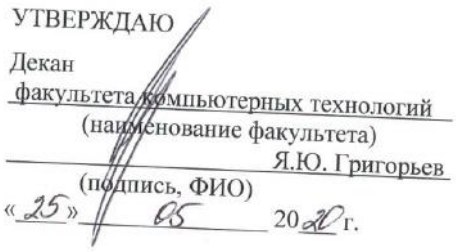
Министерство науки и высшего образования Российской Федерации
Федеральное государственное бюджетное образовательное
учреждение высшего образования
«Комсомольский-на-Амуре государственный университет»



РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ
Оценка рисков информационной безопасности автоматизированных систем

Направление подготовки	*10.05.03 "Информационная безопасность автоматизированных систем"*
Направленность (профиль) образовательной программы	*Обеспечение информационной безопасности распределенных информационных систем*
Квалификация выпускника	*специалист по защите информации*
Год начала подготовки *(по учебному плану)*	*2020*
Форма обучения	*очная*
Технология обучения	*традиционная*

Курс	Семестр	Трудоемкость, з.е.
5	*9*	*4*

Вид промежуточной аттестации	Обеспечивающее подразделение
Экзамен	*Кафедра ИБАС - Информационная безопасность автоматизированных систем*

Комсомольск-на-Амуре 2020

Разработчик рабочей программы:

Доцент УБАС _____ Власов А.А.

(должность, степень, ученое звание) (подпись) (ФИО)

СОГЛАСОВАНО:

Заведующий кафедрой

УБАС _____ Лошманов А.Ю.

(наименование кафедры) (подпись) (ФИО)

1 Общие положения

Рабочая программа дисциплины «Оценка рисков информационной безопасности автоматизированных систем» составлена в соответствии с требованиями федерального государственного образовательного стандарта, утвержденного приказом Министерства образования и науки Российской Федерации № 1509 от 01.12.2016, и основной профессиональной образовательной программы подготовки «Анализ безопасности информационных систем»
по направлению 10.05.03 "Информационная безопасность автоматизированных систем".

Практическая подготовка реализуется на основе:

Профессиональный стандарт утвержденного приказом Министерства труда и социальной защиты от 15 сентября 2016 года N 522н №843 "Специалист по защите информации в автоматизированных системах" зарегистрированного в Министерстве юстиции Российской Федерации 28 сентября 2016 года, регистрационный N 43857. Обобщенная трудовая функция: B/03.6 Управление защитой информации в автоматизированных системах.

Задачи дисциплины	Приобретение обучаемыми необходимого объёма знаний и практических навыков анализа и оценки рисков информационной безопасности автоматизированных систем
Основные разделы / темы дисциплины	1. Классификация и идентификация рисков информационной безопасности автоматизированных систем 2. Методы оценки рисков информационной безопасности автоматизированных систем

2 Перечень планируемых результатов обучения по дисциплине (модулю), соотнесенных с планируемыми результатами образовательной программы

Процесс изучения дисциплины «Оценка рисков информационной безопасности автоматизированных систем» направлен на формирование следующих компетенций в соответствии с ФГОС ВО и основной образовательной программой (таблица 1):

Таблица 1 – Компетенции и планируемые результаты обучения по дисциплине

Код и наименование компетенции	Планируемые результаты обучения по дисциплине		
	Перечень знаний	Перечень умений	Перечень навыков
Профессиональные			
ПК-7 способностью разрабатывать научно-техническую документацию, готовить научно-технические отчеты, обзоры, публикации по результатам выполненных работ	**З1(ПК-7)** Знает структурные и функциональные схемы защищенных автоматизированных систем	**У1(ПК-7)**Умеет проводить анализ структурных и функциональных схем защищенных автоматизированных информационных систем	**Н1(ПК-7)** Владеет навыками выявления потенциальных уязвимостей информационной безопасности автоматизированных систем
ПК-8 способностью разрабатывать и	**З1(ПК-8)** Знает способы проведения	**У1ПК-8** Умеет выбирать способ	**Н1(ПК-8)** Владеет навыками

анализировать проектные решения по обеспечению безопасности автоматизированных систем	анализа защищенности информационной инфраструктуры автоматизированных систем	проведения анализа защищенности информационной инфраструктуры автоматизированных систем	проведения анализа защищенности информационной инфраструктуры автоматизированных систем

3 Место дисциплины (модуля) в структуре образовательной программы

Дисциплина «Оценка рисков информационной безопасности автоматизированных систем» изучается на 5 курсе(ах) в 9 семестре(ах).

Дисциплина входит в состав блока 1 «Дисциплины (модули)» и относится к базовой части.

Для освоения дисциплины необходимы знания, умения, навыки и (или) опыт практической деятельности, сформированные в процессе изучения дисциплин «Стандартизация защищенных автоматизированных систем», Учебная практика (учебно-лабораторный практикум).

Знания, умения и навыки, сформированные при изучении дисциплины «Оценка рисков информационной безопасности автоматизированных систем», будут востребованы при изучении последующих дисциплин: Организация и технология защиты информации в распределенных информационных системах

Дисциплина «Оценка рисков информационной безопасности автоматизированных систем» частично реализуется в форме практической подготовки. Практическая подготовка организуется путем выполнения лабораторных работ.

Дисциплина «Оценка рисков информационной безопасности автоматизированных систем» в рамках воспитательной работы направлена на формирование у обучающихся умения аргументировать, самостоятельно мыслить, развивает профессиональные умения, ответственности за выполнение учебно-производственных заданий, проводить мониторинг защищенности информации в автоматизированных системах и оценку рисков информационной безопасности автоматизированных систем.

4 Объем дисциплины (модуля) в зачетных единицах с указанием количества академических часов, выделенных на контактную работу обучающихся с преподавателем (по видам учебных занятий) и на самостоятельную работу обучающихся

Общая трудоемкость (объем) дисциплины составляет 4 з.е., 144 акад. час.

Распределение объема дисциплины (модуля) по видам учебных занятий представлено в таблице 2.

Таблица 2 – Объем дисциплины (модуля) по видам учебных занятий

Объем дисциплины	**Всего академических часов**
Общая трудоемкость дисциплины	144
Контактная аудиторная работа обучающихся с преподавателем (по видам учебных занятий), всего	48
В том числе:	
занятия лекционного типа (лекции и иные учебные занятия, предусматривающие преимущественную передачу учебной информации педагогическими работниками)	16
занятия семинарского типа (семинары, практические занятия, практикумы, лабораторные работы, коллоквиумы и иные аналогичные занятия)	32
Самостоятельная работа обучающихся и контактная работа, включающая групповые консультации, индивидуальную работу обучающихся с преподавателями (в том числе индивидуальные консультации); взаимодействие в электронной информационно-образовательной среде вуза	60
Промежуточная аттестация обучающихся – Экзамен	36

5 Содержание дисциплины (модуля), структурированное по темам (разделам) с указанием отведенного на них количества академических часов и видов учебной работы

Таблица 3 – Структура и содержание дисциплины (модуля)

Наименование разделов, тем и содержание материала	Виды учебной работы, включая самостоятельную работу обучающихся и трудоемкость (в часах)			
	Контактная работа преподавателя с обучающимися			СРС
	Лекции	Семинарские (практические занятия)	Лабораторные занятия	
Раздел 1Классификация и идентификация рисков информационной безопасности автоматизированных систем	6		16	25
Раздел 2 Методы оценки рисков информационной безопасности	10		16	35

Наименование разделов, тем и содержание материала	Виды учебной работы, включая самостоятельную работу обучающихся и трудоемкость (в часах)			
	Контактная работа преподавателя с обучающимися			СРС
	Лекции	Семинарские (практические занятия)	Лабораторные занятия	
автоматизированных систем				
ИТОГО по дисциплине	**16**		**32**	**60**

6 Внеаудиторная самостоятельная работа обучающихся по дисциплине (модулю)

При планировании самостоятельной работы студенту рекомендуется руководствоваться следующим распределением часов на самостоятельную работу (таблица 4):

Таблица 4 – Рекомендуемое распределение часов на самостоятельную работу

Компоненты самостоятельной работы	Количество часов
Изучение теоретических разделов дисциплины	20
Подготовка к занятиям семинарского типа	20
Подготовка и оформление РГР	20
	60

7 Оценочные средства для проведения текущего контроля и промежуточной аттестации обучающихся по дисциплине (модулю)

Фонд оценочных средств для проведения текущего контроля успеваемости и промежуточной аттестации представлен в Приложении 1.

Полный комплект контрольных заданий или иных материалов, необходимых для оценивания результатов обучения по дисциплине (модулю), практике хранится на кафедре-разработчике в бумажном и электронном виде.

8 Учебно-методическое и информационное обеспечение дисциплины (модуля)

8.1 Основная литература

1. Скобелин С.Ю. Использование цифровых технологий при доказывании преступной деятельности / С.Ю. Скобелин // Российский следователь. 2019. N 3. С. 26 - 28.

2. Средство оценки безопасности Microsoft Security Assessment Tool / Microsoft Security Assessment Tool. Available at https://technet.microsoft.com/ru-ru/security/cc185712.aspx, accessed 08.11.2020.

3. Федеральный закон от 28.08.2004 г. No 98-ФЗ «О коммерческой тайне» / Federal Law of 28.08.2004, No 98-FZ «On Commercial Secrets» (in Russian).

4. Постановление Правительства РФ от 01.11.2012 No 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»

8.2 Дополнительная литература

1. ГОСТ Р ИСО/МЭК 27000-2021. Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Общий обзор и терминология
2. Колиснеченко, Д. Серверное применение Linux / Д. Колиснеченко, М. Матвеев, Р. Прокди – Санкт-Петербург : БХВ-Петербург, 2016. – 510 с.
3. Уильям, Р. Windows 7 для продвинутых. Настройка, работа и администрирование/ Р. Уильям – Санкт-Петербург : Питер, 2015. – 576 с.

8.3 Методические указания для студентов по освоению дисциплины

Обучение дисциплине «Оценка рисков информационной безопасности автоматизированных систем» предполагает изучение курса на аудиторных занятиях и в ходе самостоятельной работы. Аудиторные занятия проводятся в форме лекций и практических занятий.

Таблица 5 Методические указания к отдельным видам деятельности

Вид учебного занятия	Организация деятельности студента
Лекция	Написание конспекта лекций: кратко, схематично, последовательно фиксировать основные положения. Выделять ключевые слова, формулы, отмечать на полях уточняющие вопросы по теме занятия
Лабораторные занятие	Работа с автоматизированными рабочими местами.
Самостоятельная работа	Для более глубокого изучения разделов дисциплины предусмотрены отдельные виды самостоятельной работы: подготовка к практическим занятиям, изучение теоретических разделов дисциплины, подготовка РГР.

Самостоятельная работа является наиболее продуктивной формой образовательной и познавательной деятельности студента в период обучения. СРС направлена на углубление и закрепление знаний студента, развитие практических умений. СРС по дисциплине «Организация и технология защиты конфиденциальной информации в информационных системах» включает следующие виды работ:

– работу с лекционным материалом, поиск и обзор литературы и электронных источников информации по индивидуальному заданию;

– опережающую самостоятельную работу;

– изучение тем, вынесенных на самостоятельную проработку;

– подготовку к практическим занятиям;

– выполнение и оформление РГР.

