новосиб. гос. техн. ун-т. - Новосибирск, [2014]. - Режим доступа: http://elibrary.nstu.ru/source?bib_id=vtls000208799. - Загл. с экрана.

2. Линник С. Е. Противодействия атакам на популярные сетевые сервисы : учебно-методическое пособие / С. Е. Линник, И. Л. Рева ; Новосиб. гос. техн. ун-т. - Новосибирск, 2015. - 55, [1] с. : ил., табл.. - Режим доступа: http://elibrary.nstu.ru/source?bib_id=vtls000222748

3. Туманов С. А. Система защиты информации от несанкционированного доступа на основе "DallasLock 8.0" : учебно-методическое пособие / С. А. Туманов, И. Л. Рева ; Новосиб. гос. техн. ун-т. - Новосибирск, 2016. - 54, [1] с. : ил.. - Режим доступа: http://elibrary.nstu.ru/source?bib_id=vtls000227592

8.2 Специализированное программное обеспечение

1 Microsoft Windows
2 Microsoft Office

9. Материально-техническое обеспечение

Компьютерный класс

№	Наименование	Назначение
1	Презентационное оборудование (мультимедиа-проектор, экран, компьютер для управления)	Визуальное сопровождение занятий
2	Компьютерный класс (Компьютеры объединены в локальную сеть с выходом в Internet)	Компьютеры объединены в локальную сеть с выходом в Internet

Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Новосибирский государственный технический университет»

Кафедра защиты информации

“УТВЕРЖДАЮ”
ДЕКАН АВТФ
к.т.н., доцент И.Л. Рева
“___”_____ _____ г.

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

УЧЕБНОЙ ДИСЦИПЛИНЫ

Основы информационной безопасности

Образовательная программа: 09.03.02 Информационные системы и технологии,
специализация: Информационные системы в промышленности и бизнесе

Новосибирск 2017

1. **Обобщенная структура фонда оценочных средств учебной дисциплины**
Обобщенная структура фонда оценочных средств по **дисциплине** «Основы информационной безопасности» приведена в Таблице.

Таблица

Формируемые компетенции	**Показатели сформированности компетенций (знания, умения, навыки)**	**Темы**	**Этапы оценки компетенций**	
			Мероприятия текущего контроля (курсовой проект, РГЗ(Р) и др.)	**Промежуточная аттестация (экзамен, зачет)**
ОПК.7 способность определять информационные ресурсы, подлежащие защите, угрозы безопасности информации и возможные пути их реализации на основе анализа структуры и содержания информационных процессов и особенностей функционирования объекта защиты	у1. уметь определять информационную инфраструктуру и информационные ресурсы организации, подлежащие защите	Классификация угроз информационной безопасности. Классификация источников угроз информационной безопасности. Государственная система правового обеспечения защиты информации в Российской Федерации Концепция информационной безопасности Российской Федерации. Определение информации. Виды защищаемой информации. Правовые аспекты информационной безопасности. Международное и российское законодательство в сфере информационной безопасности Причины, виды, каналы утечки. Оценка эффективности СЗИ. Методы и модели оценки уязвимости информации. Разработка "политики" информационной безопасности Угрозы нарушения конфиденциальности, целостности, доступности информации.	РГЗ	Зачет, вопросы: Понятие информационной безопасности. Национальная безопасность. Доктрина информационной безопасности Российской Федерации. Национальные интересы РФ в информационной сфере и их обеспечение. Виды угроз информационной безопасности РФ. Источники угроз информационной безопасности РФ. Угрозы конституционным правам и свободам человека. Угрозы информационному обеспечению государственной политики РФ. Состояние информационной безопасности РФ и основные задачи по ее обеспечению. Стратегические национальные приоритеты. Система обеспечения национальной безопасности. Силы обеспечения национальной безопасности. Средства обеспечения национальной безопасности. Правовая защита, виды права. Информация, виды

