ФГБОУ ВО «БАШКИРСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»
ИНСТИТУТ ИСТОРИИ И ГОСУДАРСТВЕННОГО УПРАВЛЕНИЯ

Утверждено:
на заседании кафедры
протокол № 8 от «24» февраля 2021 г.

Зав. кафедрой /Исмагилова А.С.

Согласовано:
Председатель УМК института

/Гильмутдинова Р.А.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Дисциплина
Экономика защиты информации

Обязательная часть (Б1.О.34)

программа специалитета

Специальность
10.05.05 Безопасность информационных технологий в правоохранительной сфере

Специализация
«Организация и технологии защиты информации (по отраслям)»

Квалификация
специалист по защите информации

Разработчик (составитель) доцент кафедры, к.филос.н.	Миронова Н.Г.

Для приема: 2021 г.

Уфа 2021 г.

Составитель: к.филос.н. Миронова Наталия Геннадьевна

Рабочая программа дисциплины *утверждена* на заседании кафедры протокол от «24» февраля 2021 № 8

Дополнения и изменения, внесенные в рабочую программу дисциплины, утверждены на заседании
кафедры_____
_____
_____,
протокол № ____ от «____» _____ 20 _ г.

Заведующий кафедрой / Исмагилова А.С. /

Дополнения и изменения, внесенные в рабочую программу дисциплины, утверждены на заседании
кафедры_____
_____
_____,
протокол № ____ от «____» _____ 20 _ г.

Заведующий кафедрой _____/ Исмагилова А.С. /

Дополнения и изменения, внесенные в рабочую программу дисциплины, утверждены на заседании кафедры
_____
_____
_____,
протокол № ____ от «____» _____ 20 _ г.

Заведующий кафедрой _____/ _____Ф.И.О./

Дополнения и изменения, внесенные в рабочую программу дисциплины, утверждены на заседании кафедры
_____
_____
_____,
протокол № ____ от «____» _____ 20 _ г.

Заведующий кафедрой _____/ _____Ф.И.О./

Список документов и материалов

1. Перечень планируемых результатов обучения по дисциплине, соотнесенных с установленными в образовательной программе индикаторами достижения компетенций

По итогам освоения дисциплины обучающийся должен достичь следующих результатов обучения:

Категория (группа) компетенций (при наличии ОПК)	**Формируемая компетенция (с указанием кода)**	**Код и наименование индикатора достижения компетенции**	**Результаты обучения по дисциплине**
Экономическая культура, в т.ч. финансовая грамотность	УК-9 Способен принимать обоснованные экономические решения в различных областях жизнедеятельности;	УК-9-1. Знает экономические и социальные условия и последствия реализации профессиональных решений.	Знать экономические и социальные условия и последствия реализации профессиональных решений.
		УК-9-2. Знает принципы и методы экономических наук для решения профессиональных задач.	Знать принципы и методы экономических наук для решения профессиональных задач
		УК-9.3. Умеет оценивать эффективность управленческих решений и анализировать экономические показатели деятельности подразделения; находить информацию по тематике и выбирать информационные ресурсы и источники знаний в электронной среде; оценивать стоимость владения подсистемой информационной безопасности.	Уметь управленческих решений и анализировать экономические показатели деятельности подразделения; находить информацию по тематике и выбирать информационные ресурсы и источники знаний в электронной среде; оценивать стоимость владения подсистемой информационной безопасности.
		УК-9.4. Владеет навыками принятия обоснованных различными методами и подходами экономических решений в различных областях жизнедеятельности.	Владеть навыками принятия обоснованных различными методами и подходами экономических решений в различных областях жизнедеятельности.
Проектно-технологические	ОПК-4 Способен выполнять технико-экономическое обоснование проектных решений по созданию систем обеспечения информационной безопасности, разрабатывать рабочую техническую документацию в соответствии с действующими нормативными и методическими	ОПК-4.1. Знает подходы к обоснованию затрат на информационную безопасность, методы и модели установления зависимости между затратами на защиту информации и уровнем защищенности.	Знать подходы к обоснованию затрат на информационную безопасность, методы и модели установления зависимости между затратами на защиту информации и уровнем защищенности.
		ОПК-4.2. Умеет оценивать эффективность проектных решений по разработке систем обеспечения информационной	Уметь оценивать эффективность проектных решений по разработке систем обеспечения информационной

	документами в области защиты информации	безопасности документацию в соответствии с действующими нормативными и методическими документами в области защиты информации	безопасности документацию в соответствии с действующими нормативными и методическими документами в области защиты информации
		ОПК-4.3. Умеет разрабатывать проектную документацию, анализируя экономические показатели проекта;	Уметь разрабатывать проектную документацию, анализируя экономические показатели проекта;
		ОПК-4.4. Умеет пользоваться методиками оценки стоимости владения для подсистемы информационной безопасности, определять зависимость между затратами на ИБ и уровнем защищенности, определять зависимость между затратами и уровнем защищенности и эффективности в проектах по информационной безопасности.	Уметь пользоваться методиками оценки стоимости владения для подсистемы информационной безопасности, определять зависимость между затратами на ИБ и уровнем защищенности, определять зависимость между затратами и уровнем защищенности и эффективности в проектах по информационной безопасности.
		ОПК-4.5. Владеет навыками оценки и обоснования затрат на ИБ, навыками обоснования проектных решений по созданию систем обеспечения безопасности информации, навыками разработки рабочей технической документации в соответствии с действующими нормативными и методическими документами в области защиты информации.	Владеть навыками оценки и обоснования затрат на ИБ, навыками обоснования проектных решений по созданию систем обеспечения безопасности информации, навыками разработки рабочей технической документации в соответствии с действующими нормативными и методическими документами в области защиты информации.

2. Цель и место дисциплины в структуре образовательной программы

Дисциплина «Экономика защиты информации» относится к обязательной части.

Дисциплина изучается на 5 курсе в 9 семестре.

Цели изучения дисциплины: формирование знаний и навыков применения методик экономической оценки стоимости владения СЗИ, умения определять зависимость и баланс между затратами на информационную безопасность и уровнем защищенности, оценивать риски ИБ, оценивать экономическую эффективность системы защиты информации.

3. Содержание рабочей программы (объем дисциплины, типы и виды учебных занятий, учебно-методическое обеспечение самостоятельной работы обучающихся)

Содержание рабочей программы представлено в Приложении № 1.

4. Фонд оценочных средств по дисциплине

4.1. Перечень компетенций и индикаторов достижения компетенций с указанием соотнесенных с ними запланированных результатов обучения по дисциплине. Описание критериев и шкал оценивания результатов обучения по дисциплине.

УК-9. Способен принимать обоснованные экономические решения в различных областях жизнедеятельности.

Код и наименование индикатора достижения компетенции	**Результаты обучения по дисциплине**	Критерии оценивания результатов обучения	
		зачтено	Не зачтено
УК-9-1. Знает экономические и социальные условия и последствия реализации профессиональных решений.	Знать экономические и социальные условия и последствия реализации профессиональных решений.	Не знает	Демонстрирует хорошее знание указанных понятий, способов и принципов, способен увязать их с практикой управления службой защиты информации.
УК-9-2. Знает принципы и методы экономических наук для решения профессиональных задач.	Знать принципы и методы экономических наук для решения профессиональных задач	Не знает или показывает очень слабые знания	Демонстрирует хорошее знание указанных понятий, способов и принципов, способен увязать их с практикой управления службой защиты информации.
УК-9.3. Умеет оценивать эффективность управленческих решений и анализировать экономические показатели деятельности подразделения; находить информацию по тематике и выбирать информационные ресурсы и источники знаний в электронной среде; оценивать стоимость владения подсистемой информационной безопасности.	Уметь управленческих решений и анализировать экономические показатели деятельности подразделения; находить информацию по тематике и выбирать информационные ресурсы и источники знаний в электронной среде; оценивать стоимость владения подсистемой информационной безопасности.	Не умеет или показывает очень слабые навыки	Демонстрирует хорошее теоретическое знание компетенции, владение практической стороной при решении задач организации службы защиты информации.
УК-9.4. Владеет навыками принятия обоснованных различными методами и подходами экономических решений в различных областях жизнедеятельности.	Владеть навыками принятия обоснованных различными методами и подходами экономических решений в различных областях жизнедеятельности.	Не владеет или показывает очень слабые навыки	Демонстрирует хорошее владение компетенцией

ОПК-4. Способен выполнять технико-экономическое обоснование проектных решений по созданию систем обеспечения информационной безопасности, разрабатывать рабочую

техническую документацию в соответствии с действующими нормативными и методическими документами в области защиты информации.

Код и наименование индикатора достижения компетенции	**Результаты обучения по дисциплине**	Критерии оценивания результатов обучения	
		Не знает	Демонстрирует хорошее знание указанных понятий, способов и принципов, способен увязать их с практикой управления службой защиты информации.
ОПК-4.1. Знает подходы к обоснованию затрат на информационную безопасность, методы и модели установления зависимости между затратами на защиту информации и уровнем защищенности.	Знать подходы к обоснованию затрат на информационную безопасность, методы и модели установления зависимости между затратами на защиту информации и уровнем защищенности.	Не знает или показывает очень слабые знания	Демонстрирует хорошее знание указанных понятий, способов и принципов, способен увязать их с практикой управления службой защиты информации.
ОПК-4.2. Умеет оценивать эффективность проектных решений по разработке систем обеспечения информационной безопасности документацию в соответствии с действующими нормативными и методическими документами в области защиты информации	Уметь оценивать эффективность проектных решений по разработке систем обеспечения информационной безопасности документацию в соответствии с действующими нормативными и методическими документами в области защиты информации	Не умеет или показывает очень слабые навыки	Демонстрирует хорошее теоретическое знание компетенции, владение практической стороной при решении задач организации службы защиты информации.
ОПК-4.3. Умеет разрабатывать проектную документацию, анализируя экономические показатели проекта;	Уметь разрабатывать проектную документацию, анализируя экономические показатели проекта;	Не умеет или показывает очень слабые навыки	Демонстрирует хорошее теоретическое знание компетенции, владение практической стороной при решении задач организации службы защиты информации.
ОПК-4.4. Умеет пользоваться методиками оценки стоимости владения для подсистемы информационной безопасности, определять зависимость между затратами на ИБ и уровнем защищенности, определять зависимость между затратами и уровнем защищенности и эффективности в проектах по информационной безопасности.	Уметь пользоваться методиками оценки стоимости владения для подсистемы информационной безопасности, определять зависимость между затратами на ИБ и уровнем защищенности, определять зависимость между затратами и уровнем защищенности и эффективности в проектах по информационной безопасности.	Не умеет или показывает очень слабые навыки	Демонстрирует хорошее теоретическое знание компетенции, владение практической стороной при решении задач организации службы защиты информации.
ОПК-4.5. Владеет навыками оценки и обоснования затрат на ИБ, навыками	Владеть навыками оценки и обоснования затрат на ИБ, навыками обоснования проектных решений по	Не владеет или показывает	Демонстрирует хорошее владение компетенцией

обоснования проектных решений по созданию систем обеспечения безопасности информации, навыками разработки рабочей технической документации в соответствии с действующими нормативными и методическими документами в области защиты информации.	созданию систем обеспечения безопасности информации, навыками разработки рабочей технической документации в соответствии с действующими нормативными и методическими документами в области защиты информации.	очень слабые навыки	

4.2. Типовые контрольные задания или иные материалы, необходимые для оценивания результатов обучения по дисциплине, соотнесенных с установленными в образовательной программе индикаторами достижения компетенций. Методические материалы, определяющие процедуры оценивания результатов обучения по дисциплине

УК-9. Способен принимать обоснованные экономические решения в различных областях жизнедеятельности.