Контроль самостоятельной работы студентов и качество освоения дисциплины осуществляется посредством:

– представления в указанные контрольные сроки результатов выполнения заданий

для текущего контроля;

– выполнения и защиты РГР;

8.4 Современные профессиональные базы данных и информационные справочные системы, используемые при осуществлении образовательного процесса по дисциплине

1. Электронно-библиотечная система ZNANIUM.COM – http://www. znanium.com.
2. Консультант+
3. Научная электронная библиотека Elibrary http://elibrary.ru.

8.5 Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины (модуля)

1. Сайт университета www.knastu.ru[Электронный ресурс]:. Раздел сотрудникам, документы СМК, режим доступа – свободный. Загл. с экрана
2. Научная электронная библиотека Elibrary http://elibrary.ru.

С целью повышения качества ведения образовательной деятельности в университете создана электронная информационно-образовательная среда. Она подразумевает организацию взаимодействия между обучающимися и преподавателями через систему личных кабинетов студентов, расположенных на официальном сайте университета в информационно-телекоммуникационной сети «Интернет» по адресу https://student.knastu.ru. Созданная информационно-образовательная среда позволяет осуществлять взаимодействие между участниками образовательного процесса посредством организации дистанционного консультирования по вопросам выполнения практических заданий.

8.6 Лицензионное программное обеспечение, используемое при осуществлении образовательного процесса по дисциплине

Таблица 6 – Перечень используемого программного обеспечения

Наименование ПО	Реквизиты
Microsoft® Windows Professional 7 Russian	Лицензионный сертификат № 46243844 от 09.12.2009
Open Office или аналог	Свободно-распространяемое
Операционная система Kali Linux или аналог	Свободно-распространяемое
Операционная система Ubuntu или аналог	Свободно-распространяемое
Обозреватель Google Chrome или аналог	Свободно-распространяемое

9 Организационно-педагогические условия

Организация образовательного процесса регламентируется учебным планом и расписанием учебных занятий. Язык обучения (преподавания) — русский. Для всех видов аудиторных занятий академический час устанавливается продолжительностью 45 минут.

При формировании своей индивидуальной образовательной траектории обучающийся имеет право на перезачет соответствующих дисциплин и

профессиональных модулей, освоенных в процессе предшествующего обучения, который освобождает обучающегося от необходимости их повторного освоения.

9.1 Образовательные технологии

Учебный процесс при преподавании курса основывается на использовании традиционных, инновационных и информационных образовательных технологий. Традиционные образовательные технологии представлены лекциями и семинарскими (практическими) занятиями. Инновационные образовательные технологии используются в виде широкого применения активных и интерактивных форм проведения занятий. Информационные образовательные технологии реализуются путем активизации самостоятельной работы студентов в информационной образовательной среде.

9.2 Занятия лекционного типа

Лекционный курс предполагает систематизированное изложение основных вопросов учебного плана.

На первой лекции лектор обязан предупредить студентов, применительно к какому базовому учебнику (учебникам, учебным пособиям) будет прочитан курс.

Лекционный курс должен давать наибольший объем информации и обеспечивать более глубокое понимание учебных вопросов при значительно меньшей затрате времени, чем это требуется большинству студентов на самостоятельное изучение материала.

9.3 Занятия семинарского типа

Семинарские занятия представляют собой детализацию лекционного теоретического материала, проводятся в целях закрепления курса и охватывают все основные разделы.

Основной формой проведения семинаров является обсуждение наиболее проблемных и сложных вопросов по отдельным темам, а также разбор примеров и ситуаций в аудиторных условиях. В обязанности преподавателя входят: оказание методической помощи и консультирование студентов по соответствующим темам курса.

Активность на семинарских занятиях оценивается по следующим критериям:

· ответы на вопросы, предлагаемые преподавателем;

· участие в дискуссиях;

· выполнение проектных и иных заданий;

· ассистирование преподавателю в проведении занятий.

Ответ должен быть аргументированным, развернутым, не односложным, содержать ссылки на источники.

Доклады и оппонирование докладов проверяют степень владения теоретическим материалом, а также корректность и строгость рассуждений.

Оценивание заданий, выполненных на семинарском занятии, входит в накопленную оценку.

9.4 Самостоятельная работа обучающихся по дисциплине (модулю)

Самостоятельная работа студентов – это процесс активного, целенаправленного приобретения студентом новых знаний, умений без непосредственного участия преподавателя, характеризующийся предметной направленностью, эффективным контролем и оценкой результатов деятельности обучающегося.

Цели самостоятельной работы:

· систематизация и закрепление полученных теоретических знаний и практических умений студентов;

· углубление и расширение теоретических знаний;

· формирование умений использовать нормативную и справочную документацию, специальную литературу;

· развитие познавательных способностей, активности студентов, ответственности и организованности;

· формирование самостоятельности мышления, творческой инициативы, способностей к саморазвитию, самосовершенствованию и самореализации;

· развитие исследовательских умений и академических навыков.

Самостоятельная работа может осуществляться индивидуально или группами студентов в зависимости от цели, объема, уровня сложности, конкретной тематики.

Технология организации самостоятельной работы студентов включает использование информационных и материально-технических ресурсов университета.

Контроль результатов внеаудиторной самостоятельной работы студентов может проходить в письменной, устной или смешанной форме.

Студенты должны подходить к самостоятельной работе как к наиважнейшему средству закрепления и развития теоретических знаний, выработке единства взглядов на отдельные вопросы курса, приобретения определенных навыков и использования профессиональной литературы.

9.5 Методические указания для обучающихся по освоению дисциплины

При изучении дисциплины обучающимся целесообразно выполнять следующие рекомендации:

1. Изучение учебной дисциплины должно вестись систематически.

2. После изучения какого-либо раздела по учебнику или конспектным материалам рекомендуется по памяти воспроизвести основные термины, определения, понятия раздела.

3. Особое внимание следует уделить выполнению отчетов по практическим занятиям и индивидуальным комплексным заданиям на самостоятельную работу.

4. Вся тематика вопросов, изучаемых самостоятельно, задается на лекциях преподавателем. Им же даются источники (в первую очередь вновь изданные в периодической научной литературе) для более детального понимания вопросов, озвученных на лекции.

При самостоятельной проработке курса обучающиеся должны:

· просматривать основные определения и факты;

· повторить законспектированный на лекционном занятии материал и дополнить его с учетом рекомендованной по данной теме литературы;

· изучить рекомендованную литературу, составлять тезисы, аннотации и конспекты наиболее важных моментов;

· самостоятельно выполнять задания, аналогичные предлагаемым на занятиях;

· использовать для самопроверки материалы фонда оценочных средств.

1. Методические указания при работе над конспектом лекции

В ходе лекционных занятий необходимо вести конспектирование учебного материала. Обращать внимание на категории, формулировки, раскрывающие содержание тех или иных явлений и процессов, научные выводы и практические рекомендации, положительный опыт в ораторском искусстве. Желательно оставить в рабочих конспектах поля, на которых делать пометки из рекомендованной литературы, дополняющие материал прослушанной лекции, а также подчеркивающие особую важность тех или иных теоретических положений. Задавать преподавателю уточняющие вопросы с целью уяснения теоретических положений, разрешения спорных ситуаций.

2. Методические указания по самостоятельной работе над изучаемым материалом и при подготовке к лабораторным занятиям

Начинать надо с изучения рекомендованной литературы. Необходимо помнить, что на лекции обычно рассматривается не весь материал, а только его часть. Остальная его часть восполняется в процессе самостоятельной работы. В связи с этим работа с рекомендованной

литературой обязательна. Особое внимание при этом необходимо обратить на содержание основных положений и выводов, объяснение явлений и фактов, уяснение практического приложения рассматриваемых теоретических вопросов. В процессе этой работы необходимо стремиться понять и запомнить основные положения рассматриваемого материала, примеры, поясняющие его, а также разобраться в иллюстративном материале. Оформлять отчеты следует руководствуясь внутренними нормативными документами КнАГУ.

3. Методические указания для выполнения лабораторных работ и РГР

ЛАБОРАТОРНАЯ РАБОТА № 1

Название работы

Организация консалтинговой компании

Цель

Познакомиться на практике с организационной структурой компании по проведению аудиту информационной безопасности предприятия.

Программно-аппаратные средства

Компьютерная лаборатория, стандартные средства Microsoft Office.

Понятийный аппарат

Консалтинг — деятельность по консультированию производителей, продавцов, покупателей по широкому кругу вопросов в сфере технологической, технической, экспертной деятельности. Цель консалтинга — помочь менеджменту в достижении заявленных целей[16]. Консалтинговые компании специализируются по отдельным направлениям деятельности (например, финансовом, организационном, стратегическом)

Основная задача консалтинга заключается в анализе, обосновании перспектив развития и использования научно-технических и организационно-экономических инноваций с учетом предметной области и проблем клиента. Иными словами, консалтинг - это любая помощь, оказываемая внешними консультантами, в решении той или иной проблемы.

Информационная безопасность (ИБ) некоторой ИС – это уровень ее защищенности от случайного или преднамеренного вмешательства в

нормальный процесс функционирования, а также от попыток хищения, изменения или разрушения их компонентов.

Система защиты информации (СЗИ) – это система, обеспечивающая информационную безопасность некоторой ИС.

Аудит информационной безопасности – это системный процесс получения объективных качественных и количественных оценок текущего состояния информационной безопасности некоторой информационной системы, в соответствии с определенными критериями и показателями безопасности.

Конфиденциальность (Confidentiality of Information) – это свойство информации быть известной только допущенным пользователям ИС.

Целостность (Integrity of Information) – это свойство информации быть неизменной в семантическом отношении.

Доступность (Availability of Information) – это свойство информации быть свободной на доступ в определенный момент времени.

Доступ к информации (Access to Information) – возможность ознакомления с информацией, ее обработка. Например, чтение, копирование, модификация или уничтожение информации.

Целостность, конфиденциальность и доступность ресурсов ИС вполне возможно измерять, например, на качественных шкалах, привлекая экспертов.

ОБЩИЕ СВЕДЕНИЯ

Круг проблем, решаемых консалтингом, весьма широк, кроме того, специализация компаний, предоставляющих консалтинговые услуги, может быть различной: от узкой, ограничивающейся каким-либо одним направлением консалтинговых услуг (например, аудит), до самой широкой, охватывающей полный спектр услуг в этой области. Соответственно этому, каждый специалист (или каждая фирма), работающая в данной области, вкладываете понятие консалтинга собственный смысл и придает ему

собственный оттенок, определяемый направлением деятельности конкретной компании.

Итак, Консалтинг - это вид интеллектуальной деятельности, основная задача которого заключается в анализе, обосновании перспектив развития и использования научно-технических и организационно-экономических инноваций с учетом предметной области и проблем клиента.