				собственной информации. Направления и цели защиты информации и их взаимосвязь. Угрозы информации. Виды угроз. Концептуальная модель безопасности продукции. Концептуальная модель безопасности личности. Концептуальная модель безопасности информации. Методы и модели оценки угроз информации. Организационная защита. Служба безопасности, структура и назначение. Физические средства защиты информации. Политика безопасности. Методики оценки уязвимостей и рисков.
ПК.10/ЭИ способность проводить анализ информационной безопасности объектов и систем на соответствие требованиям стандартов в области информационной безопасности	з2. знать требования стандартов в области информационной безопасности	Доктрина информационной безопасности Российской Федерации Методы и средства обеспечения информационной безопасности. Понятие информация и ее виды. Концептуальные модели безопасности. Правовые аспекты информационной безопасности. Международное и российское законодательство в сфере информационной безопасности Угрозы нарушения конфиденциальности, целостности, доступности информации.	Контрольная работа	Зачет, вопросы: Направления и цели защиты информации и их взаимосвязь. Угрозы информации. Виды угроз. Концептуальная модель безопасности продукции. Концептуальная модель безопасности личности. Концептуальная модель безопасности информации. Методы и модели оценки угроз информации.
ПК.7/ПТ способность проводить анализ исходных данных для проектирования подсистем и средств обеспечения информационной безопасности и участвовать в проведении технико-экономического обоснования соответствующих проектных решений	з1. знать методы анализа инфраструктуры информационной системы и ее безопасности	Классификация угроз информационной безопасности. Классификация источников угроз информационной безопасности. Государственная система правового обеспечения защиты информации в Российской Федерации Доктрина информационной безопасности Российской Федерации Информация как объект юридической защиты Методы и средства обеспечения информационной безопасности. Определение информации. Виды защищаемой информации. Понятие информация и ее виды. Концептуальные модели безопасности. Разработка "политики" информационной безопасности	РГЗ	Зачет, вопросы: Угрозы информации. Виды угроз. Концептуальная модель безопасности продукции. Концептуальная модель безопасности личности. Концептуальная модель безопасности информации. Методы и модели оценки угроз информации. Организационная защита. Служба безопасности, структура и назначение. Физические средства защиты информации. Политика безопасности. Методики оценки уязвимостей и рисков.

2. Методика оценки этапов формирования компетенций в рамках дисциплины.

Промежуточная аттестация по **дисциплине** проводится в 8 семестре - в форме дифференцированного зачета, который направлен на оценку сформированности компетенций ОПК.7, ПК.10/ЭИ, ПК.7/ПТ.

Зачет проводится в устной (письменной) форме, по билетам.

Кроме того, сформированность компетенций проверяется при проведении мероприятий текущего контроля, указанных в таблице раздела 1.

В 3 семестре обязательным этапом текущей аттестации являются расчетно-графическое задание (работа) (РГЗ(Р)), контрольная работа. Требования к выполнению РГЗ(Р), контрольной работы, состав и правила оценки сформулированы в паспорте РГЗ(Р), контрольной работы.

Общие правила выставления оценки по дисциплине определяются балльно-рейтинговой системой, приведенной в рабочей программе учебной дисциплины.

На основании приведенных далее критериев можно сделать общий вывод о сформированности компетенций ОПК.7, ПК.10/ЭИ, ПК.7/ПТ, за которые отвечает дисциплина, на разных уровнях.

Общая характеристика уровней освоения компетенций.

Ниже порогового. Уровень выполнения работ не отвечает большинству основных требований, теоретическое содержание курса освоено частично, пробелы могут носить существенный характер, необходимые практические навыки работы с освоенным материалом сформированы не достаточно, большинство предусмотренных программой обучения учебных заданий не выполнены или выполнены с существенными ошибками.

Пороговый. Уровень выполнения работ отвечает большинству основных требований, теоретическое содержание курса освоено частично, но пробелы не носят существенного характера, необходимые практические навыки работы с освоенным материалом в основном сформированы, большинство предусмотренных программой обучения учебных заданий выполнено, некоторые виды заданий выполнены с ошибками.

Базовый. Уровень выполнения работ отвечает всем основным требованиям, теоретическое содержание курса освоено полностью, без пробелов, некоторые практические навыки работы с освоенным материалом сформированы недостаточно, все предусмотренные программой обучения учебные задания выполнены, качество выполнения ни одного из них не оценено минимальным числом баллов, некоторые из выполненных заданий, возможно, содержат ошибки.

Продвинутый. Уровень выполнения работ отвечает всем требованиям, теоретическое содержание курса освоено полностью, без пробелов, необходимые практические навыки работы с освоенным материалом сформированы, все предусмотренные программой обучения учебные задания выполнены, качество их выполнения оценено числом баллов, близким к максимальному.

Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Новосибирский государственный технический университет»
Кафедра защиты информации

Паспорт зачета

по дисциплине «Основы информационной безопасности», 8 семестр

1. Методика оценки

Зачет проводится в устной (письменной) форме, по билетам. Билет формируется по следующему правилу: первый вопрос выбирается из диапазона вопросов ОПК.7, второй вопрос из диапазона вопросов ПК.10/ЭИ, ПК.7/ПТ (список вопросов приведен ниже). В ходе экзамена преподаватель вправе задавать студенту дополнительные вопросы из общего перечня (п. 4).