Код и наименование индикатора достижения компетенции	Результаты обучения по дисциплине	Оценочные средства
УК-9-1. Знает экономические и социальные условия и последствия реализации профессиональных решений.	Знать экономические и социальные условия и последствия реализации профессиональных решений.	практическое задание; опрос, компьютерный тест
УК-9-2. Знает принципы и методы экономических наук для решения профессиональных задач.	Знать принципы и методы экономических наук для решения профессиональных задач	практическое задание; ролевая/деловая игра; опрос
УК-9.3. Умеет оценивать эффективность управленческих решений и анализировать экономические показатели деятельности подразделения; находить информацию по тематике и выбирать информационные ресурсы и источники знаний в электронной среде; оценивать стоимость владения подсистемой информационной безопасности.	Уметь управленческих решений и анализировать экономические показатели деятельности подразделения; находить информацию по тематике и выбирать информационные ресурсы и источники знаний в электронной среде; оценивать стоимость владения подсистемой информационной безопасности.	практическое задание; ролевая/деловая игра; опрос; отчет (по практическим занятиям, контрольной СР)
УК-9.4. Владеет навыками принятия обоснованных различными методами и подходами экономических решений в различных	Владеть навыками принятия обоснованных различными методами и подходами экономических решений в	практическое задание; ролевая/деловая игра; опрос; отчет (по практическим занятиям, контрольной СР)

областях жизнедеятельности.	различных областях жизнедеятельности.	

ОПК-4. Способен выполнять технико-экономическое обоснование проектных решений по созданию систем обеспечения информационной безопасности, разрабатывать рабочую техническую документацию в соответствии с действующими нормативными и методическими документами в области защиты информации.

Код и наименование индикатора достижения компетенции	**Результаты обучения по дисциплине**	**Оценочные средства**
ОПК-4.1. Знает подходы к обоснованию затрат на информационную безопасность, методы и модели установления зависимости между затратами на защиту информации и уровнем защищенности.	Знать подходы к обоснованию затрат на информационную безопасность, методы и модели установления зависимости между затратами на защиту информации и уровнем защищенности.	практическое задание; опрос, компьютерный тест
ОПК-4.2. Умеет оценивать эффективность проектных решений по разработке систем обеспечения информационной безопасности документацию в соответствии с действующими нормативными и методическими документами в области защиты информации	Уметь оценивать эффективность проектных решений по разработке систем обеспечения информационной безопасности документацию в соответствии с действующими нормативными и методическими документами в области защиты информации	практическое задание; ролевая/деловая игра; опрос; отчет (по практическим занятиям, контрольной СР)
ОПК-4.3. Умеет разрабатывать проектную документацию, анализируя экономические показатели проекта;	Уметь разрабатывать проектную документацию, анализируя экономические показатели проекта;	практическое задание; ролевая/деловая игра; опрос; отчет (по практическим занятиям, контрольной СР)
ОПК-4.4. Умеет пользоваться методиками оценки стоимости владения для подсистемы информационной безопасности, определять зависимость между затратами на ИБ и уровнем защищенности, определять зависимость между затратами и уровнем защищенности и эффективности в проектах по информационной безопасности.	Уметь пользоваться методиками оценки стоимости владения для подсистемы информационной безопасности, определять зависимость между затратами на ИБ и уровнем защищенности, определять зависимость между затратами и уровнем защищенности и эффективности в проектах по информационной безопасности.	практическое задание; ролевая/деловая игра; опрос; отчет (по практическим занятиям, контрольной СР)
ОПК-4.5. Владеет навыками оценки и обоснования затрат на ИБ, навыками обоснования проектных решений по созданию систем обеспечения безопасности информации, навыками разработки рабочей технической документации в соответствии с действующими нормативными и методическими документами в области защиты информации.	Владеть навыками оценки и обоснования затрат на ИБ, навыками обоснования проектных решений по созданию систем обеспечения безопасности информации, навыками разработки рабочей технической документации в соответствии с действующими нормативными и методическими документами в области защиты информации.	практическое задание; ролевая/деловая игра; опрос; отчет (по практическим занятиям, контрольной СР)

Критериями оценивания при модульно-рейтинговой системе являются баллы, которые выставляются преподавателем за виды деятельности (оценочные средства) по итогам изучения разделов 1-3 дисциплины, перечисленных в рейтинг-плане дисциплины.

Для зачета: текущий контроль – максимум 50 баллов; рубежный контроль – максимум 50 баллов, поощрительные баллы – максимум 10).

Шкалы оценивания для зачета:

зачтено – от 60 до 110 рейтинговых баллов (включая 10 поощрительных баллов),

не зачтено – от 0 до 59 рейтинговых баллов).

Рейтинг – план дисциплины
«Экономика защиты информации»

Специальность: 10.05.05 Безопасность информационных технологий в правоохранительной сфере

курс 5, семестр 9

Виды учебной деятельности студентов	Балл за конкретное задание	Число заданий за семестр	Баллы	
			Минимальный	Максимальный
Модуль (Раздел) 1				
Текущий контроль				**14**
Аудиторная работа				
1. Практические задания	**2**	**6**	**5**	12
2. Устный опрос	**1**	**2**	**0**	2
Рубежный контроль				**10**
1. Тестовый контроль	**0,5**	**20**	**0**	10
Модуль (Раздел) 2				
Текущий контроль				**13**
Аудиторная работа				
1. Практические задания	**3**	**4**	**5**	12
2. Устный опрос	**1**	**1**	**0**	1
Рубежный контроль				**10**
1. Тестовый контроль	**0,5**	**20**	**0**	10
Модуль (Раздел) 3				
Текущий контроль				**23**
Аудиторная работа				
1. Практические задания	**3**	**7**	**10**	21
2. Устный опрос	**1**	**2**	**0**	2
Рубежный контроль				**30**
1. Исследовательский доклад (коллоквиум)	**20**	**1**	**10**	20
2. Тест итоговый	**0,5**	**20**	**5**	10
Поощрительные баллы				
1. Студенческая олимпиада				**0**
2. Публикация статей				**10**
Посещаемость (баллы вычитаются из общей суммы набранных баллов)				
1. Посещение лекционных занятий			**0**	**–6**
2. Посещение практических (семинарских, лабораторных) занятий			**0**	**–10**
Итоговый контроль				
Зачет				

Примерная тематика курсовых проектов (работ)

Курсовое проектирование не предусмотрено

Планы практических/семинарских занятий

Раздел 1. Представление о подходах к оценке стоимости СЗИ

Практические занятия № 1-2. Расчет экономических показателей, использующихся при оценке экономической эффективности СЗИ (4 часа)

Цель: практическое знакомство с подходами и методиками оценки экономической эффективности системы защиты информации.

Содержание занятия:

а. Теоретическая часть: опрос.

б. Практическая часть: следует выполнить нижеприведенные задания, руководствуясь лекционным материалом.

Задание 1. На основании таблицы определите коэффициенты (руководствуясь теоретическим материалом):

№	Показатель (значение на начало отчетного периода)	Тыс.р.
1	Основные производственные фонды (ОПФ)	100000
2	Поступило ОПФ за отчетный период	900
3	Выбыло ОПФ за отчетный период	800
4	Объем выпущенной продукции и услуг за отчетный период	400000

Найти

А) коэффициент использования основных средств на конец года (фондоотдачу, фондоемкость, фондовооруженность)

Б) коэффициент выбытия основных средств

В) коэффициент обновления и прироста оборудования.

Задание 2.

Основные производственные фонды предприятия на начало года составили 470 млн. руб. В августе того же года приобретен комплекс технических средств защиты стоимостью 100 млн. руб., а 1 октября продано устаревшее оборудование по остаточной стоимости 186 млн. рублей. Найдите среднегодовую стоимость основных производственных фондов.

Задание 3.

Предприятие производит 4000 изделий в год, ежеквартально приобретая материал для производства (в год предприятию требуется 360 тонн материала для производства); период технологической подготовки производства 5 дней, среднее отклонение между поставками материала – 4 дня. Надо рассчитать величину производственного запаса материала для обеспечения производственной программы.

Задание 4.

Фирма реализовала в 1 квартале года 5000 изделий, покрыв свои расходы, но не получив прибыли. Общие постоянные расходы составили 70 тыс рублей ежеквартально, плюс расходы на производство каждого 1-го изделия – 60 рублей. Во втором квартале было изготовлено 6000 изделий. Какова прибыль в рублях и рентабельность в % за оба квартала?

Примечание: Рентабельность затрат – коэффициент, равный отношению балансовой прибыли от реализации к сумме затрат на производство и реализацию продукции (прибыль/себестоимость*100%), где прибыль = (доходы)-(расходы на производство)

Задание 5. После внедрения СЗИ стоимостью 900 тыс рублей положительный эффект (снижение потерь) оценен в 1325 тыс. Оцените рентабельность затрат (в процентах).

Задание 6. (по материалам лекции №3). На основе исходных оценок требуется найти показатель ALE (Annual Loss Expectancy) уменьшения среднегодовых потерь фирмы из-за инцидентов безопасности. ALE найдите как разницу между среднегодовым ущербом ДО – и ПОСЛЕ внедрения защитных мер (ALE=Ущ1-Ущ2, где Ущ1 – ущерб от инцидентов

безопасности в текущем году, Ущ2 – в предыдущем). Данные для оценки ущерба за 2 года: в прошлом году было 8 успешных для злоумышленников попыток взлома базы данных, в этом году – 1; оценка финансовых потерь от взлома в прошлом году 120000, в этом 15000. Число уязвимостей и сократилось в 4 раза (после применения мер защиты).

Практические занятия № 3. Расчет экономических показателей, использующихся при оценке экономической эффективности СЗИ (2 часа)

Цель занятия: теоретические изучение нормативов и стандартов, действующих в области организации ЗИ.

Содержание занятия: выбор тематики КСР и доклады по теме семиара.

Выбор задания (объекта) для выполнения КСР (0,7 часа)

Всем студентам предлагается ознакомиться с заданием самостоятельной контрольной работы (исследовательская работа) и найти/выбрать объект исследования. Результат выбора фиксируется преподавателем. Каждому студенту следует отчитываться о промежуточных результатах исследования на каждом семинаре (в ходе устного опроса), а на последнем занятии представить на общее обсуждение результаты экономических расчетов по совершенствованию СЗИ объекта исследования.

Теоретическая часть – темы докладов (1,3 часа)

1. Законодательные акты, регулирующие экономические вопросы защиты информации.
2. Экономические проблемы информационных ресурсов и защиты информации.
3. Место информации в структуре общественного производства. Информация как фактор производства, актив и источник рисков в условиях цифровой экономики.
4. Основные подходы к определению затрат на защиту информации. Классификация затрат на защиту информации.
5. Рассмотрение и решение проблем экономической безопасности в России в начальной период экономических реформ.
6. Нормативные основы обеспечения экономической безопасности.
7. Стоимость информационных ресурсов и активов, принципы ее оценки. Составляющие стоимости информационных массивов.

Практическое занятие 4. Определение затрат на защиту информации. Экономический анализ и оценка угроз при проектировании системы информационной безопасности

Цель: практическое знакомство с подходами и методиками анализа угроз при проектировании и модернизации системы защиты информации.