Консалтинг решает вопросы управленческой, экономической, финансовой, инвестиционной деятельности организаций, стратегического планирования, оптимизации общего функционирования компании, ведения бизнеса, исследования и прогнозирования рынков сбыта, движения цен и т.д. Иными словами, консалтинг - это любая помощь, оказываемая внешними консультантами, в решении той или иной проблемы.

Основная цель консалтинга заключается в улучшении качества руководства, повышении эффективности деятельности компании в целом и увеличении индивидуальной производительности труда каждого работника.

Согласно распространенному мнению, к услугам внешних консультантов обращаются в основном и в первую очередь те организации, которые оказались в критическом положении. Однако помощь в критических ситуациях - отнюдь не основная функция консалтинга.

КОНТРОЛЬНЫЕ ВОПРОСЫ

1. Что такое консалтинг?
2. Какова основная задача консалтинга?
3. Что понимают под информационной безопасностью?
4. Что представляет собой система защиты информации?
5. Что понимают под аудитом ИБ?
6. Перечислите основные свойства информации.
7. Каковы способы измерения свойств информации?

ЗАДАНИЕ НА ЛАБОРАТОРНУЮ РАБОТУ № 1

Название работы

Организация консалтинговой компании

Задание

1. Изучить основной теоретический материал
2. Создать структурную модель консалтинговой компании.
3. Провести организационные мероприятия по подготовке проведения аудита.
4. Уточнить цели и задачи аудита
5. Сформировать рабочую группу
6. Подготавливается и согласовывается техническое задание на проведение аудита компании (по вариантам).
7. Собирать информацию и дать оценку следующих мер и средств:
   - ✓ организационных мер в области информационной безопасности;
   - ✓ программно-технических средств защиты информации;
   - ✓ обеспечения физической безопасности.

Структура основной части отчета

1. Структура и описание консалтинговой компании.
2. Перечень услуг консалтинговой компании.
3. Состав рабочей группы:
4. Цели и задачи аудита ИБ:
5. Техническое задание:
6. Придумать или использовать реальную ИС некоторой организации (по вариантам).
7. Исходные данные о заказчике:
8. Выводы по результатам анализа исходных данных от заказчика
9. Ответы на контрольные вопросы:

ЛАБОРАТОРНАЯ РАБОТА № 2

Название работы

Табличные методы оценки и анализа информационных рисков.

Цель

Познакомиться на практике с табличными методами оценки и анализа рисков информационной безопасности.

Программно-аппаратные средства

Компьютерная лаборатория, стандартные средства Microsoft Office.

Понятийный аппарат

Система – это совокупность технических средств, людей и бизнес-процессов, совместное использование которых способствует достижению определенных целей (согласно ГОСТ 34).

Информационная система (ИС) – это любая система (например, компьютерная – КИС – включающая в себя мейнфреймы, локальные сети, узлы доступа, компьютеры), или программное обеспечение (ПО, запущенное в рамках системы), которые используют информационные ресурсы для удовлетворения нужд собственника или пользователей системы.

Риск информационной безопасности – это возможные потери собственника ИС, связанные с реализацией некоторой угрозы через одну или несколько уязвимостей ИС или СЗИ.

Угроза ИБ (Threat) – составляющая риска, которая определяет совокупность условий и факторов, которые прямо или косвенно могут стать причиной нарушения целостности, доступности или конфиденциальности информации, обрабатываемой некоторой ИС, или выхода из строя элемента или всей системы в целом.

Уязвимость (Vulnerability) – составляющая риска, которая определяет некоторое «неудачное» свойство СЗИ или ИС, дающее возможность реализовать ту или иную угрозу ИБ.

Определение риска – это процесс выявления риска, а также его составляющих: угроз и уязвимостей.

Оценка риска – это процесс определения шкал, критериев и измерения по ним существующих рисков. Оценка рисков используется для определения растущего потенциала угроз и рисков, ассоциированных с ИС. Для оценки рисков, как правило, применяют косвенные шкалы, критерии для которых бывают объективными (например, вероятность выхода из строя некоторого узла оборудования в течение определенного срока), либо субъективными (например, оценка владельцем информационного ресурса уровня риска выхода из строя некоторого узла инфосистемы).

Анализ риска – это процесс определения и оценки риска ИБ некоторой информационной системы, проведенный по одной из существующих методик.

Управление рисками – это процесс анализа рисков и выполнение некоторых действий ведущих к снижению рисков до приемлемого уровня.

Подходы к оценке, анализу и управлению рисками ИБ

В настоящее время важнейшими задачами, стоящими перед руководителями, ответственными за организацию режима информационной безопасности (ИБ), является задача оценивания, анализа и управления информационными рисками (ИР). Для решения этих задач необходимо ответить на следующие вопросы:

1. На какие критерии и показатели необходимо опираться при проведении оценивания системы защиты информации?
2. Как оценить информационные риски предприятия?
3. Какую методику выбрать для анализа и управления рисками применительно к конкретной организации?

Для ответа на эти вопросы и решения задач обеспечения ИБ в технологически развитых странах появилось новое поколение стандартов информационной безопасности, посвященных практическим вопросам организации режима ИБ в организациях. Это международные и национальные стандарты оценки и управления информационной

безопасностью: ISO 15408, ISO 17799, BS 7799, BSI, а также стандарты аудита, в определенной степени отражающие вопросы ИБ: COBIT, SAC, COSO, SAS 55178 и др.

В соответствии с этими стандартами организация режима ИБ организации состоит из следующих этапов:

1. Постановка целей обеспечения ИБ организации.
2. Создание эффективной системы управления ИБ.
3. Расчет качественных и количественных показателей для оценки соответствия ИБ поставленным целям.
4. Применение инструментария обеспечения ИБ и оценки ее текущего состояния.
5. Использование некоторой методики с разработанной системой критериев и мер обеспечения ИБ, в процессе анализа и управления рисками информационной безопасности для обеспечения текущего состояния дел в организации.

Ключевым моментом деятельности системы информационной безопасности является обеспечение достоверности всех информационных процессов организации, так как руководство современной компании по существу имеет дело только с информацией и на ее основе принимает решение. Однако на обеспечение ИБ нельзя потратить все деньги организации, поэтому необходимо выяснить разумную стоимость системы защиты информации (СЗИ). Выделяют следующие подходы к оценке стоимости СЗИ:

1. Наукообразный подход – заключается в том, чтобы создать инструменты оценивания стоимости защищаемой информации (например, с помощью экспертных систем), привлекая для этого организацию, как собственника информации, с целью оценивания стоимости информационных ресурсов, выделению существенных для данной организации угроз и уязвимостей, определения вероятности

их реализации, определение ущерба. Существенно, что при этом организация сама осознает проблему сохранности своей информации.

2. Практический подход – эксперты-практики в области ИБ выделили оптимальный вариант затрат на обеспечение ИБ организации, а именно: стоимость СЗИ должна составлять примерно 10-20% от стоимости самой информационной системы организации. Этот подход дает возможность заранее спрогнозировать затраты на обеспечение ИБ.

В анализе рисков, по любой известной методике, естественное требование состоит в определении рисков и их составляющих – угроз и уязвимостей. При этом возникает требование полноты составленного списка классов рисков. В ряде руководств по ИБ такие списки приводятся. Например, в германском стандарте BSI, имеется каталог угроз для различных элементов информационных систем (ИС). Положительный момент от использования таких списков состоит в их полноте, т.к. классы угроз обычно исчисляются десятками, они достаточно широки и покрывают все существующее множество рисков. Отрицательный момент заключается в сложности оценки уровня рисков и подбора эффективных контрмер для конкретного класса рисков. В связи с этим, оценивание рисков обычно проводят по отдельным, конкретным подклассам рисков.

После определения рисков, определяются шкалы и критерии по которым они измеряются. Шкалы могут быть прямыми (например, шкалы измерения физических величин) и косвенными (например, шкала измерения субъективного свойства «ценность информационного ресурса»). Для оценки рисков прямые шкалы как правило не применяются.

Критерии для оценки рисков бывают объективными (например, вероятность выхода из строя некоторого узла оборудования в течение определенного срока), либо субъективными (например, оценка владельцем информационного ресурса уровня риска выхода из строя некоторого узла инфосистемы).

В методиках анализа рисков ИБ обычно применяют субъективные критерии, для измерения которых используют качественные шкалы. Это связано с тем, что оценка риска должна отражать субъективную точку зрения владельца информационных ресурсов, а также учитывать не только техническую, но и организационную и правовую стороны обеспечения ИБ.

Для правильного оценивания рисков очень важно рассчитать вероятность того или иного события. Применительно к оценке рисков ИБ используют два толкования вероятности: вероятность бывает объективная и субъективная. Под объективной вероятностью понимается относительная частота появления какого-либо события в общем объеме наблюдений. Этот подход применяется при анализе результатов большого числа наблюдений. Под субъективной вероятностью понимается мера уверенности эксперта (или нескольких экспертов) в том, что данное событие произойдет.

Для оценки рисков ИБ существует ряд подходов. Наиболее распространенные из них – оценка рисков по двум и трем факторам.

Суть оценки рисков по двум факторам заключается в том, что риск тем больше, чем больше вероятность инцидента и ущерб причиненный им. Данную оценку можно выразить формулой:

$$R = P_I \circ C,$$

где R (Risk) – значение риска, P_I (Incident Probability) – вероятность инцидента, C (Cost) – возможный ущерб, наносимый ИС при конкретном инциденте (обычно в денежном эквиваленте). Если P и C – количественные величины, то символ $\circ$ – обозначает обычную операцию умножения и R – это математическое ожидание потерь. Если переменные – качественные величины, то умножение не определено и для расчета уровня риска обычно строят таблицы рисков.

Второй подход к оценке рисков, заключается в использовании методик учитывающих три фактора: угроза, уязвимость, ущерб.

В основе методов оценки угроз и уязвимостей могут лежать:

1. Экспертные системы.
2. Статистические данные.
3. Учет факторов, влияющие на уровни угроз и уязвимостей.

При трехфакторном подходе оценку риска можно выразить формулой:

$$R = P_I \circ C,$$

$$P_I = P_T \cdot P_V,$$

где P_T (Threat Probability) – вероятность угрозы, P_V (Vulnerability Probability) – вероятность уязвимости. Аналогично, как в предыдущем подходе, символ $\circ$ – обозначает обычную операцию умножения, в случае если измерительные шкалы количественные. В ином случае, вновь прибегают к табличному способу оценки рисков, но уже в зависимости от трех факторов.

ТАБЛИЧНЫЕ МЕТОДЫ ОЦЕНКИ И АНАЛИЗА РИСКОВ ИБ

В настоящее время известно множество табличных методов оценки рисков ИБ организации. Важно, чтобы организации сама выбрала для себя подходящий метод, который обеспечивал бы корректные и достоверные воспроизводимые результаты.

Рассмотрим некоторые методы, которые рекомендованы международными стандартами информационной безопасности, главным образом ISO 17799 (BS 7799). Существенно, что в них количественные показатели существующих или предлагаемых физических ресурсов компании оцениваются с точки зрения стоимости их замены или восстановления работоспособности ресурса, то есть количественными методами. А существующие или предполагаемые программные ресурсы оцениваются так же, как и физические, то есть при помощи определения затрат на их приобретение или восстановление количественными методами.