Форма билета для зачета

НОВОСИБИРСКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ
Факультет АВТФ

Билет № _____
к зачету по дисциплине «Основы информационной безопасности»

1. Вопрос 1
2. Вопрос 2.

Утверждаю: зав. кафедрой ____ _____ должность, ФИО
(подпись)
(дата)

2. Критерии оценки

- Ответ на билет (тест) для зачета считается **неудовлетворительным**, если студент при ответе на вопросы не дает определений основных понятий, не способен показать причинно-следственные связи явлений, при решении задачи допускает принципиальные ошибки, оценка составляет *0 баллов.*
- Ответ на билет (тест) для зачета засчитывается на **пороговом** уровне, если студент при ответе на вопросы дает определение основных понятий, может показать причинно-следственные связи явлений, при решении задачи допускает непринципиальные ошибки, например, вычислительные, оценка составляет *35 баллов.*
- Ответ на билет (тест) для зачета билет засчитывается на **базовом** уровне, если студент

при ответе на вопросы формулирует основные понятия, законы, дает характеристику процессов, явлений, проводит анализ причин, условий, может представить качественные характеристики процессов, не допускает ошибок при решении задачи, оценка составляет *40 баллов.*

- Ответ на билет (тест) для зачета билет засчитывается на **продвинутом** уровне, если студент при ответе на вопросы проводит сравнительный анализ подходов, проводит комплексный анализ, выявляет проблемы, предлагает механизмы решения, способен представить количественные характеристики определенных процессов, приводит конкретные примеры из практики, не допускает ошибок и способен обосновать выбор метода решения задачи, оценка составляет 45 *баллов.*

3. Шкала оценки

Зачет считается сданным, если сумма баллов по всем заданиям билета оставляет не менее 35 баллов (из 45 возможных).

В общей оценке по дисциплине баллы за зачет учитываются в соответствии с правилами балльно-рейтинговой системы, приведенными в рабочей программе дисциплины.

4. **Вопросы к** зачету **по дисциплине «**Основы информационной безопасности**»**

1. Понятие информационной безопасности.
2. Национальная безопасность.
3. Доктрина информационной безопасности Российской Федерации.
4. Национальные интересы РФ в информационной сфере и их обеспечение.
5. Виды угроз информационной безопасности РФ.
6. Источники угроз информационной безопасности РФ.
7. Угрозы конституционным правам и свободам человека.
8. Угрозы информационному обеспечению государственной политики РФ.
9. Состояние информационной безопасности РФ и основные задачи по ее обеспечению.
10. Стратегические национальные приоритеты.
11. Система обеспечения национальной безопасности.
12. Силы обеспечения национальной безопасности.
13. Средства обеспечения национальной безопасности.
14. Правовая защита, виды права.
15. Информация, виды собственной информации.
16. Направления и цели защиты информации и их взаимосвязь.
17. Угрозы информации.
18. Виды угроз.
19. Концептуальная модель безопасности продукции.
20. Концептуальная модель безопасности личности.
21. Концептуальная модель безопасности информации.
22. Методы и модели оценки угроз информации.
23. Организационная защита.
24. Служба безопасности, структура и назначение.
25. Физические средства защиты информации.

26. Политика безопасности.
27. Методики оценки уязвимостей и рисков.

Билет №1

Понятие информационной безопасности.
Угрозы информации.

Билет №2

Доктрина информационной безопасности Российской Федерации.
Виды угроз.

Билет №3

Виды угроз информационной безопасности РФ.
Концептуальная модель безопасности информации.

Билет №4

Угрозы конституционным правам и свободам человека.
Методы и модели оценки угроз информации.

Билет №5

Стратегические национальные приоритеты.
Физические средства защиты информации.

Билет №6

Силы обеспечения национальной безопасности.
Методики оценки уязвимостей и рисков.
Билет №7

Средства обеспечения национальной безопасности.
Концептуальная модель безопасности продукции.
Билет №8

Правовая защита, виды права.
Информация, виды собственной информации.
Билет №9

Национальная безопасность.
Направления и цели защиты информации и их взаимосвязь.

Билет №10

Концептуальная модель безопасности продукции.
Национальные интересы РФ в информационной сфере и их обеспечение.
Билет №11

Концептуальная модель безопасности личности.
Источники угроз информационной безопасности РФ.