Содержание занятия:

Теоретическая часть: опрос.

Практическая часть – решение задач.

При решении задач рекомендуется использовать материал лекций и раздаточный материал с примерами и формулами (см. рассылку на почтовый ящик группы).

Задание 1. Рассчитать затраты на [возможные] потери в связи с нарушением политики инф. безопасности (это 1 из 3 компонентов затрат на ИБ при экономической оценке размера инвестиций в СЗИ). Оценки делать экспертным методом. Объектом информационной защиты считать СЭД (систему корпоративного электронного документооборота), о которой известны такие сведения:

1) стоимость владения/использования СЭД (в год) = 130000,

2) стоимость восстановления рабочего состояния «упавшего» сервера, на котором хранятся корпоративные электронные документы – ок. 12000 за 1 восстановительное мероприятие (по данным прошлого года, событие случалось дважды),
3) Стоимость восстановления базы, испорченной из за того, что не было актуальной резервной копии базы на момент падения сервера (1 случай в прошедшем году, обошедшийся в 35000).
4) Цена простоя из-за недоступности сервера/ИС/интернета – 1000 в час (экспертная оценка), количество подобных инцидентов за прошлый год – около 10, в среднем по 1 часу длительностью каждый.
5) «Цена» дискредитации в глазах клиентов из-за задержек с обработкой данных или цена потери клиента из-за сбоев именно в СЭД – примерно 500 за 1 клиента (по экспертной оценке), а число таких инцидентов за год было 5,
6) «цена» дискредитации в глазах контрагентов или утечки их конфиденциальных и/или их персональных данных в отрытый доступ (экспертная оценка) – 50000 (инцидентов за прошлый год не случалось (но может случиться, если…); (оценка экспертная - по опыту аналогичных фирм),
7) учесть и другие риски и оценить их приближенно (например, затраты с порчей или уничтожением базы документов или всей СЭД при причине поломки техники или злонамеренных и ошибочных действий персонала фирмы).
8) Текущие расходы на комплектующие, расходные материалы, ремонты для сервера, рабочих станций, принтеров, с помощью которых осуществляется работа персонала с СЭД (покупка которых связана с необходимостью поддержания работы корпоративного электронного документооборота) – еще примерно 15000 в среднем ежегодно (оценка инженеров).
9) Стоимость трудозатрат обслуживающего персонала (инженеров/админа/операторов) – ок. 80000 ежемесячно, не считая выплат внешним специалистам за внеплановые ремонты.

В дополнение к этому в планах по улучшению надежности работы СЭД принято решение приобрести сетевое серверное хранилище за 25000 руб. (для резервного копирования базы документов а также обеспечения дистанционной работы сотрудников с эл.документами через мобильные устройства).

Задание 2. Посчитать ТСО (ССВ) указанной СЭД на 3 года вперед (с функцией дисконтирования). В качестве коэффициента дисконтирования возьмите ставку рефинансирования ЦБ РФ (она же ключевая ставка) составляет 7,5% годовых. Ставка действует с 17 сентября 2018 года по 28 октября 2018 года. Формула (см. лекционный материалы): $$TCO = K + \sum_{t=1}^{n} \frac{C_t}{(1+r)^t}$$

Задание 3. Оцените эффект (и рентабельность) планируемых расходов на дополнительные меры (см. задание 1) по улучшению надежности работы СЭД на 1 следующий год по простейшей формуле оценки эффективности затрат на СЗИ: ROI=(ALE-TCO)/TCO

Примечание: ТСО – стоимость защитных мер на создание или модернизацию системы информационной безопасности за 1 год, например (считается простым суммированием планируемых в течение года затрат на лицензию, оборудование и ПО, внедрение, обучение, обслуживание, техподдержка и т.д. – по аналогии с тем, как описано ранее либо по формуле дисконтирования если затраты планируются на несколько лет а не на год).

ALE (уменьшение среднегодовых потерь – за счет снижения рисков ущерба после внедрения системы защиты информации) – может быть досчитана как разница между среднегодовым ущербом ДО – и ПОСЛЕ внедрения СБИ. (ALE от англ. Annual Loss Expectancy - среднегодовые потери организации в результате инцидентов безопасности). Если ROI >1 – инвестиция рентабельна и указывает, во сколько раз доходы превышают расходы.

Практические занятия 5,6. Подходы к определению затрат на ЗИ. Обоснование экономических затрат на СЗИ. Тестирование. (4 часа)

Цель: практическое знакомство с подходами и методиками оценки затрат на СЗИ.
Содержание занятия: Занятие содержит теоретическую и практическую части.

Теоретическая часть: опрос и ознакомление с формулами и методиками, которые следует применять при выполнении заданий практической части.
Практическая часть: решение задач.

Задача 1. Фирма принимает решение, имеет ли смысл вкладываться в модернизацию СЗИ на ближайшие 6 лет, которая сразу потребует затрат 100000 у.е., а затем еще по 5000 у.е. ежегодно. Ожидаемые потери от всех остаточных рисков реализации угроз за 6 предстоящих лет оценены в 25000. Ожидаемый положительный эффект от внедрения СЗИ оценен в 30000 у.е. ежегодно (за счет снижения ущерба при устранении некоторых уязвимостей).
Необходимая норма прибыли (рентабельность) =10%. Надо с помощью расчетов определить, есть ли смысл инвестировать в модернизацию СЗИ.

Задача 2. Определение ущерба информационных активам от угрозы (по методике, на основе конкретных исходных данных).

Задача 3. Определение затрат на защиту информации (классификация затрат на ЗИ, определение размера целесообразных затрат на обеспечение защиты) (Расчеты выполняются по конкретным исходным данным).

Задание 4. Описать (письменно) общий подход и обобщенный алгоритм расчета (обоснования) затрат на СЗИ организации.

Тестирование в дистанционном курсе (Тест №1) (0,5 часа)

Раздел 2. Оценка рисков ИБ

Практические занятия 7 (семинар). Управление ресурсами в процессе защиты информации. Угрозы информационным ресурсам. Информационные риски (2 часа)

Цель занятий: теоретические знакомство с практикой анализа угроз ИБ, подходов и методик оценки рисков ИБ при создании СЗИ.
Содержание: подготовка студентов к докладам и устное изложение усвоенного материала.

Темы докладов:

1. Место информационной безопасности в системе безопасности
2. Концепция и политика безопасности предприятия/фирмы/организации.
3. Информационные объекты защиты и основные группы угроз.
4. Управление ресурсами в процессе защиты информации.
5. Интеллектуальная собственность предприятия и ее защиты: нормативы и стандарты в этой области. Патентное законодательство в России и состояние дел в вопросе его защиты.
6. Способы экономической оценки стоимости информации, составляющей коммерческую тайну.
7. Способы оценки цены потерь от утраты контроля над конфиденциальной информацией.
8. Способы оценки выгоды злоумышленника от хищения информационных активов.
9. Риски (их классификация), связанные с информационной безопасностью. Оценка риска. Управление рисками при осуществлении хозяйственно-экономической деятельности.

Риски в информационной деятельности.

10. Оценка рисков при защите информации.
11. Методы расчетов, учитывающие характер и особенности производства и реализации контрафактной продукции, созданной с использованием информации, приобретенной противоправным путем.
12. Стоимостная оценка ущерба, нанесенного владельцу информации в связи с утратой прав на ее коммерческую реализацию на основе лицензионных соглашений.
13. Подходы к управлению рисками.

Практическое занятие № 8. Подходы к определению затрат на ЗИ. Обоснование экономических затрат на СЗИ (2 часа)

Цель: практическое знакомство с подходами и методиками оценки рисков ИЮ при выстраивании системы защиты информации.

Содержание занятия: решение задач.

Задача 1. Оцените риски, сделайте вывод (руководствуясь 3-факторной методикой и матрицей рисков-угроз, которая перед задачей):

- если не принять меры защиты, вероятность негативного события P(X)=0,9, уровень ущерба – высокий (ценность защищаемого актива 20000 у.е.), уровень уязвимости – высокий (50% потери полезной стоимости актива).
- если принять полумеры (стоимостью 1100 у.е.), то вероятность угрозы P(X)=0,6, уровень уязвимости снизится до 15%,
- если принять меры защиты (затраты на такой уровень защиты будут выше – 2600 у.е.), вероятность угрозы P(X)=0,3, уровень уязвимости – низкий (5%),

Как поступить? - Обоснуйте свой выбор.

Задача 2. Используя 5 балльную шкалу рисков (см. таблицу ниже), оцените исходные и остаточные риски по 2 факторной методике (можете использовать методику «дерево событий» для наглядности процесса расчетов) , если известны исходные оценки:

- атаки на сервер происходили в предыдущем году примерно 1 раз в квартал, в случае успеха атаки для злоумышленников (а такое случились 2-жды за прошлый год) затраты на восстановление рабочего состояния составили в среднем 5000 у.е. за каждый инцидент
- 1 раз случилось возгорание в серверной, но его вовремя ликвидировали, хотя пришлось потратить 9000 у.е. на замену проводки и т.п. (если бы поджог случился ночью, могла бы быть уничтожен сервер, периферийная техника и локальная база данных общей стоимостью на сумму 100000).
- На следующий год принято решение установить более надежную систему пожаротушения, проводку и систему оповещения стоимостью 18000 у.е., - ожидается, что это исключит опасность возгорания.

Значение шкалы (балл)	вероятность	Количественное описание вероятности
0	Очень низкая	Частота возникновения угрозы в среднем 1 раз в 3 года (вероятность возникновения 0,2-0,4)
1	Низкая	1 раз в год (Вероятность возникновения 0,4-0,6)
2	Средняя	1 раз в 4 месяца (Вероятность возникновения 0,6-0,8)
3	Высокая	1 раз в месяц (Вероятность возникновения более 0,8)
4	Очень высокая	1 раз в неделю (Вероятность возникновения более 0,9)

Задача 3. По условиям задачи 2 оцените ожидаемые среднегодовые потери ALE от реализации обоих рисков в следующем году (при условии, что эти риски будут приняты руководством без попыток их предупредить).

Практические занятия № 9,10. Оценка рисков (4 часа)

Содержание занятия: выполнение теоретических докладов и решение задач

Теоретическая часть (1 час)

Теоретический «семинар» на темы (или устный опрос по темам ниже):
1. Подходы и методы оценки рисков.
2. Подходы и методы оценки вероятности угроз

Примечание: Эти 2 темы докладов должен подготовить каждый студент письменно, в виде текстового отчета, (с формулами, где это имеет смысл):

Практическая часть (3 часа)

Задача 1. Имеется ИС ценностью 200 у.е.; угрозу ей могут нести действия внешних злоумышленников или внутренних сотрудников (по невнимательности или злому умыслу и проч.), причем, судя по опыту прошлого периода, сотрудники наносят ущерб в среднем в 4 раза чаще внешних злоумышленников. Среди опасных действий сотрудников 30% приходится на порчу баз данных (ущерб при этом составляет 50 у.е.), 50% всех инцидентов безопасности, связанных с ущербом ИС со стороны сотрудников, связаны с некорректными действиями, из-за которых ИС выходит из строя, и организация несет ущерб 10 у.е. за каждый инцидент. Остальные инциденты безопасности, связанные с действием сотрудников при работе с ИС прямого ущерба не наносят. благодаря имеющимся мерам безопасности. Внешний злоумышленник может попытаться нанести ущерб ИС через имеющиеся уязвимости одним из двух равновероятных способов: взломать доступ к ИС через сеть и украсть данные (возможный ущерб из-за потери контроля на данными оценен в 50 у.е., но доля всех успешных попыток такой кражи составляет 1/2) либо вывести из строя ИС через сеть (ущерб от 1 инцидента 10 у.е., но благодаря имеющимся мерам защиты успехом для злоумышленника завершается лишь 8 из 10 таких попыток). Постройте дерево событий/угроз, оцените риски по каждому виду уязвимости.