Если обнаружится, что какое-либо прикладное ПО имеет особые требования к конфиденциальности или целостности, например, исходный текст имеет высокую коммерческую ценность, то оценка этого ресурса производится в количественном выражении по той же схеме, что и для информационных ресурсов.

Количественные показатели информационных ресурсов (ИР) рекомендуется оценивать по результатам опросов сотрудников компании – владельцев информации, то есть должностных лиц компании, которые могут определить ценность информации, ее характеристики и степень критичности, исходя из фактического положения дел. На основе результатов опроса производится оценивание показателей и степени критичности ИР для наихудшего варианта развития событий, вплоть до рассмотрения потенциальных воздействий на бизнес-процессы организации, при возможном несанкционированном ознакомлении с конфиденциальной информацией, нарушении ее целостности, недоступности на различные сроки, вызванных отказами в обслуживании систем обработки данных и даже физическом уничтожении. При этом процесс получения количественных показателей может дополняться соответствующими методиками оценивания других критически важных ресурсов компании, учитывающих:

1. Безопасность персонала.
2. Разглашение частной информации.
3. Требования по соблюдению законодательных и нормативных положений.
4. Ограничения, вытекающие из законодательства.
5. Коммерческие и экономические интересы.
6. Финансовые потери и нарушения в производственной деятельности.
7. Общественные отношения.
8. Коммерческая политика и коммерческие операции.
9. Потеря репутации компании.

Далее количественные показатели используются там, где это допустимо и оправдано, а качественные – там, где количественные оценки по ряду причин затруднены. Наибольшее распространение получило оценивание качественных показателей при помощи специально разработанных числовых шкал, аналогичных рассмотренной далее

Следующей операцией является заполнение пар опросных листов, в которых по каждому из типов угроз и связанных с ним группе ресурсов оцениваются вероятности реализации угроз, уровни угроз и уровни уязвимостей как степень легкости, с которой реализованная угроза способна привести к негативному воздействию. Оценивание производится в качественных шкалах. Например, уровень угроз и уязвимостей оценивается по шкале «высокий-низкий».

Необходимую информацию собирают, опрашивая топ-менеджеров компании, сотрудников коммерческих, технических, кадровых и сервисных служб, выезжая на места и анализируя документацию компании.

Пример проведения табличной оценки рисков

Проведем анализ следующих типов угроз ИБ для некоторой организации:

1. Умышленные несанкционированные действия людей.
2. Непредвиденные случайности.
3. Ошибки со стороны персонала.
4. Нарушение работоспособности оборудования, ошибки в ПО и отказы средств связи.

Далее составляется перечень ИР. Для каждого ресурса перечисляются относящиеся к нему уязвимости и соответствующие им угрозы. Если существует уязвимость без связанной с ней угрозы, или существует угроза, не связанная с какими-либо уязвимостями, то рисков нет. Но и эти случаи следует предусмотреть.

Относящиеся к каждому типу негативных воздействий уровни рисков, соответствующих показателям ценности ресурсов, показателям угроз и уязвимостей, оцениваются при помощи таблицы, аналогичной таблице 1.

Показатель ценности ресурса (для каждого ресурса и угрозы)	Уровень угрозы (вероятность ее осуществления)								
	Низкий (Н)			Средний (С)			Высокий (В)		
	Уровень уязвимости			Уровень уязвимости			Уровень уязвимости		
	Н	С	В	Н	С	В	Н	С	В
0	0	1	2	1	2	3	2	3	4
1	1	2	3	2	3	4	3	4	5
2	2	3	4	3	4	5	4	5	6
3	3	4	5	4	5	6	5	6	7
4	4	5	6	5	6	7	6	7	8

Таблица 1. Уровни рисков, соответствующие показателям ценности ресурсов, угроз и уязвимостей.

Количественный показатель риска определяется в шкале от 1 до 8 и вносится в соответствующую ячейку таблицы. Каждая строка в таблице определяет показатель ценности ресурса, а каждый столбец – степень опасности угрозы и уязвимости для ресурса. Например, ресурс имеет показатель ценности – 3, угроза имеет степень – «высокая», а уязвимость – «низкая». Показатель риска в этом случае будет равен – 5. Размер таблицы, учитывающей количество степеней опасности угроз, степеней опасности уязвимостей и категорий ценности ресурсов, может быть изменен в соответствии со спецификой конкретной организации.

Описанный подход определяется классификацией рассматриваемых рисков. После того, как оценивание рисков было выполнено первый раз, его результаты целесообразно сохранить, например, в базе данных. Эта мера в дальнейшем позволит легко повторить последующее оценивание рисков компании.

Ранжирование угроз

В матрице или таблице можно наглядно отразить связь между угрозами, негативными воздействиями и возможностями их реализации. Для этого нужно выполнить следующие шаги.

На первом шаге оценить показатель негативного воздействия по заранее определенной шкале, например, от 1 до 5, для каждого ресурса, которому угрожает опасность.

На втором шаге по заранее заданной шкале, например, также от 1 до 5, оценить вероятность реализации каждой угрозы.

На третьем шаге вычислить показатель риска путем перемножения чисел в колонках II и III, по которому и производится ранжирование угроз.

В этом примере (таблица 2) для наименьшего негативного воздействия и для наименьшей вероятности реализации выбран показатель 1.

I Описание угрозы	II Показатель негативного воздействия	III Вероятность реализации угрозы	IV Показатель риска	V Ранг угрозы
Угроза A	5	2	10	2
Угроза B	2	4	8	3
Угроза C	3	5	15	1
Угроза D	1	3	3	5
Угроза E	4	1	4	4
Угроза F	2	4	8	3

Таблица 2. Ранжирование угроз.

Данная процедура позволяет сравнивать и ранжировать по приоритету угрозы с различными негативными воздействиями и возможностями реализации. В определенных случаях дополнительно могут потребоваться стоимостные показатели.

Оценка негативного воздействия угрозы

Эта задача решается при помощи оценивания двух значений: ценности ресурса и частоты повторяемости риска.

Сначала каждому ресурсу присваивается определенное значение, соответствующее потенциальному ущербу от воздействия угрозы. Такие показатели присваиваются ресурсу по отношению ко всем возможным угрозам. Суммированием баллов всех ресурсов анализируемой ИС определяется количественный показатель риска для всей системы.

Далее оценивается показатель частоты повторяемости риска. Частота зависит от вероятности возникновения угрозы и степени легкости, с которой

может быть использована уязвимость (уровень уязвимости). В результате получается таблица, аналогичная таблице 3.

Уровень угрозы (вероятность ее осуществления)								
Низкий			Средний			Высокий		
Уровень уязвимости			Уровень уязвимости			Уровень уязвимости		
Н	С	В	Н	С	В	Н	С	В
0	1	2	1	2	3	2	3	4

Таблица 3. Показатель частоты повторяемости риска.

Затем определяется показатель пары ресурс/угроза. На каждую пару ресурс/угроза составляется таблица, аналогичная таблице 4, в которой суммируются показатель ценности ресурса и показатель угрозы. Фактически таблица представляет собой матрицу, элементы которой равны сумме номеров строки и столбца конкретного элемента. Эту таблицу можно использовать в дальнейшем, для обоснования критичности того или иного ресурса – чем больше показатель пары ресурс/угроза, тем более критичен ресурс и на его защиту следует обратить больше внимания, на этапе управления рисками.

Показатель ценности ресурса	Показатель частоты повторяемости риска				
	0	**1**	**2**	**3**	**4**
0	0	1	2	3	4
1	1	2	3	4	5
2	2	3=2+1	4	5	6
3	3	4	5=3+2	6	7
4	4	5	6	7	8

Таблица 4. Показатели пары ресурс/угроза.

На заключительном этапе суммируются все итоговые баллы по всем ресурсам ИС и формируется ее общий балл. Его можно использовать для выявления тех элементов системы, защита которых должна быть приоритетной.

Разделение рисков на приемлемые и неприемлемые

Дополнительный способ оценивания рисков состоит в их разделении на допустимые и недопустимые. Возможность применения подобного подхода основывается на том, что количественные показатели рисков используются

только для того, чтобы их упорядочить и определить, какие действия необходимы в первую очередь. Этого можно достичь и с меньшими затратами.

Таблица, используемая в данном подходе, содержит не числа, а только символы Д (риск допустим) и Н (риск недопустим). Например, может быть использована таблица, аналогичная таблице 5.

Показатель ценности ресурса	**Показатель частоты повторяемости риска**				
	0	**1**	**2**	**3**	**4**
0	Д	Д	Д	Д	Н
1	Д	Д	Д	Н	Н
2	Д	Д	Н	Н	Н
3	Д	Н	Н	Н	Н
4	Н	Н	Н	Н	Н

Таблица 5. Разделение рисков на приемлемые и неприемлемые.

При этом вопрос о том, как провести границу между допустимыми и недопустимыми рисками, как правило, предлагается решить топ-менеджерам, ответственным за организацию информационной безопасности организации.

КОНТРОЛЬНЫЕ ВОПРОСЫ

1. Что понимают под информационной системой?
2. Что представляет собой система защиты информации?
3. Что такое риск ИБ, угроза, уязвимость?
4. Что представляет собой определение, оценка, анализ и управление рисками ИБ?
5. Опишите подходы к оценке, анализу и управлению рисками ИБ.
6. Опишите двух- и трехфакторный подходы к оцениванию информационных рисков.
7. Опишите табличные методы оценивания рисков ИБ.

ЗАДАНИЕ НА ЛАБОРАТОРНУЮ РАБОТУ № 2

Название работы

Табличные методы оценки и анализа информационных рисков.

Задание

1. Изучить основной теоретический материал лабораторной работы.
2. Изучить табличную методику оценки рисков.
3. Придумать или использовать реальную ИС некоторой организации (Из лаб. работы №1).
4. Внести структурную схему и описание вашей ИС в отчет.
5. Составить и внести в отчет перечни типов угроз ИБ и информационные ресурсы, присутствующие в данной ИС.
6. По изученной методике оценить риски ИБ данной ИС (аналогично таблице 1).
7. Выполнить ранжирование угроз ИБ вашей ИС (аналогично таблице 2).
8. Определить показатель частоты повторяемости риска (аналогично таблице 3).
9. Определить показатели пары ресурс/угроза (аналогично таблице 4).
10. Выполнить разделение рисков ИБ на приемлемые и неприемлемые (аналогично таблице 5). Как вы провели границу между допустимыми и недопустимыми рисками?
11. Сделайте выводы по результатам анализа вашей ИС.
12. Внести ответы на контрольные вопросы в отчет.