Билет №12

Организационная защита.
Угрозы информационному обеспечению государственной политики РФ.

Билет №13

Состояние информационной безопасности РФ и основные задачи по ее обеспечению.
Служба безопасности, структура и назначение.

Билет №14

Политика безопасности.
Система обеспечения национальной безопасности.

Билет №15

Понятие информационной безопасности.
Угрозы информации.

Билет №16

Доктрина информационной безопасности Российской Федерации.
Виды угроз.

Билет №17

Виды угроз информационной безопасности РФ.
Концептуальная модель безопасности информации.

Билет №18

Угрозы конституционным правам и свободам человека.
Методы и модели оценки угроз информации.

Билет №19

Стратегические национальные приоритеты.
Физические средства защиты информации.

Билет №20

Силы обеспечения национальной безопасности.
Методики оценки уязвимостей и рисков.
Билет №21

Средства обеспечения национальной безопасности.
Концептуальная модель безопасности продукции.

Билет №22

Правовая защита, виды права.
Информация, виды собственной информации.
Билет №23

Национальная безопасность.
Направления и цели защиты информации и их взаимосвязь.

Билет №24

Концептуальная модель безопасности продукции.
Национальные интересы РФ в информационной сфере и их обеспечение.
Билет №25

Концептуальная модель безопасности личности.
Источники угроз информационной безопасности РФ.

Билет №26

Организационная защита.
Угрозы информационному обеспечению государственной политики РФ.

Билет №27

Состояние информационной безопасности РФ и основные задачи по ее обеспечению.
Служба безопасности, структура и назначение.

Билет №28

Политика безопасности.
Система обеспечения национальной безопасности.

Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Новосибирский государственный технический университет»
Кафедра защиты информации

Паспорт
расчетно-графического задания (работы)

по дисциплине «Основы информационной безопасности», 8 семестр

1. Методика оценки

В рамках расчетно-графического задания (работы) по дисциплине студенты должны провести анализ предоставленного (выбранного самостоятельно) объекта информатизации, малого предприятия и.т.д., провести оценку рисков и анализ угроз информационной безопасности, обосновать результаты расчетов, предоставить способы устранения выявленных угроз безопасности.

Обязательные структурные части РГЗ.

1) Анализ объекта;
2) Оценка рисков;
3) Анализ угроз;
4) Предложение способов защиты;

Оцениваемые позиции:

2. Критерии оценки

- Работа считается **не выполненной,** если выполнены не все части РГЗ(Р), отсутствует анализ объекта, нет соответствия требованиям к работе, оценка составляет 0 баллов.
- Работа считается выполненной **на пороговом** уровне, если части РГЗ(Р) выполнены формально: анализ объекта проведен куце, недостаточно обоснованы результаты, оценка составляет 15 – 20 баллов.
- Работа считается выполненной **на базовом** уровне, если анализ объекта выполнен в полном объеме, достаточно обоснованы результаты расчетов, проведен анализ и оценка рисков, не представлены способы устранения недостатков, оценка составляет 20 - 25 баллов.
- Работа считается выполненной **на продвинутом** уровне, если анализ объекта выполнен в полном объеме, достаточно обоснованы результаты расчетов, проведен анализ и оценка рисков, представлены способы устранения выявленных недостатков, оценка составляет 25- 30 баллов.

3. Шкала оценки

В общей оценке по дисциплине баллы за РГЗ(Р) учитываются в соответствии с правилами балльно-рейтинговой системы, приведенными в рабочей программе дисциплины.

4. Примерный перечень тем РГЗ(Р)

1. Для предприятия малого бизнеса провести:

- Анализ объекта,
- Оценка рисков;
- Анализ угроз;
- Предложение по введению способов и средств защиты;

5. Пример выполнения РГЗ

Оценка рисков и анализ угроз ИБ предприятия:

Специалистами фирмы IBM[2] предложена следующая эмпирическая зависимость ожидаемых потерь от i-ой угрозы информации:

$$Ri=10(Si+Vi-4),$$

где Si – коэффициент, характеризующий возможную частоту возникновения существующей угрозы; Vi – коэффициент, характеризующий значение возможного ущерба при её возникновении. Предложенные специалистами значения коэффициентов следующие:

Таблица 9 - Значения коэффициента Si для расчёта зависимости ожидаемых потерь

Ожидаемая (возможная) частота появления угрозы	Предполагаемое значение Si
Почти никогда	0
1 раз в 1000 лет	1
1 раз в 100 лет	2
1 раз в 10 лет	3
1 раз в год	4
1 раз в месяц (примерно, 10 раз в год)	5
1-2 раза в неделю (примерно, 100 раз в год)	6
3 раза в день (1000 раз в год)	7

Таблица 10 - Возможные значения коэффициента Vi для расчёта зависимости ожидаемых потерь

Значения возможного ущерба при проявлении угрозы, долл.	Предполагаемое значение Vi
1	0
10	1
100	2
1000	3
10000	4

100000	5
1000000	6
10000000	7

Суммарная стоимость потерь определяется формулой:

$$R = \sum_{\forall i} R_i .$$

На основании предложенной эмпирической формулы рассчитаем число ожидаемых потерь для незащищённой, частично-защищённой и защищённой систем, где незащищённая система – система, не содержащая средств защиты от НСД; частично-защищённая система- имеются средства антивирусной защиты и установлены пароли на вход в систему); защищённая система – система, где установлены средства защиты, перекрывающие возможные каналы утечки информации с некоторым запасом прочности.

Незащищённая система:

1. Потери от компьютерных вирусов

В данной системе средства вычислительной техники заражаются компьютерными вирусами в среднем 1-2 раза в неделю, и при этом организации наносится ущерб, равный в среднем 1000$. На основании вышеприведённых таблиц

Ri=10(6+3-4) =105=100000$.

2. Потери от взлома пароля (пароль 4 символа, используются 70 знаков).

Взлом происходит в среднем 3 раза в день, ущерб составляет 100$.

Ri=10(7+2-4) =105=100000$.

3. Потери от взлома криптографической защиты.

Взлом происходит в среднем один раз в месяц, ущерб составляет 10000$.

Ri=10(5+4-4) =105=100000$.

4. Потери от DOS-атак (сбой или отказ ИС).

Атаки происходят в среднем 1 раз в месяц, ущерб составляет 100$.

Ri=10(5+2-4)=103=1000$.

5. Потери от троянских программ.

Атаки происходят в среднем 1 раз в месяц, ущерб составляет 100$.

Ri=10(5+2-4)=103=1000$.

6. Потери от логических бомб.

Атаки происходят в среднем 1 раз в месяц, ущерб составляет 10$.

Ri=10(5+1-4)=102=100$.

7. Потери от перехвата информации (подключение к сети).

Несанкционированное подключение происходит 1-2 раза в неделю, ущерб составляет 10$.

Ri=10(6+1-4)=103=1000$.

8. Потери от срыва связи.

Срыв связи в результате действий злоумышленника происходит примерно 1 раз в месяц, ущерб составляет 10$.

Ri=10(5+1-4)=102=100$.

9. Потери от перехвата злоумышленником ПЭМИН.

Примерно 1 раз в 10 лет, ущерб составляет 1000$.

Ri=10(3+3-4)=102=100$.

Суммарная стоимость потерь незащищённой системы будет равна:

$$R = \sum_{\forall i} R_i = 303300\$$$

.

Частично защищённая система (уже существующая):

1. Потери от компьютерных вирусов.

В данной системе при использовании антивирусного средства, средства вычислительной техники заражаются компьютерными вирусами в среднем 1 раз в месяц, и при этом организации наносится ущерб, равный в среднем 1000$. На основании вышеприведённых таблиц

Ri=10(5+3-4)=104=10000$.

2. Потери от взлома пароля (пароль 7 символов, используется 70 знаков).

При использовании пароля в 7 символов, вероятность подбора пароля составит 1 раз в месяц, ущерб составляет 100$.

Ri=10(5+2-4)=103=1000$.

Остальные элементы, подлежащие защите аналогичны защищённой системе.

Суммарная стоимость потерь частично защищённой системы будет

$$R = \sum_{\forall i} R_i = 12140\$$$

.

Защищённая система:

1. Потери от компьютерных вирусов.

В данной системе при использовании антивирусного средства, средства вычислительной техники заражаются компьютерными вирусами в среднем 1 раз в год, и при этом организации наносится ущерб, равный в среднем 1000$. На основании вышеприведённых таблиц

Ri=10(4+3-4)=103=1000$.

2. Потери от взлома пароля (пароль 8 символов, используются 70 знаков).

При использовании различного рода биометрических датчиков и цифровых ключей, вероятность подбора пароля составит 1 раз в 100 лет, ущерб составляет 100$.

Ri=10(2+3-4) =101=10$.