Задача 2. Постройте дерево решений для проекта по выведению на рынок нового лекарства (руководствуйтесь обозначениями, приведенными в примерах в лекции по данной теме).

Условия: Фармацевтическая компания разработала формулу нового лекарства от головной боли. Руководство компании стоит перед выбором: продать лицензию на эту разработку за 100 млн. сейчас или самой продолжить работу с данным препаратом. В случае продолжения разработки, компании необходимо провести доклинические испытания, вероятность успеха которых, исходя из прошлого опыта, оценивается специалистами в 80%. В случае неудачи доклинических испытаний проект завершается (ликвидационная стоимость активов равна нулю). Затраты на доклинические испытания оцениваются в 50 млн. В случае успеха доклинических испытаний, компания может продать лицензию на данный препарат уже за 200 млн. или продолжить разработку самостоятельно. В последнем случае необходимо провести клинические испытания, затраты на которые оцениваются в 150 млн., а вероятность успеха в 60% (ликвидационная стоимость в случае неудачи также равна нулю). Наконец, в случае успешного завершения клинических испытаний, компания может приступить к производству препарата. Для этого она может закупить и установить конвейер малой мощности (стоимость 400 млн.) или конвейер большой мощности (стоимость 1000 млн.). При этом, существует еще рыночная неопределенность относительно успешности препарата на

рынке. В случае, если он будет пользоваться высоким спросом, денежные потоки составят 1800 млн. для большого и 700 млн. для малого конвейера. В случае умеренного спроса – 600 млн. для большого и 300 млн. для малого конвейера соответственно. Ситуации высокого и умеренного спроса равновероятны.

Построив дерево (граф) решений, найдите оптимальное решение по нему.

Задача 3.

Для предупреждения угроз, описанных в задаче 1, могут быть приняты дополнительные меры защиты (приобретена более надежная ИС); как ожидается в результате вероятность порчи БД по виде сотрудников снизится до 0,1 (ущерб тот же), а ущерб от некорректных действий пользователя вообще исчезнет; вероятность кражи данных злоумышленником снизится в 5 раз, а вероятность вывода из строя ИС злоумышленником понизится до уровня 0,2 (вместо 0,8).

Найдите ожидаемую сумму потерь от обеих угроз ИС до и после принятия дополнительным мер защиты. (за пример решения можно взять задачу из лекции по теме)

Задача 4. Пусть известны основные угрозы активам фирмы и уже подсчитан ожидаемый годовой ущерб от этих угроз (ALE):

Информационный ресурс (актив)	угроза	SLE (в руб.)	ARO	ALE (в руб.) - *посчитать*
Серверная	пожар	340000	0,05	…
Документация и базы, составляющие коммерческую тайну	НСД/хищение	140000	0,1	…
Оборудование (серверы, сетевое оборудование)	неисправность	95000	0,1	…
ИС и иные данные, не составляющие тайны, но используемые для реализации рабочих процессов (стоимость восстановления в случае уничтожения)	Вирусы, случайное удаление или иная порча персоналом	40000	1	…
ИСПДн клиентов	НСД/хищение	280000	2	…

Для снижения рисков намечены меры безопасности по каждому виду угроз.

- усиление мер пожарной безопасности стоимостью 2000 $ снизит риск пожара вдвое (т.е. RM = 0.5),
- установка новой ОС на сервер снизит более чем на треть частоту поломок файлового сервера и хищения коммерческой тайны, но обойдется в 1500$, и по угрозе «кража данных о кредитных карт клиентов» риск немного снизится (RM=0.1).

При этом, если злоумышленники будут пытаться нанести ущерб некоторым из указанных активов, то после дополнительных мер защиты им это станет сделать сложнее:

- по 2 угрозе (хищение коммерческой тайны) ожидаемая выгода для вора (GI) м.б. ок. 2000$, затраты на хищение (EBS) – 100$, после принятия мер защиты (EAS) еще 200$
- по 5 угрозе (кража информации о кредитной карте клиента) ожидаемая выгода для вора м.б. ок. 200$, затраты на хищение – 50$, после принятия мер защиты еще 50 $.

Оцените (по образцу примера из лекции на тему «Оценка рисков ИБ») какие из этих мер целесообразны, исходя из критерия максимизации экономического эффекта (ROI) и минимизации показателя успешности атаки с точки зрения потенциального злоумышленника (ROA).

Практическое занятие № 11. Семинар. Тестирование (2 часа)

Цель занятия: проверка закрепления знаний по разделам 1 и 2 курса «Экономика защиты информации».
Содержание занятия: Доклады:

1. Экономическая оценка ущерба от результатов противоправного использования информации (опыт, методики для конкретных видов угроз, конкретные примеры).
2. Состояние и последние изменения российского законодательства в области страхования информационных рисков для субъектов и объектов КИИ.
3. Интеллектуальная собственность предприятия и ее защиты: нормативы и стандарты в этой области. Патентное законодательство в России и состояние дел в вопросе его защиты.
4. Способы оценки цены потерь от утраты контроля над конфиденциальной информацией, от кибератак. Экономическая оценка стоимости защитных мер от указанных угроз.
5. Способы экономической оценки стоимости информации, составляющей коммерческую тайну.
6. Предпринимательские риски, связанные с информацией.

- Опрос устный.
- Выполнение теста № 2 в дистанционном курсе «ЭЗИ» в СДО (0,5 часа).

Раздел 3. Оценка экономической эффективности СЗИ

Практические занятия № 12,13. Оценка совокупной стоимости владения СЗИ и методы оценки эффективности СЗИ (4 часа)

Цель: практическое знакомство с подходами и методиками оценки рисков информационной безопасности при проектировании и модернизации системы защиты информации.

Содержание занятия: решение задач, выполнение заданий.

Задание 1. Запланирована установка оборудования стоимостью 13,5 млн. рублей, расходы на монтаж оборудования 0,9 млн., срок службы до списания – 6 лет, остаточная стоимость оборудования к концу срока службы не должна превышать 0,5 млн. Надо определить сумму амортизационных отчислений (с накоплением за весь период, линейным методом), а также норму амортизации.

Задание 2. Установлено 16 экземпляров оборудования стоимостью по 140 тысяч каждый, затраты на установку всех 16 экземпляров 1250 тыс. руб, срок службы – 6 лет года, совокупная ликвидационная стоимость всего этого оборудования – 1300 руб. Оцените норму амортизации.

Задание 3. Стоит задача модернизации СЗИ и его ТЭО (оценить эффективность проекта модернизации путем подсчета ROI и коэффициента нейтрализации угроз). Исходные данные:

А) Оценка активов. Пусть в фирме «К…» выявлены такие информационные активы, с учетом имеющихся потоков информации в организации (см. в таблице ниже). В результате анализа их ценности активам выставлены оценки значимости (ценность по 5 балльной шкале - от 0 (малоценный актив) до 4 (критически важный актив)):

Таблица. Информационные активы предприятия

Наименование актива	Форма представления	Владелец актива	Угроза и ее вероятность (выская/средняя/низкая)	Ценность актива (качественная оценка)
Личные дела персонала	документ	Руководители, специалисты	Угроза доступности (Н)	2 средняя
Внутренняя	документ	Руководители,	НСД, утрата (С)	4 Критически

переписка		специалисты		значимая
Информация о технических и программных средствах	документ	Руководители, специалисты	Угроза доступности (С)	1 малая
Финансовая документация	документ	Руководители, специалисты	НСД (С)	1 малая
Бухгалтерская документация в ИС	документ	Руководители, специалисты	Угроза доступности (Н)	2 средняя
Программное обеспечение	Информация на цифровом носителей	Специалисты техподдержки	Нарушение работоспособности, целостности (Н)	2 средняя
Сотрудники как носители информации	персонал	Специалисты техподдержки	Потеря трудоспособности, увольнение (потеря контроля) (Н)	1 малая
Техническое обеспечение (компьютерная и сетевая техника)	Материалный объект	Специалисты техподдержки	Полная или частичная утрата (первоначальной стоимости) (Н)	2 средняя
Внутренние документы о орг.структуре и процессах организации, в т.ч. сведения о системе безопасности	Документы, иная информация	Специалисты, руководители	НСД (В)	3 высокая
Информационные услуги	информация	Руководители, специалисты (в т.ч. внешние)	Утрата доступности (С)	2 средняя

Активы экспертно ранжированы по ценности (ранги от 1 (самый ценный) до 10 (ценность в контексте ИБ минимальна по субъективной оценке)):

Наименование актива	Ценность актива (ранг)
Личные дела персонала	1
Информация о технических и программных средствах	2
Внутренние документы о орг.структуре и процессах организации, в т.ч. сведения о системе безопасности	3
Бухгалтерская документация в ИС	4
Информационные услуги	5
Финансовая документация	6
Внутренняя переписка	7
Техническое обеспечение (компьютерная и сетевая техника)	8
Программное обеспечение	9
Сотрудники как носители информации	10

Б) Оценка угроз и степени уязвимости активов. Пусть экспертным путем составлен перечень уязвимостей, связанных активами, уязвимостям сопоставлены условные уровни, в таблице ниже приведены оценки уязвимости по 3-балльной качественной шкале (Н-низкая уязвимость, С - средняя, В - высокая):

группа уязвимостей	Личные дела персонала	Информация о технических и программных средствах	Внутренние документы о орг.структуре и процессах организации, в т.ч. сведения о системе безопасности	Бухгалтерская документация в ИС	Информационные услуги	Финансовая документация	Внутренняя переписка	Техническое обеспечение (компьютерная и сетевая техника)	Программное обеспечение	Сотрудники как носители информации
1. Среда и инфраструктура										
Нестабильная работа электросети			низкая	низкая		низкая	низкая	средняя	средняя	
2. Аппаратное обеспечение										
Недостаточное обслуживание	высокая	средняя	средняя	средняя	средняя	средняя	средняя	средняя	средняя	средняя
Отсутствие контроля изменения конфигурации	высокая	высокая	высокая	высокая	низкая	высокая	высокая	низкая	высокая	низкая
3. Программное обеспечение										
Отсутствие механизмов идентификации и аутентификации	средняя	высокая	высокая	средняя	высокая	средняя	высокая	низкая	средняя	высокая
Незащищенные базы паролей	средняя	высокая	высокая	низкая	высокая	средняя	высокая	низкая	средняя	высокая
Прохое управление паролями	средняя	высокая	высокая	низкая	высокая	средняя	высокая	низкая	средняя	высокая
Ошибки назначения прав доступа	высокая	высокая	высокая	высокая	высокая	высокая	высокая	низкая	высокая	средняя
Незащищенное подключение к сетям	средняя	высокая	высокая	низкая	высокая	низкая	высокая	низкая	средняя	высокая
4. Работа с документами										
Хранение в незащищенных местах	средняя	высокая	средняя	высокая	высокая	высокая	высокая	низкая	низкая	средняя
Невнимательность сотрудников	средняя	высокая	средняя	высокая	высокая	высокая	высокая	средняя	средняя	средняя
Бесконтрольное копирование и доступ	высокая	высокая	средняя	высокая	высокая	высокая	высокая	низкая	средняя	средняя
5. Персонал										

Неправильное использование ПО и ТС	низкая	средняя	средняя	средняя	средняя	средняя	низкая	средняя	средняя	средняя
Потеря трудоспособности, увольнение (потеря контроля)	низкая	низкая	низкая	низкая	низкая	низкая	низкая	низкая	низкая	низкая
6. Общие уязвимости										
Неадекватные результаты проведения ремонта и техобслуживания	низкая	низкая	низкая	низкая	низкая	низкая	низкая	средняя	низкая	низкая

В) Оценка рисков. Составьте таблицу угроз и проставьте для каждого актива уровень риска. Оценка уровня риска предполагается по 3 факторной методике – в зависимости от (1) ценности активов, (2) вероятности угрозы им, (3) степени уязвимости. Для каждого актива учитываются уязвимости и соответствующие им угрозы (либо по каждой угрозе суммируется по всем активам ее совокупный уровень риска). Составьте таблицу качественной оценки рисков (шапка: **Риск | Актив | Ранг риска** путем применения вышеуказанного правила к каждому из 10 вышеперечисленных активов. Ранжируйте угрозы по уровням совокупного риска (всем активам).