Структура основной части отчета

1. Структура и описание ИС (Из лаб. работы №1).
2. Перечень типов угроз:
3. Перечень ИР:
4. Оценка риска (таблица 1):
5. Ранжирование угроз (таблица 2):
6. Показатель частоты повторяемости риска (таблица 3):
7. Показатель пары ресурс/угроза (таблица 4):
8. Разделение рисков на приемлемые и неприемлемые (таблица 5):
9. Выводы по результатам анализа ИС
10. Ответы на контрольные вопросы:

ЛАБОРАТОРНАЯ РАБОТА № 3

Название работы

Расчет рисков информационной безопасности.

Цель

Познакомиться на практике с методом расчета рисков ИБ на основе модели анализа угроз и уязвимостей

Программно-аппаратные средства

Компьютерная лаборатория, стандартные средства Microsoft Office

Понятийный аппарат

На данном этапе развития предметной области «оценка, анализ и управление рисками ИБ» существует множество методик, позволяющих качественно или количественно оценить защищенность информационной системы (ИС) организации. Рассмотрим методику оценки риска, основанной на построении модели угроз, уязвимостей и расчете общего риска для каждого ресурса ИС. Сначала перечислим и дополним некоторые из основных понятий этой модели.

Информационная система (ИС, Information System) – это любая система (например, компьютерная – КИС – включающая в себя мейнфреймы, локальные сети, узлы доступа, компьютеры и т.д.), или программа (запущенная в рамках системы), которая использует информационные ресурсы для удовлетворения нужд собственника или пользователя системы. Любая информационная система предлагает пользователям определенный набор услуг (сервисов).

Информация, информационные ресурсы (Information Resources) – это данные в любом виде, которые можно использовать для решения определенных задач, поставленных владельцем или пользователем системы. Например, информационным ресурсом может считаться книга, бумажный документ, любой файл (электронный документ, изображение, видеофайл, база данных), а также отдельно взятый сайт или полностью портал.

В исходной методике свойствами ресурса являются лишь: перечень угроз, воздействующих на него, и критичность ресурса. Однако с каждым информационным ресурсом напрямую связан некоторый носитель информации. Также, любой информационный ресурс (любую информацию) можно охарактеризовать такими свойствами, как время жизни, актуальность, конфиденциальность, целостность и доступность. Схема взаимодействия элементов модели предметной области «оценка, анализ и управление рисками ИБ» изображена на рис. 1.

Рис. 1. Основные компоненты общей модели предметной области «оценка, анализ и управление рисками ИБ».

Угроза ИБ (Threat) – составляющая риска, которая определяет совокупность условий и факторов, которые прямо или косвенно могут стать причиной нарушения целостности, доступности или конфиденциальности информации, обрабатываемой некоторой ИС, или выхода из строя элемента или всей системы в целом. Применительно к ИС также используют понятие ***базовые угрозы ИБ*** (Base Threats) – это нарушение конфиденциальности,

целостности или доступности информации, обрабатываемой ИС, или информационного ресурса. В исходной методике свойствами угрозы является перечень уязвимостей, при помощи которой она может быть реализована.

Уязвимость (Vulnerability) – составляющая риска, которая определяет некоторое «неудачное» свойство СЗИ или ИС, дающее возможность реализовать ту или иную угрозу ИБ. В исходной методике от Digital Security уязвимость характеризуется свойствами: вероятность реализации угрозы через данную уязвимость и критичность реализации угрозы ИБ.

Инцидент ИБ (Incident) – факт реализации угрозы ИБ.

Критичность информационного ресурса – степень значимости ресурса для ИС. Т.е. как сильно реализация угроз ИБ повлияет на работу ИС в целом. Задать критичность ресурса (AC) можно в уровнях, на шкале от 1 до 100, или в денежном эквиваленте. Также можно задать критичность ресурса отдельно по конфиденциальности, целостности и доступности (AC_c, AC_i, AC_a).

Критичность реализации угрозы ИБ – степень влияния реализации угрозы ИБ на работу ресурса. Критичность реализации (ER) можно задать в процентах. Также можно задать критичность ресурса отдельно по конфиденциальности, целостности и доступности (ER_c, ER_i, ER_a).

Вероятность реализации угрозы через данную уязвимость в течение года (P(V)) – степень возможности реализации угрозы через данную уязвимость в тех или иных условиях. Указывается в процентах.

Максимальное критичное время простоя (T_{max}) – значение времени простоя, которое является критичным для организации. Т.е. ущерб, нанесенный организации при простаивании ресурса в течение критичного времени простоя, максимальный. При простаивании ресурса в течение времени, превышающего критичное, ущерб, нанесенный организации, не увеличивается.

Риск информационной безопасности – это возможные потери собственника ИС, связанные с реализацией некоторой угрозы через одну или несколько уязвимостей ИС или СЗИ.

Определение риска – это процесс выявления риска, а также его составляющих: угроз и уязвимостей.

Оценка риска – это процесс определения шкал, критериев и измерения по ним существующих рисков. Оценка рисков используется для определения растущего потенциала угроз и рисков, ассоциированных с ИС. Для оценки рисков, как правило, применяют косвенные шкалы, критерии для которых бывают объективными (например, вероятность выхода из строя некоторого узла оборудования в течение определенного срока), либо субъективными (например, оценка владельцем информационного ресурса уровня риска выхода из строя некоторого узла инфосистемы).

Анализ риска (Risk Analysis) – это процесс определения и оценки риска ИБ некоторой информационной системы, проведенный по одной из существующих методик.

Управление рисками (Risk Management) – это процесс анализа рисков и выполнение некоторых действий ведущих к снижению рисков до приемлемого уровня.

МЕТОДИКА ОЦЕНКА РИСКА

Для оценки рисков ИБ организации, защищенность каждого ценного ресурса определяется при помощи анализа угроз, действующих на конкретный ресурс, и уязвимостей, через которые данные угрозы могут быть реализованы. Оценивая вероятность реализации актуальных для ценного ресурса угроз и степень влияния реализации угрозы на ресурсы, анализируются информационные риски ресурсов организации.

В результате работы алгоритма оценки рисков определяются следующие характеристики ИС:

1. Список информационных ресурсов (ИР).
2. Значения риска для каждого ценного ИР организации.
3. Значения риска для ИР после задания контрмер (остаточный риск).
4. Эффективность контрмер.

Для того чтобы оценить риск информационного ресурса, необходимо проанализировать все угрозы, действующие на ИС, и уязвимости, через которые возможна реализация угроз. Исходя из полученных от владельца ИС данных, можно построить модель актуальных угроз и уязвимостей для конкретной организации. На основе модели будет проведен анализ вероятности реализации угроз информационной безопасности на каждый ресурс и, исходя из этого, рассчитаны риски ИБ.

Входные данные алгоритма:

- информационные ресурсы;
- критичность ресурсов;
- угрозы, действующие на ресурсы;
- уязвимости, через которые реализуются угрозы;
- вероятность реализации угрозы через данную уязвимость;
- критичность реализации угрозы через данную уязвимость.

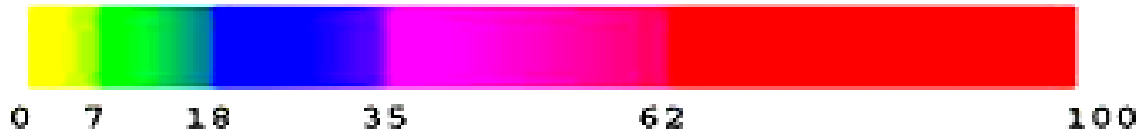
С точки зрения базовых угроз ИБ существует два режима работы алгоритма:

1. Одна базовая угроза (суммарная).
2. Три базовые угрозы.

Выбор шкалы для оценки риска и разбиение ее на уровни

При работе с алгоритмом используется числовая шкала от 0 до 100%. Шкалу разбивают максимум на 100 уровней. При разбиении шкалы на меньшее число уровней, каждый уровень занимает определенный интервал на шкале. Причем, возможно два варианта разделения:

– равномерное;



– логарифмическое.

Расчет рисков информационной безопасности

1. На первом этапе рассчитывается **уровень угрозы по уязвимости** (Th) на основе критичности и вероятности реализации угрозы через данную уязвимость. Уровень угрозы показывает, насколько критичным является воздействие данной угрозы на ресурс с учетом вероятности ее реализации.

$$\mathrm{Th} = \frac{\mathrm{ER}}{100} \times \frac{\mathrm{P(V)}}{100},$$

$$\mathrm{Th}_{\mathrm{c,i,a}} = \frac{\mathrm{ER}_{\mathrm{c,i,a}}}{100} \times \frac{\mathrm{P(V)}_{\mathrm{c,i,a}}}{100},$$

где $\mathrm{ER}_{\mathrm{c,i,a}}$ – критичность реализации угрозы (указывается в %), $\mathrm{P(V)}_{\mathrm{c,i,a}}$ – вероятность реализации угрозы через данную уязвимость по конфиденциальности, целостности и доступности (указывается в %).

Здесь вычисляется одно (Th) или три значения ($\mathrm{Th_c}$, $\mathrm{Th_i}$, $\mathrm{Th_a}$) в зависимости от количества базовых угроз. Значение уровня угрозы по уязвимости лежит в отрезке [0, 1].

2. Чтобы рассчитать **уровень угрозы по всем уязвимостям** (CTh), через которые возможна реализация данной угрозы на ресурс, просуммируем полученные уровни угроз через конкретные уязвимости по следующим формулам.

Для режима с одной базовой угрозой:

$$\mathrm{CTh} = 1 - \prod_{\mathrm{i}=1}^{\mathrm{n}} (1 - \mathrm{Th}).$$

Для режима с тремя базовыми угрозами:

$$\mathrm{CTh_c} = 1 - \prod_{\mathrm{i}=1}^{\mathrm{n}} (1 - \mathrm{Th_c}),$$

$$CTh_i = 1 - \prod_{i=1}^{n} (1 - Th_i),$$

$$CTh_a = 1 - \prod_{i=1}^{n} (1 - Th_a).$$

Значение уровня угрозы по всем уязвимостям лежит в отрезке [0, 1].

3. Далее рассчитывается **общий уровень угроз по ресурсу** (CThR) с учетом всех угроз, действующих на ресурс.

Для режима с одной базовой угрозой:

$$CThR = 1 - \prod_{i=1}^{n} (1 - CTh).$$

Для режима с тремя базовыми угрозами:

$$CThR_c = 1 - \prod_{i=1}^{n} (1 - CTh_c),$$

$$CThR_i = 1 - \prod_{i=1}^{n} (1 - CTh_i),$$

$$CThR_a = 1 - \prod_{i=1}^{n} (1 - CTh_a).$$

Значение общего уровня угрозы лежит в отрезке [0, 1].

4. Итоговый **риск по ресурсу** (R), характеризующий возможные потери собственника ИС, связанные с реализацией некоторой угрозы через любую уязвимость, рассчитывается следующим образом.

Для режима с одной базовой угрозой:

$$R = CThR \times D,$$

где D – критичность ресурса. Для угроз нарушения целостности или доступности определяется заранее (в деньгах или уровнях в год), а в случае угрозы нарушения доступности ресурса (DoS – отказ в обслуживании) критичность ресурса в год рассчитывается по формуле:

$$D_{а/год} = D_{а/час} \times T,$$

где $D_{а/час}$ – критичность простоя ресурса в час, T – общее время простоя.