3. Потери от взлома криптографической защиты.

При использовании средств криптографической защиты, вероятность взлома составит в среднем 1 раз в 10 лет, ущерб составляет 10000$.

Ri=10(3+4-4) =103=1000$.

4. Потери от DOS-атак (сбой или отказ ИС).

При использовании firewalla атаки происходят в среднем 1 раз в 10 лет, ущерб составляет 100$.

Ri=10(3+2-4)=101=10$.

5. Потери от троянских программ.

При использовании средств антивирусной защиты, атаки происходят в среднем 1 раз в год, ущерб составляет 100$.

Ri=10(4+2-4)=102=100$.

6. Потери от логических бомб.

При использовании средств антивирусной защиты, атаки происходят в среднем 1 раз в год, ущерб составляет 10$.

Ri=10(4+1-4)=101=10$.

7. Потери от перехвата информации (подключение к сети).

При использовании VPN, несанкционированное подключение происходит 1 раз в год, ущерб составляет 10$.

Ri=10(4+1-4)=101=10$.

8. Потери от срыва связи.

При использовании firewalla и административных мер, срыв связи в результате действий злоумышленника происходит примерно 1 раз в год, ущерб составляет 10$.

Ri=10(4+1-4)=101=10$.

Суммарная стоимость потерь защищённой системы будет равна:

$$R = \sum_{\forall i} R_i = 2150\$$$.

Эквивалентный выигрыш средств от установки дополнительных СЗИ в незащищенной сети составляет:

$$\Delta = 303300 - 2150 = 301150\$$$.

Эквивалентный выигрыш средств от установки дополнительных СЗИ частично защищенной сети составляет:

$$\Delta = 12140 - 2150 = 9990\$$$.

Анализ риска завершается составлением и принятием ПБ. Она оформляется в виде документа, в общем виде (без излишней детализации) определяющего задачи в области защиты и особенности процесса защиты ресурсов. ПБ определяет стратегию и тактику построения системы безопасности компании. В российской терминологии документ, определяющий стратегию, называют концепцией, а документ, определяющий тактику, - политикой. На Западе принято создавать единый документ, включающий в себя оба аспекта.

ПБ отражает причины, по которым организация использует подключение к открытой, общедоступной сети, и определяет перечень сервисов, предоставляемых всем внутренним и внешним пользователям внутри и вне интранета организации.

На втором этапе с учетом составленной ПБ и согласно полученным решениям составляется план обеспечения ИБ (иногда он называется планом защиты) - официальный документ, описывающий конкретные действия по реализации средств поддержания безопасности системы, который регулярно пересматривается и при необходимости корректируется.

План защиты содержит следующие разделы.

1. Текущее состояние - описание существующей на момент подготовки плана системы защиты.

2. Рекомендации - выбор основных мер, средств и способов защиты, реализующих ПБ для интранета. Будем называть этот комплекс мер системой безопасности. Здесь очень важно установить компромисс между ее ценой и удобством использования. В зависимости от желаемого уровня безопасности и выбранного способа защиты интранета могут потребоваться дополнительные аппаратные средства: маршрутизаторы и выделенные хосты, специальное ПО, а также ставка эксперта по безопасности. Что и составляет

максимальную сумму на установку дополнительных СЗИ.

Для примера рассмотрим, общую стоимость защиты для ОИ, применительно к учебному городку №1 ВАИУ (г. Воронеж).

Для организации защищенного ОИ в качестве системы защиты информации выберем Secret Net v. 4.0 стоимостью 980$. Также необходимо выбрать межсетевой экран Symantec Client Security 3.1 СТОИМОСТЬЮ 57$

Для защиты серверов от вирусных программ применяем программу Dr. Web для Windows - Антивирус +Антиспам стоимостью 166 $.

Для предотвращения от взлома криптографической защиты серверов служб применим средство криптозащиты "УКДС-С" стоимостью 740 $.

Средства VPN для защиты системы от несанкционированного подключения устанавливать не будем в связи с их дороговизной (более 2000$ за 1 комплект) и тем, что межсетевые экраны реализуют большинство способов зашиты, реализуемых в VPN путем специальных настроек.

Суммарная стоимость средств защиты ОИ составляет:

$$\sum = 980 + 57 + 166 + 740 = 1061\$$$

3. Ответственность - список ответственных сотрудников и разграничение сфер их деятельности.

4. Расписание - определение порядка работы механизмов защиты, в том числе и средств контроля.

5. Пересмотр положений плана защиты с указанием периода пересмотра.