Для **оценки рисков** используйте правило начисления «штрафных баллов» для каждого актива, например, 9-балльную шкалу уровней риска:

(1)Степень серьезности происшествия (цена потери, ущерба)	(2) Уровень угрозы (вероятность реализации угрозы)								
	Низкий			средний			высокий		
	(3) уровни уязвимостей*			(3) Уровни уязвимостей			(3) Уровни уязвимости		
	Н	С	В	Н	С	В	Н	С	В
Negligible	0	1	2	1	2	3	2	3	4
Minor	1	2	3	2	3	4	3	4	5
Moderate	2	3	4	3	4	5	4	5	6
Serious	3	4	5	4	5	6	5	6	7
Critical	4	5	6	5	6	7	6	7	8

Задание 4. После оценки важности и уязвимости активов из задачи (3) м.б. проведен аудит реального состояния уровня безопасности этих активов при существующей СЗИ. В результате аудита выявили, что задачи обеспечения защиты информации решаются в настоящее время в такой мере:

№	Мероприятия в рамках действующей СЗИ	Степень выполнения
1	Орг.меры защиты коммерческой тайны	средняя
2	Физическая, аппаратная, программная защита коммерческой тайны	средняя
3	Организация защищенного делопроизводства для финансовой, бухгалтерской, управленческой документации	средняя
4	Предотвращение необоснованного допуска и открытого доступа к внутренним документам и иным сведениям, составляющим коммерческую тайну и ПДн	средняя
5	Выявление и локализация каналов утечки конфиденциальной информации при выполнении деловых процессов в организации	средняя
6	Система пожаротушения и сигнализация для предотвращения физической утраты носителей информации	низкая

7	Обеспечение охраны территории и система видеонаблюдения в защищаемых помещениях	средняя

Пусть по результатам обследования и анализа требований к СЗИ, например, выявлено, что потери из-за инцидентов ИБ составили в среднем **120000 руб** за прошедший год. Для снижения этих потерь предложена система дополнительных мер ИБ:

- организационные меры силами своих специалистов (3 сотрудника технического отдела и отдела ИБ с окладом в среднем по 24000 руб. в месяц): усовершенствовать политику паролей (смена пароля раз в месяц, использование сложного пароля), выполнить разграничение доступа к документам на сервере; внедрить более безопасные регламенты и способы ведения документации, усовершенствовать силами отдела ИБ процедуры обработки инцидентов нарушения безопасности, выделить защищенные помещения для размещения ЭВМ и средств связи и хранения носителей информации; разработать регламенты подготовки, использования, хранения, уничтожения и учета документированной информации, регламентировать доступ пользователей к конфиденциальной информации, ввести запрет на использование открытых каналов связи для передачи конфиденциальной информации, вести постоянный контроль за соблюдением установленных требований по защите информации,
- заменять по возможности в течение следующих лет сейфы и другие устройства для хранения документации,
- установить на рабочие места и сервер новые антивирусные пакеты (общей стоимостью 9000 р. в год),
- приобрести дополнительные аппаратные средства защиты: источник бесперебойного питания для сервера, обновить оборудование видеонаблюдения (монитора видеооператора, видеомонитор у проходной, заменить программного обеспечения вывода видеосигнала, заменить соединительный кабель и устаревшие видеокамеры в помещениях и на прилегающей территории на новые). **Однократные** затраты на покупку оборудование для модернизации системы видеонаблюдения:

Наименование оборудования	количество	Цена 1 шт., руб.	Сумма, руб.
монитор	2	6000	12000
Видеокамеры AS-2	4	3500	14000
Видеокамеры AS-4	3	4000	12000
Видеокамера КРС 500	3	2000	6000
Видеокамера высокого разрешения КРС S20	4	4000	16000
Кабель (м) и проч.	400	100	40000
Затраты на доставку, установку оборудования			24000
Затраты на своих специалистов по установке и настройке системы видеонаблюдения (руб.)	2 человека по 8 часов	1000 (за один 8-часовой день)	2000

Требуется

1. Рассчитать стоимость проекта модернизации СЗИ (ТСО проекта), в т.ч.:
   1.1. общую сумму затрат на проект усовершенствования системы видеонаблюдения,
   1.2. найти ежегодные затраты на обслуживание указанного компонента СЗИ на 4 года вперед.
2. Оцените целесообразность приобретения перечисленного оборудования (проведите экономическое обоснование проекта модернизации СЗИ) на будущий 4-летний период предполагаемого использования видекамер и прочих дополнительных средств защиты).

Методические указания

Задания выполняются с использованием теоретических сведений и формул из лекций № 3-6.

Подсказка к выполнению пункта (1.2) задания №4: учтите ежегодные расходы (на 4 года) на зарплату, амортизацию ОФ (списание ¼ остаточной стоимости), закупку расходных материалов и расходы на ремонт приобретенного оборудования (считаем, что через 4 года это оборудование устареет и предполагается его заменить на другое - на эти 4 года рассчитываем обоснование и оценку эффективности проекта). При расчетах ежегодных затрат на модернизацию СЗИ используйте формулу совокупных эксплуатационных затрат/расходов:

$$З_{эксп} = ЗП + А_г + Рм + Ремонт + I + Н + Пр, \quad \text{где:}$$

ЗП – заработная плата персонала, занятого обслуживанием программного или технического средства, с отчислениями на социальные нужды, надбавками/премиями/больничными: ФЗП=($ЗП_{основная}$+$ЗП_{дополнительная}$)+социальные отчисления со всей ЗП; ($ЗП_{дополнительная}$ в среднем составляет 10% от основной заработной платы исполнителя);

I – налоги, включаемые в себестоимость (налог на имущество).

Ремонт - затраты на текущий ремонт всех видов оборудования на год закладываются из расчета 5% в год от начальной стоимости;

Рм – расходные материалы на бумагу, картриджи и пр. (как считать – решает экономист, например, 1% от балансовой стоимости основного оборудования, которое планируем приобрести);

$А_г$ – расходы на амортизацию оборудования (аппаратных средств), программного обеспечения; амортизационные $А_г$ отчисления определяются по формуле $A_г = \frac{Ф_б - Ф_л}{Т_{сл}}$, исходя из первоначальной балансовой стоимости основных фондов ($Ф_б$), их ликвидационной стоимости ($Ф_л$) на конец срока использования (считаем =0) и срока службы ($Т_{сл}$= 4 года) до списания (или исходя из действующих норм амортизации ($Н_а$) $H_а = \frac{A_г}{Ф_б} \times 100\%$

Н – накладные расходы, связанные с реализацией проекта, расходы на электроэнергию для аппаратуры и персонала (как считать, решает экономист, например 20% от всех статей расхода (включая ФЗП, ежегодной амортизации нового оборудования, расходов на ремонт, на расходные материалы).

Пр – прочие расходы, включающие расходы на оплату услуг сторонней организации (сопровождение ПО), в прочие траты могут быть заложены ежегодные средние страховые отчисления во внутренний страховой фонд на случай необходимости ликвидации ущерба от реализации угроз, не перекрытых СЗИ.

При решении задач рекомендуется использовать теоретический раздаточный материал с примерами и формулами, а также материалы лекций (см. рассылку студентам на почтовый ящик группы). В частности, для оценки эффективности можно использовать формулу: $roi = \frac{\Delta Доходы - \Delta Расходы}{\Delta Инвестиции}$ Здесь: ΔДоходы - изменение в доходах, обусловленное инвестициями ИБ; ΔРасходы - изменение в расходах, обусловленное инвестициями ИБ; ΔИнвестиции - инвестиции, сделанные в ИБ). Если roi < 0, т.е. неэффективный проект СЗИ; иначе эффективный.

Возможен и **иной способ расчета экономического эффекта** и эффективности **(ROI),** например: $\mathbf{Э_{эф} = (З_2 – З_1) / З_1}$

Если полученное число положительное, проект, как минимум, безубыточен с точки зрения предупреждения рисков. Здесь совокупные расходы на модернизацию СЗИ обозначить как $З_2$ Годовые эксплуатационные расходы на обслуживание модернизированной СЗИ (подсчитанная ранее сумма следующих видов затрат:

1. амортизационная стоимость нового оборудования на конец каждого года + расходы на зарплату его обслуги (ежегодно)).
2. Затраты на текущий ремонт.
3. Затраты на материалы.
4. Накладные расходы)

Требуется знать прежние расходы на СЗИ, а также себестоимость техобслуживания ИС ДО модернизации, а также рассчитать ожидаемые потери при реализации угроз (затраты на погашение потерь плюс все затраты на прежнюю защиту информации, например, в сумме это будет $З_1$).

Еще одна оценка эффективности использования СЗИ: $E_{СЗИ} = \frac{R_{полн} - R_{ост}}{S_{СЗИ}}$. Если $E_{СЗИ} > 1$, то данное СЗИ целесообразно использовать, и напротив, если ЕСЗИ ≤ 1 – то нецелесообразно (подробнее см. лекционный материал).

Также можно использовать коэффициент нейтрализации угроз: $K_{НУ} = \frac{\sum_{i=1}^{n} a_i \cdot z_i}{a_{max} \cdot \sum_{i=1}^{n} z_i}$ где a_{max} – максимальное значение оценки, равное 10; n – количество угроз, zi – уровень значимости i угрозы, зависящий от ущерба di и вероятности pi этой угрозы $z_i = p_{ri} \cdot d_i$. Для подсчета следует экспертно определить вероятность реализации каждой i-ой угрозы: $p_{ri} = p_{ti} \cdot p_{vi}$ где p_{ri} – вероятность или доля утраты исходной ценности актива при реализации i-ой угрозы; p_{ti} – вероятность возникновения i-ой угрозы; p_{vi} – вероятность возникновения уязвимости для реализации i-ой угрозы. (в вашем случае вероятности выражены качественными оценками низкая, средняя и высокая, - сопоставьте им, например, условно, значения: до 0,2 – низкая, 0,4 – средняя, от 0,8 - высокая).