Для режима с тремя базовыми угрозами:

$$R_{c,i,a} = CThR_{c,i,a} \times D_{c,i,a},$$

$$R = (1-(1-\frac{R_c}{100})(1-\frac{R_i}{100})(1-\frac{R_a}{100}))\times 100,$$

где $D_{c,i,a}$ – критичность ресурса по каждой из трех угроз заданная в деньгах или уровнях в год.

5. Общий **риск по информационной системе** (CR) рассчитывается по следующим формулам.

Для режима с одной базовой угрозой:

$$CR = \sum_{i=1}^{n} R_i$$

– для случая оценки в деньгах;

$$CR = (1-\prod_{i=1}^{n}(1-\frac{R_i}{100}))\times 100$$

– для случая оценки в уровнях.

Для режима с тремя базовыми угрозами:

$$CR_{c,i,a} = \sum_{i=1}^{n} R_i,$$

$$CR = CR_c + CR_i + CR_a$$

– для случая оценки в деньгах;

$$CR_{a,c,i} = (1-\prod_{i=1}^{n}(1-\frac{R_i}{100}))\times 100,$$

$$CR = (1-(1-\frac{R_c}{100})(1-\frac{R_i}{100})(1-\frac{R_a}{100}))\times 100$$

– для случая оценки в уровнях. В обоих режимах подразумевается R_i – риск i-го ресурса, $CR_{c,i,a}$ – риск по ИС для каждого вида угроз.

6. Для расчета **эффективности введенной контрмеры** (E) необходимо заново пройти шаги 1-5 с учетом заданной контрмеры и определить значение двух рисков – риска без учета контрмеры (R_{old}) и риск с учетом заданной контрмеры (R_{new}) или с учетом того, что уязвимость закрыта.

Эффективность введения контрмеры рассчитывается по формуле:

$$E = \frac{R_{old} - R_{new}}{R_{old}}.$$

В результате работы алгоритма пользователь получает следующие данные:

1. Риск реализации по трем базовым угрозам (или по одной суммарной угрозе) для ресурса.
2. Риск реализации суммарно по всем угрозам для ресурса.
3. Риск реализации по трем базовым угрозам (или по одной суммарной угрозе) для ИС.
4. Риск реализации по всем угрозам для ИС.
5. Риск реализации по всем угрозам для ИС после задания контрмер.
6. Эффективность контрмеры.

Пример расчета рисков ИБ на основе модели угроз и уязвимостей

Рассмотрим расчет рисков только для одного ресурса ИС – сервера, т.к. для остальных ресурсов риск рассчитывается аналогично.

1. Входные данные по всем ресурсам ИС.

Ресурс	Угрозы	Уязвимости
Ресурс 1 Сервер (Критичность ресурса D = 100 у.е.)	Угроза 1. Неавторизованное проникновение злоумышленника внутрь охраняемого периметра.	Уязвимость 1. Отсутствие регламента доступа в помещения с ресурсами, содержащими ценную информацию.
		Уязвимость 2. Отсутствие системы наблюдения за ресурсом.
	Угроза 2. Неавторизованная модификация информации в системе электронной почты, хранящейся на ресурсе.	Уязвимость 1. Отсутствует авторизация на внесение изменений в систему электронной почты.
		Уязвимость 2. Отсутствие регламента работы с системой криптографической защиты электронной почты.
	Угроза 3. Разглашение конфиденциальной информации – ключей доступа к ресурсу – сотрудниками организации.	Уязвимость 1. Отсутствие соглашений о сохранении конфиденциальности ключевой информации.
		Уязвимость 2. Распределение ключевой информации между несколькими сотрудниками.

2. Входные данные по парам ресурс/угроза для каждого ресурса ИС.

Ресурс 1. Сервер		
Угроза/уязвимость	**Вероятность реализации угрозы через данную уязвимость в течении года %, P(V)**	**Критичность реализации угрозы через данную уязвимость %, ER**
Угроза 1/уязвимость 1	50	60
Угроза 1/уязвимость 2	20	60
Угроза 2/уязвимость 1	60	40
Угроза 2/уязвимость 2	10	40
Угроза 3/уязвимость 1	10	80
Угроза 3/уязвимость 2	80	80

3. Расчет уровней угрозы по каждой (Th) и по всем (CTh) уязвимостям для каждого ресурса ИС.

Ресурс 1. Сервер		
Угроза/уязвимость	**Уровень угрозы по каждой уязвимости %, Th** $\mathrm{Th} = \frac{\mathrm{ER}}{100} \times \frac{\mathrm{P(V)}}{100}$	**Уровень угрозы по всем уязвимостям, через которые она может быть реализована %, CTh** $\mathrm{CTh} = 1 - \prod_{i=1}^{n} (1 - \mathrm{Th})$
Угроза 1/уязвимость 1	0.3	0.384
Угроза 1/уязвимость 2	0.12	
Угроза 2/уязвимость 1	0.24	0.27
Угроза 2/уязвимость 2	0.04	
Угроза 3/уязвимость 1	0.08	0.669
Угроза 3/уязвимость 2	0.64	

4. Расчет общего уровня угроз (CThR) действующего на ресурс для каждого ресурса ИС.

Ресурс 1. Сервер		
Угроза/уязвимость	**Уровень угрозы по всем уязвимостям %, CTh**	**Общий уровень угроз по ресурсу %, CThR** $\mathrm{CThR} = 1 - \prod_{i=1}^{n} (1 - \mathrm{CTh})$
Угроза 1/уязвимость 1	0.384	0.8511
Угроза 1/уязвимость 2		
Угроза 2/уязвимость 1	0.27	
Угроза 2/уязвимость 2		
Угроза 3/уязвимость 1	0.669	
Угроза 3/уязвимость 2		

5. Расчет итогового риска по ресурсу (R) для всех ресурсов ИС.

Ресурс 1. Сервер		
Угроза/уязвимость	**Общий уровень угроз по ресурсу %, CThR**	**Риск по ресурсу у.е., R** $R = CThR \times D$
Угроза 1/уязвимость 1	**0.8511**	**85.11**
Угроза 1/уязвимость 2		
Угроза 2/уязвимость 1		
Угроза 2/уязвимость 2		
Угроза 3/уязвимость 1		
Угроза 3/уязвимость 2		

6. Расчет общего риска по информационной системе (CR).

Для нашего примера (режима с одной базовой угрозой и случая оценки в деньгах) необходимо просуммировать все риски (R) по каждому ресурсу ИС:

$$CR = \sum_{i=1}^{n} R_i .$$

Но так как мы описали здесь лишь один ресурс, то CR = 85.11 у.е.

КОНТРОЛЬНЫЕ ВОПРОСЫ

1. Что такое информационная система?
2. Что понимают под информацией и информационными ресурсами?
3. Назовите и охарактеризуйте основные свойства ИР.
4. Что такое угроза ИБ?
5. Что такое уязвимость?
6. Что такое риск ИБ?
7. Что понимают под оценкой, анализом и управлением рисками ИБ?

ЗАДАНИЕ НА ЛАБОРАТОРНУЮ РАБОТУ № 3

Название работы

Расчет рисков информационной безопасности.

Задание (не забудьте оформить отчет)

1. Изучить основной теоретический материал лабораторной работы.
2. Изучить методику оценки рисков.
3. Внести структурную схему и описание вашей ИС в отчет (Структура и описание ИС из лаб. работы №1).
4. Составить и внести в отчет перечни типов угроз ИБ и информационные ресурсы, присутствующие в данной ИС.
5. По описанной выше методике от Digital Security выполнить оценку риска ИБ для каждого информационного ресурса вашей ИС. Внесите расчеты в отчет.
6. Для упрощения вычислений реализуйте алгоритм расчета рисков на любом доступном языке программирования или в MS Excel. Внесите листинг программы в отчет.
7. Дополнительно попробуйте «реализовать» (описать) контрмеры против некоторых из имеющихся уязвимостей и рассчитать эффективность введенных контрмер.
8. Внести ответы на контрольные вопросы в отчет.

Структура основной части отчета

1. Структура и описание ИС:
2. Перечень типов угроз:
3. Перечень ИР:
4. Оценка риска:
5. Листинг программы:
6. Введены контрмеры:
7. Оценка эффективности введенных контрмер:
8. Ответы на контрольные вопросы:

Расчетно-графическая работа

Разработка рекомендаций по информационной безопасности

Цель

Разработать рекомендации по аудиту информационной безопасности предприятия.

Программно-аппаратные средства

Компьютерная лаборатория, стандартные средства Microsoft Office.

На основании информации, полученной в ходе исследования информационной инфраструктуры заказчика и результатов анализа рисков, разрабатываются рекомендации по совершенствованию системы защиты информации, применение которых позволит минимизировать риски, с приложением списка конкретных уязвимостей активного сетевого оборудования, серверов, межсетевых экранов и др.

По завершении аудита подготавливается итоговый отчет, содержащий оценку текущего уровня безопасности ИТ-инфраструктуры, информацию об обнаруженных проблемах, анализ соответствующих рисков и рекомендации по их устранению.

Структура основной части отчета

1. Исходные данные о заказчике. (Из лаб. работы №1)
2. Составить аудиторский отчёт:
    1) Оценка текущего уровня защищенности информационной системы:
        a. Описание и оценка текущего уровня защищенности информационной системы;
        b. Анализ конфигурации конфигурационной информации, найденные уязвимости;

c. Анализ рисков, связанных с возможностью осуществления внутренних и внешних угроз в отношении ресурсов информационной системы;

2) Рекомендации по технической составляющей ИБ:
   a. по изменению конфигурации существующих сетевых устройств и серверов;
   b. по изменению конфигурации существующих средств защиты;
   c. по активации дополнительных штатных механизмов безопасности на уровне системного программного обеспечения;
   d. по использованию дополнительных средств защиты;
3) Рекомендации по организационной составляющей ИБ:
   a. по разработке политики информационной безопасности;
   b. по организации службы ИБ;
   c. по разработке организационно-распорядительных и нормативно-технических документов;
   d. по пересмотру ролевых функций персонала и зон ответственности;
   e. по разработке программы осведомленности сотрудников в части информационной безопасности;
   f. Комплексный аудит по поддержке и повышению квалификации персонала

Задание для расчетно-графической работы

Изучить теоретические материалы.

Сформировать матрицу рисков ИБ для ИС.

Количественно оценить риски

Предложить набор контрмер.

Оформить отчет о проделанной работе.

Исследовать методику оценки затрат на ЗИ в организации.

Методика оценки затрат на ЗИ с использованием весовых коэффициентов

Ввод исходных данных и предварительные вычисления (таблица 1).

	A	B	C	D	E	F	G	H	I
1	Таблица 1 (Ввод исходных данных и предварительные вычисления)								
2	№	Параметры	Угроза I						Сумма
3			i1	i2	i3	i4	i5	i6	
4	1	Значения вероятности угроз Pi	0.57	0.58	0.79	0.35	0.64	0.53	
5	2	Собственные потери (прибыли) Dсоб							
6	3	Выгоды (прибыли) конкурентов Dкон							
7	4	Показатель степени *ai* в формуле веса							
8	5	Вес угрозы							

1. Определяем показатель степени в формуле веса каждой угрозы как отношение величины собственных потерь Dсобi к величине выгод конкурентов Dконi по каждой угрозе.