Экспертно делается и оценка потерь (доля ущерба) d_i (от 0 до 1)[1] в случае реализации i-ой угрозы. Затем для каждой угрозы определяется z_i уровень значимости, равный произведению вероятности её реализации на относительную оценку потерь: $z_i = p_{ri} \cdot d_i$

Шкала для принятия решения может выглядеть следующим образом:

- $K_{НУ} < 0,05$ – СЗИ нецелесообразно использовать;
- $0,05 \leq K_{НУ} < 0,2$ – СЗИ компенсирует небольшую часть угроз и может использоваться как дополнительное;
- $0,2 \leq K_{НУ} < 0,5$ – СЗИ частично компенсирует угрозы и может использоваться вместе с другими СЗИ;
- $0,5 \leq K_{НУ} < 0,8$ – СЗИ в большей степени компенсирует угрозы и может использоваться как основное, вместе с которым рекомендуется использовать дополнительные СЗИ;
- $0,8 \leq K_{НУ}$ – СЗИ рекомендуется к использованию в качестве основного; дополнительные СЗИ могут использоваться по желанию.

Практическое занятие № 14 (2 часа)

Цель: закрепление навыков самостоятельной работы с нормативными документами по оценке затрат на СЗИ (поиск, анализ, практическое применение нормативов, ГОСТов и методик).

[1] считаем, если нет иных сведений, что низкий уровень ущерба – это не более 0,1 утраты от исходной стоимости актива, 0,3 от стоимости актива – средний уровень ущерба, от 0,5 до 1– высокий уровень ущерба. Либо прост учитывается ущерб как полную остаточную (амортизированную на очередной год) стоимость актива.

Содержание: следует выбрать 1 тему, результат ее разработки изложить письменно (можно также устно в виде доклада) к концу занятия.

1. Оценка экономической значимости объекта КИИ при его категорировании (https://rtmtech.ru/wp-content/uploads/2018/09/PP-127-ot-08.02.2018.pdf) – показатели критериев значимости, значения категорий, разъяснения их сути (можно с примерами)
2. Субъекты КИИ (кто может быть к ним отнесен); из чего складывается статья расходов на выполнение требований закона № 187-ФЗ о безопасности критической информационной инфраструктуры.
3. Оценка экономического ущерба от инцидентов безопасности (кибератак, утечек от инсайдеров): статьи расходов на возмещение возможного ущерба, примерная доля каждой статьи в возможном совокупном ущербе из-за уязвимостей ИБ, с учетом экономической отрасли, к которой относится организация/предприятия (можно на конкретном примере или статистических данных не старее 2-3-летней давности.

Примечание: отчет прикрепляется к соответствующему практическому заданию в дистанционный курс «ЭЗИ». Объем отчета – до 8 страниц шрифтом TimesNewRoman, 12 кеглем, одинарный интервал. Требуется обязательно привести в отчете ссылки (URL страницы) на интернет-источники, если сведения взяты именно оттуда. Материалы и сетевые источники должны быть не старее, чем 3-летней давности (убедитесь в этом, прежде чем использовать в исследовании). Электронный отчет следует разместить для оценки в СДО ЭЗИ.

Практическое занятия № 15. Семинар (доклады) (2 часа)

Цель: закрепление навыков самостоятельной работы с нормативными документами по оценке затрат на СЗИ (поиск, анализ, практическое применение нормативов, ГОСТов и методик).

Содержание: доклады.

1. Оценка эффективности деятельности службы ИБ: анализ затрат на безопасность, и составление отчетности по затратам на безопасность, критерии и методики оценки эффективности СЗИ.
2. Зарубежная и отечественная практика экономической оценки эффективности проекта создания/модернизации СЗИ. Современное состояние законодательства, регулирующего эту сферу (налогового, в т.ч.) в условиях цифровой экономики.
3. Методы обеспечения сопоставимости расчетных величин при определении эффективности защиты информации. Приведение разновременных результатов и затрат к расчетному году; дисконтирование.
4. Оценка эффективности комплексной системы защиты информации.
5. Принципиальные подходы к экономическим расчетам эффективности инвестиционных проектов в защиту информации.

Практическое занятия № 16. Коллоквиум (2 часа)

Цель: закрепление навыков самостоятельной работы с нормативными документами по оценке затрат на СЗИ (поиск, анализ, практическое применение нормативов, ГОСТов и методик).

Содержание:

Студенты представляют (апробируют и защищают) результаты эмпирического исследования (обязательного) по результатам самостоятельной контрольной работы (см. критерии оценки и содержание исследования ниже).

Результат защиты/апробации оценивается до 12 баллов. Если исследование по теме КСР было опубликовано или представлено в виде доклада научной конференции в течение

семестра, то студент представляет эти результаты и может получить дополнительно еще 8 баллов.

Критерии оценки (в баллах*):*
На практических занятиях (кроме занятия № 16) за выполнение практических заданий одного занятия студентов выставляется до 3 баллов (за электронный отчет за 1 занятие (тему):

-3 балла выставляется студенту, если задания практического занятия выполнены верно и в полном объеме;
- 2 балла выполняется, если работа выполнена не полностью (60 и более%) или содержит ошибки в расчетах.
- 1 балл выставляется студенту, если практическое задание выполнено частично (30-60 %) и содержит ошибки.

Задания для самостоятельной контрольной работы
(исследовательский доклад)

Описание контрольной работы:

Самостоятельная контрольная письменная работа является обязательной формой отчетности студента по курсу Экономика защита информации. Исследование выполняется в форме разработки, заключающейся в формулировании и экономическом обосновании предложений по усовершенствованию или оценке СЗИ конкретного экономического объекта.

В качестве такого объекта обследования может быть взято предприятие/учреждение/организация, ставшая базой последней практики студента – или иной реальный экономический объект (например, предполагаемая база преддипломной практики, о которой есть возможность собрать сведения из открытых источников). Для проведения исследовательской работы студенту следует, руководствуясь знаниями и навыками, приобретенными в курсе ЭЗИ и в других учебных курсах, исследовать объект для получения сведений:

- род деятельности организации/предприятия и виды информации, обрабатываемые в организации;
- информационные объекты, требующие защиты,
- организационная структура или персонал (инсайдеры), имеющие доступ к защищаемым информационным ресурсам,
- угрозы и их актуальность, с учетом имеющихся (или предполагаемых) уязвимостей в системе защиты информации организации, с оценкой возможного ущерба и вероятности реализации угроз (уровней рисков по каждой актуальной угрозе/группе угроз);
- предложения по совершенствованию СЗИ организации,
- оценка экономических затрат на реализацию предложений по снижению вероятности и ущерба от наиболее актуальных угроз,
- сравнительная оценка всех предполагаемых затрат на модернизацию СЗИ в расчете на 1 год или на 3 года – с учетом специфики деятельности объекта исследования (организации/предприятия), и оценка ожидаемого экономического эффекта от внедрения предложений;
- корректировка предложений по совершенствованию СЗИ с учетом полученных результатов сравнительной оценки и окончательное формулирование предложений с прогнозной оценкой экономического и т.п. эффекта от реализации предложений.

Результаты исследования со всеми расчетами и описанием методики студент должен кв обязательном порядке изложить в виде электронного отчета и презентации, и апробировать **на коллоквиуме**, сопровождая свое выступление (до 5 минут) презентацией результатов (или, если материал представляет конфиденциальную информацию, защитить

отчет преподавателю). Максимальная оценка по результатам исследования – до 12 баллов (из 20 возможных за данный вид работы).

Обобщенные выводы о методических проблемах экономического обоснования эффективности СЗИ или оценке рисков ИБ могут быть оформлены в виде научной статьи или научного доклада (по согласованию с преподавателем и/или руководством объекта исследования) и изложены на научной конференции или в научном журнале. В этом случае количество баллов увеличивается вдвое (до 20).

Критерии оценки результатов (в зависимости от раздела за правильный ответ на устный вопрос студент может получить максимально 2 балла:

- 20 баллов выставляется студенту, если по результатам исследования сделано выступление на научной конференции или обобщенные результаты по теме исследования опубликованы в научном журнале/на научной конференции (подтверждается сертификатом участия или опубликованной статьей);
-12 баллов выставляется студенту, если результат исследования в ходе апробации обоснованы, правильны, показана экономическая или иная эффективность предлагаемых решений (апробация - выступление на коллоквиуме или защита с преподавателем), расчеты выполнены правильно, оформлены соответствующие экономические и т.д. расчеты;
-10-11 баллов, если исследование сделано но содержит мелкие недочеты или оценка эффективности предложений, выполненная студентом, низкая (предлагаемые затраты необоснованны завышены, имеются ошибки в оценке рисков, методика соблюдена не во всех аспектах). 10 баллов является минимально возможной балльной оценкой за данный вид обязательного рубежного контроля (и одним из главных оснований для зачета дисциплины).
- 0-9 баллов, если работа не сделана (не сдана, не защищена) или содержит грубые ошибки в методике расчетов.

Типовые вопросы устных опросов

Устный индивидуальный опрос проводится с целью поверки закрепления теоретических знаний, полученных при изучении разделов дисциплины. Студент излагает содержание вопроса изученной темы, либо отвечает на устный вопрос во время практического занятия, предварительно (домашняя работа) ознакомившись с материалами лекции и дополнительной литературы.

Примерные вопросы для опросов:

1. Становление индустрии информации.
2. Экономические проблемы информационных ресурсов.
3. Какие подходы к экономической оценке затрат на СЗИ знаете?
4. Цена информации – из чего складывается, что оказывает влияние на нее.
5. Основные принципы и методы защиты информации.
6. Основные подходы к определению затрат на защиту информации.
7. Классификация затрат на защиту информации.
8. Определение размера целесообразных затрат на обеспечение защиты информации.
9. Добывание информации.
10. Система ресурсообеспечения защиты информации и эффективность ее использования.
11. Управление ресурсами в процессе защиты информации.
12. Интеллектуальная собственность предприятия и ее защита.- какие угрозы следует учитывать, какие виды ущерба связаны с реализацией угроз подобным активам?
13. Виды ущерба, наносимые информации.
14. Как оценивать ущерб информационным активам/ресурсам? Описать общий подход с

учетом видов информационных активов.

15. Степень наносимого ущерба информации. - Какие нормативные и методические документы регуляторов описывают методики оценки ущерба и оценки актуальности угроз.
16. Методы и способы страхования информации.
17. Формирование бюджета службы защиты информации.
18. Статьи бюджета службы защиты информации.
19. Бюджет службы защиты информации в рамках концепции безопасности предприятия.
20. Подходы к оценке эффективности создания средств защиты информации.
21. Описать оценку эффективности комплексной системы защиты информации.
22. Описать оценку эффективности инвестиций в систему защиты информации.
23. Использование функционально-стоимостного анализа для повышения эффективности системы защиты информации.
24. В каких стандартах и нормативных документах можно найти описание методики или процедуры оценки рисков ИБ?
25. Описать методы и подходы к оценке эффективности затрат на СЗИ.
26. страхование информационных активов как снижения информационных рисков.
27. Как оценить риски реализации угроз? – общий «алгоритм» оценки.
28. Какие способы обработки рисков ИБ можете назвать?
29. Какие способы обработки рисков реализации угроз ИБ целесообразны в тех или иных случаях?
30. Страхование рисков как способ экономической защиты информации.
31. Виды страхования для обеспечения защиты информации.
32. Страхование информационных рисков.
33. Как экономически оценить эффективность предложений по совершенствованию СЗИ? – описать общий подход или порядок действий по такой оценке.

Критерии оценки ответа на устный вопрос:

- 1 выставляется студенту, если ответ полный и правильный;

-0 баллов, если ответ неверный или не был дан.

Типовые тестовые задания

При изучении дисциплины используются тестовые задания закрытого типа. Каждое тестовое задание включает вопрос и, как правило, 3-4 варианта ответов к нему. Необходимо выбрать один ответ из предложенных вариантов.

В течение курса предусмотрено 3 тестирования (по одному на каждый раздел). Два компьютерных тестирования из трех выполняются в СДО БашГУ в дистанционном курсе «Экономика защиты информации»; итоговое тестирование проводится в электронном личном кабинете студента (внеаудиторно).

1. Что понимается под прибылью предприятия при создании и эксплуатации систем информационной безопасности?

а. Разница, полученная предприятием, между выручкой и себестоимостью произведенной продукции, работ и услуг
б. Количественная оценка уменьшения потерь информации от предотвращения действия угрозы
в. Количественная оценка уменьшения потерь информации от предотвращения действия угрозы плюс реализационная прибыль от продажи произведенной продукции, работ и услуг.

2. Экономическое обоснование затрат на создание и эксплуатацию технических и программных средств защиты необходимо

а. для оценки эффективности принятых мер по защите информации на предприятии.
б. для сокращения доли бюджета предприятий, выделяемую на собственную безопасность
в. для обоснования оптимальной структуры и состава системы зашиты информации на предприятии

3. Экономический эффект от использования системы защиты информации определяется
а. исходя из анализа и классификации рисков, возникающих при защите информации
б. на основе экспертных оценок уровня понесенного или предотвращенного ущерба в результате внедрения КСЗИ
в. на основе оценки затрат на создание и эксплуатацию комплексной системы защиты информации и стоимости уровня понесенного и/или предотвращенного ущерба

4. На каком этапе построения системы информационной безопасности оценивается эффективность КСЗИ
а. на этапе обоснования структуры и технологии функционирования КСЗИ
б. на этапе технико-экономической оценки разрабатываемого проекта КСЗИ
в. на этапе обоснования задач защиты информации и определения необходимых мер обеспечения информационной безопасности на предприятии

5. Необходимым условием обоснования эффективности создания и функционирования системы информационной безопасности является
а. анализ угроз информационной безопасности предприятия
б. проведение аудита состояния информационной безопасности предприятия
в. анализ угроз и оценка состояния информационной безопасности предприятия

и т.д.

Критерии оценивания результатов тестирований:

Тесты № 1, 2, 3 содержат по 20 тестовых вопросов (каждый ответ на вопрос оценивается максимально в 0,5 балла), максимально возможная сумма баллов – 10 за каждый из трех тестов.

5. Учебно-методическое и информационное обеспечение дисциплины

5.1. Перечень основной и дополнительной учебной литературы, необходимой для освоения дисциплины

Основная литература:

1. Цуканова О.А., Смирнов С.Б. Экономика защиты информации: учебное пособие, 2-е издание, измененное и дополненное. – СПб.: НИУИТМО, 2014. – 90 с. – режим доступа: ссылка для скачивания: https://books.ifmo.ru/file/pdf/1559.pdf или on-line-чтение: http://docplayer.ru/31803283-Ekonomika-zashchity-informacii-uchebnoe-posobie.html
2. Ясенев, В.Н. Информационные системы и технологии в экономике : учебное пособие / В.Н. Ясенев. - 3-е изд., перераб. и доп. - Москва : Юнити-Дана, 2015. - 560 с.: табл., граф., ил., схемы - Библиогр.: с. 490-497 - ISBN 978-5-238-01410-4; [Электронный ресурс]. - URL: https://biblioclub.ru/index.php?page=book&id=115182

Дополнительная литература:

3. Прохорова, О.В. Информационная безопасность и защита информации: учебник / О.В. Прохорова ; Министерство образования и науки РФ, Федеральное государственное бюджетное образовательное учреждение высшего профессионального образования «Самарский государственный архитектурно-строительный университет». - Самара: Самарский государственный архитектурно-строительный университет, 2014. - 113 с.: табл., схем., ил. - Библиогр. в кн. - ISBN 978-5-9585-0603-3. [Электронный ресурс]. - URL: https://biblioclub.ru/index.php?page=book&id=438331
4. Кулешова, Е.В. Управление рисками проектов : учебное пособие / Е.В. Кулешова ; Министерство образования и науки Российской Федерации, Томский Государственный Университет Систем Управления и Радиоэлектроники (ТУСУР). - 2-е изд., доп. - Томск: Эль Контент, 2015. - 188 с.: схем., табл. - Библиогр.: с. 171-172 - ISBN 978-5-4332-0251-1; [Электронный ресурс]. - URL: https://biblioclub.ru/index.php?page=book&id=480767
5. Артемов, А.В. Информационная безопасность : курс лекций / А.В. Артемов; Межрегиональная Академия безопасности и выживания. - Орел : МАБИВ, 2014. - 257 с. : табл., схем; [Электронный ресурс]. URL: https://biblioclub.ru/index.php?page=book&id=428605

5.2. Перечень ресурсов информационно-телекоммуникационной сети «Интернет» и программного обеспечения, необходимых для освоения дисциплины, включая профессиональные базы данных и информационные справочные системы

1. Электронная библиотечная система «Университетская библиотека онлайн» - https://biblioclub.ru
2. Электронная библиотечная система «ЭБ БашГУ» - https://elib.bashedu.ru
3. Электронная библиотечная система БашГУ – www.bashlib.ru
4. Электронная библиотечная система издательства «Лань» - https://e.lanbook.com
5. Антиплагиат.ВУЗ. Договор № 81 от 27.04.2018 г. Срок действия лицензии до 04.05.2019 г., договор № 1104 от 18.04.2019 г. Срок действия лицензии до 04.05.2020 г
6. Банк нормативно-правовых актов РФ Министерства юстиции РФ - http://zakon.scli.ru/ru/legal_texts/index.php
7. Справочная правовая система Консультант Плюс. Договор №31705775411 от 07.12.2017 г. http://www.consultant-plus.ru
8. Национальные стандарты РФ в области информационной безопасности: http://www.iso27000.ru/standarty/gost-r-nacionalnye-standarty-rossiiskoi-federacii-v-oblasti-zaschity-informacii
9. Нормативные документы и материалы сайта ФСТЭК России (Федеральной службы по техническому и экспортному контролю России): https://fstec.ru/ Раздел «Национальные старты информационной безопасности» (https://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty/113-gosudarstvennye-standarty/377-gosudarstvennye-standarty)

Государственные информационно-правовые системы:

1. Научный центр правовой информации при министерстве Юстиций РФ - http://www.scli.ru
2. Официальный интернет-портал правовой информации - http://pravo.gov.ru
3. Информационно-правовая система «Законодательство России» - http://pravo.fso.gov.ru
4. Модуль «Документы - Президент России» - http://www.kremlin.ru/acts
5. Банк документов, подписанных Президентом России - http://kremlin.ru/acts/bank
6. База данных «Федеральные законы» - http://graph.garant.ru:8080/SESSION/PILOT/main.htm
7. Автоматизированная система обеспечения законодательной деятельности государственной думы (законопроекты и законодательные инициативы) - http://asozd.duma.gov.ru/
8. База данных «Издания по общественным и гуманитарным наукам» (на платформе East View) - Ссылка http://www.ebiblioteka.ru (вход из сети вуза без регистрации).

9. Банк данных "Библиотека копий официальных публикаций правовых актов» при ассоциации юристов России - http://alrf.consultant.ru/
10. Банк данных "Копии правовых актов: Российская Федерация» - http://giod.consultant.ru/
11. Банк данных "Нормативно-правовые акты Федерального Собрания Российской Федерации - http://duma.consultant.ru/

Другие профессиональные базы данных и информационно-справочные системы:

1. Электронная база данных диссертаций РГБ (авторизованный доступ по паролю в сети вуза) – Ссылка: http://dvs.rsl.ru
2. База данных «Вестники Московского университета» (на платформе East View) (вход без регистрации). - Ссылка http://www.ebiblioteka.ru/browse/udb/12.
3. Annual Reviews – обзор журналов по общественно-научной тематике и др. – доступ из сети вуза. – Ссылка: http://www.annualreviews.org/
4. Computers & Applied Sciences Complete (EBSCO) - доступ в сети вуза, язык английский. - Ссылка: http://search.ebscohost.com/
5. SCOPUS - наукометрическая, библиографическая и реферативная база данных издательской корпорации Elsevier. Язык английский, вход после регистрации или из сети вуза. – Ссылка: http://www.scopus.com/
6. Taylor and Francis – База полнотекстовых научных журналов, книг. Язык английский. – доступ из сети вуза. – Ссылка: http://www.tandf
7. Web of Science - наукометрическая, библиографическая и реферативная база данных издательской корпорации Thomson Reuters. Язык английский, вход после регистрации или из сети вуза. – Ссылка: http://apps.webofknowledge.com/
8. Wiley - Полнотекстовая база данных статей из 1400 журналов издательства Wiley по всем отраслям знаний. Язык английский. Доступ из сети вуза без регистрации. – Ссылка: http://onlinelibrary.wiley.com/
9. Сайт по информационной безопасности: http://securitypolicy.ru/; его раздел: «Документы, стандарты и методики по информационной безопасности»: http://securitypolicy.ru/
10. Докипедия: http://dokipedia.ru
11. Словари и энциклопедии On-Line- http://www.dic.academic.ru

Программное обеспечение

1. Windows 8 Russian Russian OLP NL AcademicEdition и Windows Professional 8 Russian Upgrade OLP NL Academic Edition. Договор №104 от 17.06.2013 г. Лицензии бессрочные.
2. Microsoft Office Standard 2013 Russian OLP NL Academic Edition. Договор №114 от 12.11.2014 г. Лицензии бессрочные.
3. Система централизованного тестирования БашГУ (Moodle). GNU General Public License.

6.Материально-техническая база, необходимая для осуществления образовательного процесса по дисциплине