2. Определяем вес каждой угрозы как показательную функцию вида: вероятность угрозы в степени, равной отношению собственных потерь к выгодам конкурентов по каждой угрозе.

Сущность веса угрозы заключается в следующем: рост потенциальной выгоды конкурента приводит к росту затрат на защиту от данной угрозы в сумме общих затрат на защиту при ее постоянстве.

Определение значимости защиты от каждой угрозы (таблица 2).

11	Таблица 2 (Определение значимости защиты от каждой угрозы)								
12	№	Параметры	Угроза I						Сумма
13			i1	i2	i3	i4	i5	i6	
14	6	Значения вероятности угроз Pi							
15	7	Собственные потери (прибыли) Dсоб							
16	8	Выгоды (прибыли) конкурентов Dкон							
17									
18									

3. Определяем сумму собственных потерь Dсобі и выгод конкурентов Dконі, по каждой угрозе и общую сумму по всем угрозам.

4. Определяем относительный вес потерь по каждой угрозе:

Ротні = (Dсобі + Dконі) / (сумма Dсобі + сумма Dконі).

Независимо от числа угроз сумма весов должна быть равна единице.

5. Определяем значимость защиты от каждой угрозы как произведение ее веса (вероятностный аргумент) на относительный вес (денежный вес):

Рзні = Рвесі * Ротні

Сущность значимости защиты заключается в том, что ее значение будет давать нам долю отчисления от общей суммы, выделяемую на противодействие каждой угрозе.

Определение величины средств, необходимых и распределяемых на защиту информации от прогнозируемых угроз (таблица 3).

19	Таблица 3 (Определение величины средств, необхо-димых и распределяемых на защиту информации от прогнозируемых угроз)								
20	№	Параметры	Угроза I						Сумма
21			i1	i2	i3	i4	i5	i6	
22	9	Значение сумм на противодействие каждой угрозе Dн от i							
23									

6. Строгих рекомендаций по нормам выделяемой на защиту информации суммы не существует. В разных источниках в качестве финансовых баз, от которых даются относительные величины потерь и отчислений на защиту, приводятся различные балансовые или экономические показатели. Сами коэффициенты потерь и отчислений имеют не нормативный, а констатирующий характер.

Учитывая, что в качестве базы для отчислений на защиту информации принята величина неполученной (потенциальной) прибыли, норму отчисления Dн.от от неполученной прибыли на ЗИ примем равной 0,25, и тогда:

Dн.от = 0,25 сумма Dсобі .

7. Данная норма отчисления от сберегаемой прибыли предназначена для нейтрализации суммы значимостей всех угроз, следовательно, на

предотвращение каждой угрозы должна выделяться часть доли, пропорциональная значимости защиты от этой угрозы:

Dн.от = сумма Рзнi.

Распределение сумм находится как:

Dн.от i = Dн.от * Рзнi / сумма Рзнi.

8. Рассчитываем суммы затрат, необходимые для защиты информации от каждой угрозы.

Итоговый вид указанных таблиц будет примерно следующим:

	A	B	C	D	E	F	G	H	I
1	**Таблица 1**								
2	**№ п/п**	**Параметры**	**Угроза I_i**						**Сумма Σ**
3			I_1	I_2	I_3	I_4	I_5	I_6	
4	1	Значения вероятности угроз Pi	0,65	0,63	0,43	0,63	0,42	0,81	
5	2	Собственные потери (прибыли) $D_{соб}$	$9 260	$8 310	$6 430	$15 820	$4 960	$5 130	$49 910
6	3	Выгоды (прибыли) конкурентов $D_{кон}$	$11 230	$2 460	$4 520	$15 100	$3 060	$4 130	$40 500
7	4	Показатель степени a_i в формуле веса	0,82	3,38	1,42	1,05	1,62	1,24	
8	5	Вес угрозы $P_{весi} = P_i^{a_i}$	0,7010236	0,210	0,301	0,616	0,245	0,770	
9									
10	**Таблица 2**								
11	**№ п/п**	**Параметры**	**Угроза I_i**						**Сумма Σ**
12			I_1	I_2	I_3	I_4	I_5	I_6	
13	6	Суммы собственных потерь и выгод конкурентов	$20 490	$10 770	$10 950	$30 920	$8 020	$9 260	$90 410
14	7	Относительный вес потерь	0,227	0,119	0,121	0,342	0,089	0,102	1
15	8	Значимость защиты от угрозы	0,159	0,025	0,036	0,211	0,022	0,079	0,53
16									
17	**Таблица 3**								
18	**№ п/п**	**Параметры**	**Угроза I_i**						**Общая сум**
19			I_1	I_2	I_3	I_4	I_5	I_6	
20	9	Значение сумм на противодействие каждой угрозе $D_{н.от i}$	$4 474	$704	$1 027	$5 935	$612	$2 220	$14 973

Задание

Выполнить расчетную работу в соответствии с приведенной выше методикой оценки затрат на ЗИ от различных угроз на основе алгоритма использования весовых коэффициентов.

Расчеты желательно представить как отчет в файле MS Excel. Исходные данные для расчетов возьмите согласно вашему варианту из таблицы ниже:

	Вариант									
Параметры	1	2	3	4	5	6	7	8	9	10
P1	0,67	0,53	0,68	0,55	0,63	0,6	0,59	0,57	0,64	0,54
P2	0,55	0,43	0,54	0,51	0,5	0,54	0,4	0,58	0,52	0,38
P3	0,67	0,53	0,68	0,72	0,58	0,56	0,25	0,56	0,59	0,64
P4	0,55	0,43	0,54	0,25	0,76	0,45	0,55	0,4	0,5	0,6
P5	0,49	0,56	55	0,65	0,27	0,39	0,58	0,45	0,65	0,74

P6	0,57	0,58	0,25	0,56	0,52	0,36	0,62	0,58	0,25	0,61
Dособі1	10210	9560	9870	9400	10250	9850	8900	8500	8650	8450
Dособі2	9300	7800	8200	7400	7650	8560	6950	7320	7980	7560
Dособі3	7350	6800	7230	6050	6230	7150	5980	6250	6980	6000
Dособі4	14890	15325	14780	12560	13400	14890	12740	14230	12980	13890
Dособі5	5170	4890	4650	4325	5120	4560	4890	4360	4780	3980
Dособі6	7980	6850	7200	5600	5420	5820	4900	5950	6540	6890
Dконі1	12560	11890	11325	11870	12740	11650	10650	11930	10980	10250
Dконі2	2650	2350	1980	2200	2980	2450	2130	2780	2650	2780
Dконі3	4630	4260	4890	3560	4250	4980	4780	4325	4120	4650
Dконі4	17890	16850	17250	17150	16960	16850	16450	15890	16780	16450
Dконі5	2450	2100	2350	2150	2650	2780	2455	2360	3200	2650
Dконі6	4320	3890	3780	2680	2980	3150	3450	3780	3980	4120

Постановка задачи

Руководством предприятия «XXX» за 2020 год проведен анализ угроз информационной безопасности и определены шесть типов комплексных угроз в виде возможных каналов утраты и утечки информации:

1. Физические угрозы, исходящие от персонала и направленные на информационные ресурсы предприятия – I1.

2. Физические угрозы, связанные с отказом оборудования – I2.

3. Локальные программные угрозы, направленные на операционную систему – I3.

4. Удаленные угрозы, направленные на информацию предприятия, обрабатываемую сетевыми службами – I4.

5. Программные угрозы, направленные на каналы связи – I5.

6. Угрозы неумышленных действий персонала, связанных с недостаточной квалификацией – I6.

Руководством предприятия были привлечены эксперты, которые выполнили следующую работу:

1. Провели оценку вероятности реализации каждой угрозы:

- Физические угрозы, исходящие от персонала и направленные на информационные ресурсы предприятия – P1.
- Физические угрозы, связанные с отказом оборудования – P2 .

- Локальные программные угрозы, направленные на операционную систему – Р3.
- Удаленные угрозы, направленные на информацию предприятия, обрабатываемую сетевыми службами – Р4.
- Программные угрозы, направленные на каналы связи – Р5.
- Угрозы неумышленных действий персонала, связанных с недостаточной квалификацией – Р6.

Необходимо понимать, что вероятности реализации угроз не отражает величину потерь и не пропорциональны ей. При определении значения вероятности угрозы учитываются возможности конкурентов по ведению деловой разведки.

2. Оценили собственные потери предприятия (в виде неполученной прибыли) Dсобi при реализации каждой угрозы.

3. Оценили выгоды конкурентов (полученную ими прибыль) Dконi, при успешном осуществлении ими действий, ведущих к реализации угрозы.

Требуется определить величину суммы затрат, которая может быть выделена на защиту информации от всех угроз, и ее распределение на мероприятия по защите от каждой угрозы, в зависимости от собственных потерь и приобретений конкурентов при реализации каждой угрозы.

Структура основной части отчета:

1. Постановка задачи и входные данные вашего варианта.
2. Таблицы с результатами расчетов.
3. Анализ результатов решения.
4. Ваши выводы по текущему состоянию ИБ в организации.
5. Ваши рекомендации по улучшению состояния ИБ в организации.

Варианты организаций

1. Компания имеет 5 представительств, все пять в разных странах (.ua, .ru и тд). Имеет 5 представительств в каждом от 50-100 чел. Головная компания 1000 чел в России. Отдел продаж в региональное представительство, административный отдел и отдел обработки данных. Направление деятельности компании - транснациональные грузовые перевозки.

2. Компания имеет одно представительство в России, которое является компанией, купленной годом ранее, занимающееся разработкой ПО. Головная компания до 500 чел. Представительство - до 300 чел. (Разные бренды). 2 домена – 2 бренда

3. Компания имеет головной офис со штатом 300 чел. Занимается продажей сотовых телефонов. По всей России 2000-3000 представительств – магазинах, есть упр. менеджер (локальный отд. продаж) и тарифный отдел и отд. логистики.

4. Компания – 100 чел. Сфера деятельности аутсорсинг, услуги администрирования различных систем на базе Microsoft. Клиенты в большинстве стран мира. Компания обеспечивает полную поддержку инфраструктуры клиента.

5. Компания состоит из 3-х филиалов на территории РФ. ЦО в Хабаровске. Численность ЦО 100 чел., в филиалах 20 чел. Занимается производством и разработкой средств аутентификации. Производство в филиалах, ЦО выполняет только административные действия.

6. Компания - холдинг с центральным офисом в г. Владивостоке. Занимается созданием и разработкой интернет сайтов и в неё входит ещё 4 компании, находящиеся в 4 странах мира. В каждой компании до 50 человек.