Наименование специализированных аудиторий, кабинетов, лабораторий	Вид занятий	Наименование оборудования, программного обеспечения
1	2	3
Аудитория: аудитория № 403 (гуманитарный корпус), аудитория № 405 (гуманитарный корпус), аудитория № 413 (гуманитарный корпус), аудитория № 415 (гуманитарный корпус), аудитория № 416 (гуманитарный корпус), аудитория № 418 (гуманитарный корпус), аудитория № 419 (гуманитарный корпус), аудитория № 515 (гуманитарный корпус), аудитория № 516 (гуманитарный корпус).	Лекции	**Аудитория № 403** Учебная мебель, доска, Мультимедийный-проектор Panasonic PT-LB78VE – 1 шт., Экран настенный Classic Norma 244*183 – 1 шт., учебно-наглядные пособия. **Аудитория № 405** Учебная мебель, доска, вокальные радиомикрофоны AKGWMS 40 – 2шт., Интер-ая система со встроенным короткофокусным проекто-ром PrometheanActivBoard 387 RPOMOUNTEST -1 шт., Ком-ер встраиваемый в кафедру INTELCorei3-4150/DDr3 4 Gb/HDD, Экран настенный DraperLumaAV(1:1) 96/96”244*244MV (XT1000E) -1 шт., Настольный интерактивный дисплей , ActivPanel 21S – 1 шт. , Матричный коммутатор сигналов интерфейса HDMICMPRO 4H4H – 1 шт. , Мультимедиа-проектор PanasonicPT-EW640E - 1 шт., Двух-полосный настенный громкоговоритель 20Вт/100В цвет белый(MASK4T-W)(белый) -6 шт., Петличный радиомикрофон AKGWMS45 – 1 шт. , Терминал видео конференц-связи LifeSizeIcon 600 Camera 10xPhone 2ndGeneration – 1 шт., Экран настенный DraperLumaAV(1:1) 96/96”244*244MV (XT1000E) -1 шт. **Аудитория № 413** Учебная мебель, доска, двухполосный настенный громкоговоритель 20Вт/100В цвет белый(MASK4T-W) – 6 шт., Микшер-усилитель 120Вт АРАРТ MA1225 – 1 шт. **Аудитория № 415** Учебная мебель, двухполосный настенный громкоговоритель 20Вт/100В цвет белый(MASK4T-W) – 2 шт., Интерактивная доска SMART с проектором V25, Микшер-усилитель 120Вт АРАРТ MA1225 – 1 шт. **Аудитория № 416** Учебная мебель, доска, проектор Optoma Ex542 i- 1 шт., Экран настенный Dinon – 1 шт. **Аудитория № 418** Учебная мебель, доска, Экран настенный Lumien Master Pikture 153*203 Matte White Fiber Clas(белый корпус) – 1 шт., Проектор Optoma Ex542 i - 1 шт. **Аудитория № 419** Учебная мебель, Проектор Optoma Ex542 i – 1 шт., Экран настенный Dinon – 1 шт. **Аудитория № 515** Учебная мебель, доска, терминал видео конференц-связи LifeSize Icon 600-камера, интер-ая система со встроенным короткофокусным проектором Promethean ActivBoard 387 RPO MOUNT EST, профес-сиональный LCD дисплей Flame 42ST, настольный интерактивный дисплей SMART Podium SP518 с ПО SMART Notebook, матричный

		коммутатор сигналов интерфейса HDMI CMPRO 4H4H, интер-ая напольная кафедра докладчика, ком-ер встраиваемый в кафедру IN-TEL Core i3-4150/DDr3 4 Gb/HDD 1TB/DVD-RW/Therm altake VL520B1N2E 220W/Win8Pro64, стол, трибуна, кресла секционные последующих рядов с пюпитром. **Аудитория № 516** Учебная мебель, доска, кресла секционные последующих рядов с пюпитром, мобильное мультимедийное оборудование: проектор ASK Proxima, ноутбук HP, экран.
Лаборатория компьютерный класс аудитория № 404 (гуманитарный корпус), компьютерный класс аудитория № 420 (гуманитарный корпус).	Лабораторные работы	**Компьютерный класс аудитория № 420** Учебная мебель, моноблоки стационарные 15 шт. **Компьютерный класс аудитория № 404** Учебная мебель, компьютеры -15 штук. **Программное обеспечение** 1. Windows 8 Russian Russian OLP NL AcademicEdition и Windows Professional 8 Russian Upgrade OLP NL Academic Edition. Договор №104 от 17.06.2013 г. Лицензии бессрочные. 2. Microsoft Office Standard 2013 Russian OLP NL Academic Edition. Договор №114 от 12.11.2014 г. Лицензии бессрочные. 3. Система централизованного тестирования БашГУ (Moodle). GNU General Public License.
Компьютерный класс аудитория № 415 (гуманитарный корпус), аудитория № 416 (гуманитарный корпус), аудитория № 418 (гуманитарный корпус), аудитория № 419 (гуманитарный корпус), аудитория № 509 (гуманитарный корпус), аудитория № 608 (гуманитарный корпус), аудитория № 609 (гуманитарный корпус), аудитория № 610 (гуманитарный корпус), компьютерный класс компьютерный класс аудитория № 404 (гуманитарный корпус), компьютерный класс аудитория № 420 (гуманитарный корпус).	Практические занятия	**Аудитория № 415** Учебная мебель, двухполосный настенный громкоговоритель 20Вт/100В цвет белый(MASK4T-W) – 2 шт., Интерактивная доска SMART с проектором V25, Микшер-усилитель 120Вт АРАРТ MA1225 – 1 шт. **Аудитория № 416** Учебная мебель, доска, проектор Optoma Ex542 i- 1 шт., Экран настенный Dinon – 1 шт. **Аудитория № 418** Учебная мебель, доска, Экран настенный Lumien Master Pikture 153*203 Matte White Fiber Clas(белый корпус) – 1 шт., Проектор Optoma Ex542 i - 1 шт. **Аудитория № 419** Учебная мебель, Проектор Optoma Ex542 i – 1 шт., Экран настенный Dinon – 1 шт. **Аудитория № 515** Учебная мебель, доска, терминал видео конференц-связи LifeSize Icon 600-камера, интер-ая система со встроенным короткофокусным проектором Promethean ActivBoard 387 RPO MOUNT EST, профес-сиональный LCD дисплей Flame 42ST, настольный интерактивный дисплей SMART Podium SP518 с ПО SMART Notebook, матричный коммутатор сигналов интерфейса HDMI CMPRO 4H4H, интер-ая напольная кафедра докладчика, ком-ер встраиваемый в кафедру IN-TEL Core i3-4150/DDr3 4 Gb/HDD 1TB/DVD-RW/Therm altake VL520B1N2E 220W/Win8Pro64, стол, трибуна, кресла секционные последующих рядов с пюпитром**.** **Аудитория № 516** Учебная мебель, доска, кресла секционные последующих рядов с пюпитром, мобильное мультимедийное оборудование: проектор ASK

		Proxima, ноутбук HP, экран. **Аудитория № 509** Учебная мебель, доска, мобильное мультимедийное оборудование. **Аудитория № 608** Учебная мебель, доска, мобильное мультимедийное оборудование. **Аудитория № 609** Учебная мебель, доска, мобильное мультимедийное оборудование. **Аудитория № 610** Учебная мебель, доска, учебно-наглядные пособия, LED Телевизор TCLL55P6 USBLACK – 1 шт., кронштейн для телевизора NBP 5 – 1 шт., Кабель HDMI (m)-HDH(m)ver14,10м. **Компьютерный класс аудитория № 420** Учебная мебель, моноблоки стационарные 15 шт. **Компьютерный класс аудитория № 404** Учебная мебель, компьютеры -15 штук. **Программное обеспечение** 1. Windows 8 Russian Russian OLP NL AcademicEdition и Windows Professional 8 Russian Upgrade OLP NL Academic Edition. Договор №104 от 17.06.2013 г. Лицензии бессрочные. 2. Microsoft Office Standard 2013 Russian OLP NL Academic Edition. Договор №114 от 12.11.2014 г. Лицензии бессрочные. 3. Система централизованного тестирования БашГУ (Moodle). GNU General Public License.

Приложение № 1

ФГБОУ ВО «БАШКИРСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»
ИНСТИТУТ ИСТОРИИ И ГОСУДАРСТВЕННОГО УПРАВЛЕНИЯ

СОДЕРЖАНИЕ РАБОЧЕЙ ПРОГРАММЫ

дисциплины **Экономика защиты информации**
___очная_ф/о___

Вид работы	Объем дисциплины
Общая трудоемкость дисциплины (з.е. / часов)	3/108
Учебных часов на контактную работу с преподавателем:	54,2
лекций	18
практических/ семинарских	36
лабораторных	
других (групповая, индивидуальная консультация и иные виды учебной деятельности, предусматривающие работу обучающихся с преподавателем) (ФКР)	0,2
из них, предусмотренные на выполнение курсовой работы / курсового проекта	-
Учебных часов на самостоятельную работу обучающихся (СР)	53,8
из них, предусмотренные на выполнение курсовой работы / курсового проекта	-
Учебных часов на подготовку к зачету (Контроль)	-

Форма контроля:
Зачет_9__семестр

№ п/п	Тема и содержание	Форма изучения материалов: лекции, практические занятия, семинарские занятия, лабораторные работы, самостоятельная работа и трудоемкость (в часах)				Задания по самостоятельной работе студентов	Форма текущего контроля успеваемости (коллоквиумы, контрольные работы, компьютерные тесты и т.п.)
		ЛК	ПР/СЕМ	ЛР	СР		
1	2	3	4	5	6	8	9
Раздел 1. Представление о подходах к оценке стоимости СЗИ							
1.	1.1. Экономические проблемы информационных ресурсов и экономическая безопасность. Предмет ЭЗИ. Оценка информации **Содержание**: Информация как ресурс и товар. Задачи экономики защиты информации. Экономические проблемы информационных ресурсов. Роль информации в обеспечении экономической безопасности организации. Цена информации. Добывание информации. Безопасность информационных ресурсов.	2	4		4	изучение теоретического материала; подготовка к групповому опросу;	ПЗ, опрос
2.	1.2. Основные подходы к определению затрат на ЗИ. «Алгоритм» определения затрат на защиту информации (классификация затрат на ЗИ, определение размера целесообразных затрат на обеспечение защиты). **Содержание**: Угрозы информации. Основные принципы и методы защиты информации. Классификация затрат на защиту информации.	2	4		8	изучение теоретического материала;	ПЗ, опрос

	Определение размера целесообразных затрат на обеспечение защиты. Основные подходы к определению затрат на защиту информации. Статьи расходов вообще. Основные подходы к определению затрат на защиту информации. Классификация затрат на защиту информации. Определение размера целесообразных затрат на обеспечение защиты информации						
3	1.3. Обоснование экономических затрат на СЗИ. **Содержание**: Система ресурсообеспечения защиты информации и эффективность ее использования. Управление ресурсами в процессе защиты информации. Определение размера целесообразных затрат на обеспечение защиты информации. Интеллектуальная собственность предприятия, оценка ее стоимости (и стоимости ее защиты)	4	4		8		ПЗ, опрос, компьютерный тест
Раздел 2. Оценка рисков ИБ							
4	2.1. Оценка ущерба. Риск информационной безопасности. Экономическая оценка рисков. Оценка, анализ рисков ИБ **Содержание**: Виды ущерба, наносимые информации. Степень наносимого ущерба информации. Виды рисков, методы представления рисков, методы оценки рисков, связанных с информацией.	2	6		8	изучение теоретического материала; подготовка докладов	ПЗ, опрос
5	2.2. Подходы к управлению информационными рисками.	2	4		8	изучение теоретического	ПЗ, опрос, компьютерный тест

	Страхование информационных рисков как способ экономической защиты информации **Содержание**: Подходы к управлению информационными рисками Предпринимательские риски, связанные с информацией. Страхование информационных рисков. Виды, методы и способы страхования информации.					материала; подготовка к лабораторным работам,	
Раздел 3. Оценка экономической эффективности СЗИ							
6	3.1. Формирование бюджета службы защиты информации. ТЭО СЗИ. **Содержание**: Бюджет службы защиты информации в рамках концепции (политики) информационной безопасности предприятия. О технико-экономическом обосновании создания системы обеспечения безопасности информации.	4	8		9	изучение теоретического материала; подготовка докладов	ПЗ, опрос, подготовка доклада
7	3.2. Оценка эффективности комплексной системы защиты информации. Подходы к оценке эффективности инвестиций. Оценка эффективности инвестиций в СЗИ **Содержание**: Подходы к оценке эффективности создания средств защиты информации. Оценка эффективности комплексной системы защиты информации. Оценка эффективности инвестиций в систему защиты информации. Использование функционально-стоимостного анализа для повышения эффективности	2	6		8,8	изучение теоретического материала; подготовка к лабораторным работам, подготовка докладов	ПЗ, компьютерный тест

	системы защиты информации. Оценка эффективности защиты и страхования информации.						
	Всего часов:	18	36	-	53,8		