Приложение 1

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ[1]
по дисциплине
Оценка рисков информационной безопасности автоматизированных систем

Направление подготовки	*10.05.03 "Информационная безопасность автоматизированных систем"*
Направленность (профиль) образовательной программы	*Анализ безопасности информационных систем*
Квалификация выпускника	*специалист по защите информации*
Год начала подготовки *(по учебному плану)*	*2020*
Форма обучения	*очная*
Технология обучения	*традиционная*

Курс	Семестр	Трудоемкость, з.е.
5	*9*	*4*

Вид промежуточной аттестации	Обеспечивающее подразделение
Экзамен	*Кафедра ИБАС - Информационная безопасность автоматизированных систем*

[1] В данном приложении представлены типовые оценочные средства. Полный комплект оценочных средств, включающий все варианты заданий (тестов, контрольных работ и др.), предлагаемых обучающемуся, хранится на кафедре в бумажном и электронном виде.

1 Перечень планируемых результатов обучения по дисциплине (модулю), соотнесенных с планируемыми результатами образовательной программы

Таблица 1 – Компетенции и планируемые результаты обучения по дисциплине

Код и наименование компетенции	Планируемые результаты обучения по дисциплине		
	Перечень знаний	Перечень умений	Перечень навыков
Профессиональные			
ПК-7 способностью разрабатывать научно-техническую документацию, готовить научно-технические отчеты, обзоры, публикации по результатам выполненных работ	**З1(ПК-7)** Знает структурные и функциональные схемы защищенных автоматизированных систем	**У1(ПК-7)**Умеет проводить анализ структурных и функциональных схем защищенных автоматизированных информационных систем	**Н1(ПК-7)** Владеет навыками выявления потенциальных уязвимостей информационной безопасности автоматизированных систем
ПК-8 способностью разрабатывать и анализировать проектные решения по обеспечению безопасности автоматизированных систем	**З1(ПК-8)** Знает способы проведения анализа защищенности информационной инфраструктуры автоматизированных систем	**У1ПК-8** Умеет выбирать способ проведения анализа защищенности информационной инфраструктуры автоматизированных систем	**Н1(ПК-8)** Владеет навыками проведения анализа защищенности информационной инфраструктуры автоматизированных систем

Таблица 2 – Паспорт фонда оценочных средств

Контролируемые разделы (темы) дисциплины	**Код контролируемой компетенции**	**Наименование оценочного средства**	**Показатели оценки**
1. Аудит информационной безопасности предприятия.	ПК-7	Лабораторная работа 1	Умение проводить анализ структурных и функциональных схем защищенных автоматизированных информационных систем с целью выявления потенциальных уязвимостей информационной безопасности автоматизированных систем .

2. Табличные методы оценки и анализа информационных рисков.	ПК-8	Лабораторная работа 2	Умение проводить анализ структурных и функциональных схем защищенных автоматизированных информационных систем
3. Расчет рисков информационной безопасности.	ПК-8	Лабораторная работа 3	Умение рассчитать риски информационной безопасности
Разработка рекомендации по аудиту информационной безопасности предприятия.	ПК-7 ПК-8	Расчетно-графическая работа	Умение проводить анализ защищенности информационной инфраструктуры автоматизированной системы Умение проводить анализ структурных и функциональных схем защищенных автоматизированных информационных систем с целью выявления потенциальных уязвимостей информационной безопасности автоматизированных систем

2 Методические материалы, определяющие процедуры оценивания знаний, умений, навыков и (или) опыта деятельности, характеризующие процесс формирования компетенций

Методические материалы, определяющие процедуры оценивания знаний, умений, навыков и (или) опыта деятельности, представлены в виде технологической карты дисциплины (таблица 3).

Таблица 3 – Технологическая карта

	Наименование оценочного средства	Сроки выполнения	Шкала оценивания	Критерии оценивания
3 семестр Промежуточная аттестация в форме зачета с оценкой				
1	Лабораторная работа 1	В течение семестра	10 баллов	10 баллов - студент правильно выполнил задание. Показал отличные знания, навыки и умения рамках освоенного учебного материала.

	Наименование оценочного средства	Сроки выполнения	Шкала оценивания	Критерии оценивания
				5 балла - студент выполнил задание с небольшими неточностями. Показал хорошие знания, навыки и умения рамках освоенного учебного материала. 3 балла - студент выполнил задание с существенными неточностями. Показал удовлетворительные знания, навыки и умения рамках освоенного учебного материала. 2 балла - при выполнении задания студент продемонстрировал недостаточный уровень знаний. 0 баллов – задание не выполнено.
2	Лабораторная работа 2	В течение семестра	10 баллов	10 баллов - студент правильно выполнил задание. Показал отличные знания, навыки и умения рамках освоенного учебного материала. 5 балла - студент выполнил задание с небольшими неточностями. Показал хорошие знания, навыки и умения рамках освоенного учебного материала. 3 балла - студент выполнил задание с существенными неточностями. Показал удовлетворительные знания, навыки и умения рамках освоенного учебного материала. 2 балла - при выполнении задания студент продемонстрировал недостаточный уровень знаний. 0 баллов – задание не выполнено.
3	Лабораторная работа 3	В течение семестра	10 баллов	10 баллов - студент правильно выполнил задание. Показал отличные знания, навыки и умения рамках освоенного учебного материала. 5 балла - студент выполнил задание с небольшими неточностями. Показал хорошие знания, навыки и умения рамках освоенного учебного материала. 3 балла - студент выполнил задание с существенными неточностями. Показал удовлетворительные знания, навыки и умения рамках освоенного учебного материала. 2 балла - при выполнении задания студент продемонстрировал недостаточный уровень знаний. 0 баллов – задание не выполнено.
4	Расчетно-графическая работа	В течение семестра	15 баллов	15 баллов - студент правильно выполнил задания. Показал отличные владения навыками применения полученных знаний и умений при решении профессиональных задач в рамках

	Наименование оценочного средства	Сроки выполнения	Шкала оценивания	Критерии оценивания
				усвоенного учебного материала. Ответил на все дополнительные вопросы на защите. 10 баллов - студент выполнил задание с небольшими неточностями. Показал хорошие владения навыками применения полученных знаний и умений при решении профессиональных задач в рамках усвоенного учебного материала. Ответил на большинство дополнительных вопросов на защите. 5 баллов - студент выполнил задания с существенными неточностями. Показал удовлетворительное владение навыками применения полученных знаний и умений при решении профессиональных задач в рамках усвоенного учебного материала. При ответах на дополнительные вопросы на защите было допущено много неточностей. 0 баллов - при выполнении задания студент продемонстрировал недостаточный уровень владения навыками применения полученных знаний и умений при решении профессиональных задач в рамках усвоенного учебного материала. При ответах на дополнительные вопросы на защите было допущено множество неточностей.
ИТОГО:			45 баллов	

Критерии оценки результатов обучения по дисциплине:
0 – 64 % от максимально возможной суммы баллов – «неудовлетворительно» (недостаточный уровень для промежуточной аттестации по дисциплине);
65 – 74 % от максимально возможной суммы баллов – «удовлетворительно» (пороговый (минимальный) уровень);
75 – 84 % от максимально возможной суммы баллов – «хорошо» (средний уровень);
85 – 100 % от максимально возможной суммы баллов – «отлично» (высокий (максимальный) уровень).

3 Типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности, характеризующие процесс формирования компетенций в ходе освоения образовательной программы

Примерный перечень вопросов по закреплению теоретических знаний, умений и практических навыков, предусмотренных компетенциями (вопросы к экзамену)

1. Что представляет собой менеджмент риска информационной безопасности? Перечислите задачи менеджмента риска информационной безопасности.

2. Перечислите основные этапы менеджмента риска информационной безопасности и их взаимосвязи.

3. Что включает в себя этап установление контента? Перечислите основные критерии, необходимые для менеджмента риска ИБ.

4. В чем заключается и какие этапы включает в себя оценка риска ИБ?

5. В чем заключается и какие этапы включает в себя анализ риска ИБ?

6. В чем заключается идентификация риска ИБ? Перечислите этапы идентификации риска ИБ.

7. Что включает в себя идентификация активов? Перечислите основные виды активов.

8. Что представляют собой требования безопасности для активов?

9. Что включает в себя реестр информационных активов?

10. Каким образом может быть определена ценность активов? Приведите пример критериев и соответствующих шкал для оценки возможного ущерба.

11. Что такое профиль и жизненный цикл угрозы?

12. По каким признакам классифицируются угрозы информационной безопасности?

13. Какими способами может быть выполнена оценка вероятности угроз информационной безопасности?

14. Какими способами может быть выполнена оценка уязвимостей?

15. Каким образом может быть получена количественная оценка риска информационной безопасности?

16. Что включает в себя реестр рисков информационной безопасности?

17. В чем заключается оценивание рисков информационной безопасности?

18. Какие существуют варианты обработки риской информационноŭ безопасности?

19. В чем заключается снижение риска информационноŭ безопасности? Перечислите способы снижения рисков. Какие типичные ограничения должны быть учтены?

20. В чем заключается сохранение риска информационноŭ безопасности? Перечислите факторы, влияющие не решение о принятии рисков.

21. В чем заключается предотвращение риска информационноŭ безопасности? Перечислите основные способы предотвращения риска.

22. Что такое перенос риска информационноŭ безопасности?

23. Какие задачи решаются в процессе коммуникации риска информационноŭ безопасности?

24. Какие факторы подлежат мониторингу в процессе переоценки риска информационноŭ безопасности?

25.Охарактеризовать роль лица, принимающего решения, экспертов, консультантов в задачах принятия решениŭ.

26. Привести общую схему алгоритма экспертизы.

27. Описать основные этапы экспертизы.

28. Описать основные формы опроса экспертов, взаимодеиŭствия экспертов при опросе.

29. Составить алгоритм оценивания согласованности мнениŭ экспертов.

30. Описать методы формирования исходного множества альтернатив.

31. Что такое область компромиссов, область согласия, множество Парето, множество эффективных решениŭ? Как выделяют область компромиссов?

32. Описать признаки и своиŭства методов решения многокритериальных задач принятия решениŭ. Провести классификацию методов многокритериальноŭ оценки альтернатив и методов решения многокритериальных задач принятия решениŭ.

33. Охарактеризовать аксиоматические методы многокритериальноŭ оценки альтернатив.

34. Какие принципы оптимальности используются в прямых методах многокритериальноŭ оценки альтернатив?

35. Каковы основные приемы нормализации критериев? 36. Как определяется важность критериев?

37. Построить структурные схемы методов порогов

несравнимости. К каким решениям могут приводить данные методы?

38. Построить структурную схему метода аналитической иерархии.

38. Чем различаются задачи принятия решений при риске и при определенности? В чем состоит неопределенность задачи принятия решений при риске?

39. Описать основные особенности однокритериальной модели принятия решений при риске.

40. Описать основные особенности многокритериальной модели принятия решений при риске.

41. В чем заключается неопределенность задачи принятия решений при риске? Как преодолевается эта неопределенность?

Лист регистрации изменений к РПД

	Номер протокола заседания кафедры, дата утверждения изменения	Количество страниц изменения	Подпись разработчика РПД