ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ
ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«РОССИЙСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ПРАВОСУДИЯ»
КАЗАНСКИЙ ФИЛИАЛ

Рабочая программа дисциплины (модуля)

МАТЕМАТИЧЕСКИЕ МЕТОДЫ ЗАЩИТЫ ИНФОРМАЦИИ

Набор 2023 г.

Направление подготовки: 38.03.02«Менеджмент»
Профиль подготовки: «Управление недвижимостью»

Рабочая программа разработана в соответствии с требованиями ФГОС.

Разработчик (-и): Турутина Е.Э., к.п.н.
Рабочая программа рассмотрена и одобрена на заседании кафедры правовой информатики, информационного права и естественнонаучных дисциплин протокол № 12 от 22.06.2023

Зав. кафедрой Галяутдинова Л.Р., к.ф-м..н, доцент

_____/ __Галяутдинова Л.Р._____
(подпись) (ФИО)

Казань, 2023

ПРОТОКОЛ ИЗМЕНЕНИЙ

рабочей программы дисциплины (модуля)

наименование дисциплины в соответствии с учебным планом

для набора ____ года на _____-_____уч.г.[1]

Краткое содержание изменения	Дата и номер протокола заседания кафедры

Актуализация выполнена[2]: _____

(ФИО, ученая степень, ученое звание)

_____ «__» _____ 201__г.

подпись

Зав. кафедрой _____

(ФИО, ученая степень, ученое звание)

_____ «__» _____ 20__г.

подпись

[1] Указанный протокол заполняется при актуализации РП по дисциплине (модулю) на учебный год, в течение которого соответствующая дисциплина (модуль) будет преподаваться (если год набора отличается от года преподавания дисциплины (модуля).

[2] Если отдельные элементы РП актуализированы разными педагогическими работниками, то необходимо указать соответствующую информацию, обеспечить подписание документа всеми педагогическими работниками.

Оглавление

	Наименование разделов	**Стр.**
	Аннотация рабочей программы	
1.	Цели и планируемые результаты изучения дисциплины (модуля)	
2.	Место дисциплины (модуля) в структуре ППССЗ/ОПОП	
3.	Объем дисциплины (модуля)и виды учебной работы	
4.	Содержание дисциплины (модуля)	
5.	Учебно-методическое и информационное обеспечение дисциплины (модуля)	
6.	Материально-техническое обеспечение	
7.	Карта обеспеченности литературой	
8.	Фонд оценочных средств	

Аннотация рабочей программы дисциплины
«Математические методы защиты информации»

Цель изучения дисциплины	Целью освоения дисциплины «Математические методы защиты информации» является обучение студентов формально-математическим методам защиты информации, обеспечивающим необходимый уровень информационной безопасности профессиональной деятельности.
Место дисциплины в структуре программы	Учебная дисциплина Б.1.В.В.1.1. «Математические методы защиты информации» – это дисциплина по выбору в основной образовательной программе ФГОС ВО по направлению подготовки 38.03.02 Менеджмент (уровень бакалавриата).
Компетенции, формируемые в результате освоения дисциплины	Компетентностный подход при изучении данной учебной дисциплины предполагает формирование у обучаемых следующих компетенций: **УК-1** Способен осуществлять поиск, критический анализ и синтез информации, применять истемный подход для решения поставленных задач **ПК-3** – Способен применять методы экономического анализа, обрабатывать, систематизировать, анализировать информацию, составлять документацию и использовать ее в профессиональной деятельности по управлению рисками
Содержание дисциплины	Введение в дисциплину. Методы обеспечения качества и защиты информации. Тема 1. Информационная безопасность и уровни ее обеспечения. Тема 2. Государственная политика в обеспечении информационной безопасности. Тема 3. Криптографические методы защиты информации. Тема 4. Аудит информационной безопасности. Анализ информационных рисков.
Структура дисциплины, виды учебной работы	Общая трудоемкость дисциплины составляет 4 зачетные единицы, 144 час.
Форма промежуточной аттестации	Дифференцированный зачет

1.Цели и планируемые результаты изучения дисциплины

Целью освоения дисциплины «Математические методы защиты информации» является обучение студентов формально-математическим методам защиты информации, обеспечивающим необходимый уровень информационной безопасности профессиональной деятельности.

2. Место дисциплины в структуре ОПОП

Дисциплина «Математические методы защиты информации» Б.1.В.В.1.1. относится к дисциплинам по выбору. Данная дисциплина изучается на третьем курсе студентами специальности по направлению подготовки 38.03.02. «Менеджмент» (уровень бакалавриата).
Для освоения программы дисциплины студент должен обладать знаниями, умениями, навыками, указанными в картах компетенций по дисциплине.

Требования к результатам освоения дисциплины

В совокупности с другими дисциплинами ОПОП дисциплина обеспечивает формирование следующих компетенций:

Таблица 1

№ п/п	Код компетенции	Название
1	УК-1	Способен осуществлять поиск, критический анализ и синтез информации, применять системный подход для решения поставленных задач
2	ПК-3	Способен применять методы экономического анализа, обрабатывать, систематизировать, анализировать информацию, составлять документацию и использовать ее в профессиональной деятельности по управлению рисками

Планируемые результаты освоения дисциплины в части каждой компетенции указаны в картах компетенций по ППССЗ/ОПОП.
В рамках дисциплины осуществляется воспитательная работа, предусмотренная рабочей программой воспитания, календарным планом воспитательной работы.

3. Объем дисциплины и виды учебной работы

Таблица 2.1.

Очно-заочная форма обучения на базе среднего профессионального образования

Вид учебной работы	Трудоемкость			
	зач. ед.	час.	По семестрам	
Общая трудоемкость дисциплины по учебному плану	4	144	144	-
Контактная работа	-	**12**	**12**	-
Самостоятельная работа под контролем преподавателя, НИРС	-	132	132	-
Занятия лекционного типа	-	4	4	-
Занятия семинарского типа	-	8	8	-
в том числе с практической подготовкой (при наличии)	-	-	-	-
Форма промежуточной аттестации	-	**Дифф.зачет**	**Дифф.зачет**	-

4.Содержание дисциплины (модуля)

4.1.Текст рабочей программы по темам

Тема 1. Информационная безопасность и уровни ее обеспечения.

Определение понятия "информационная безопасность". Проблема информационной безопасности общества. Составляющие информационной безопасности. Система формирования режима информационной безопасности. Задачи информационной безопасности общества. Уровни формирования режима информационной безопасности. Классификация угроз информационной безопасности. Каналы несанкционированного доступа к информации. Идентификация пользователей, аутентификация пользователей и авторизация пользователей (назначение и способы реализации). Методы разграничение доступа.

Тема 2. Государственная политика в обеспечении информационной безопасности.

Основные положения государственной политики обеспечения информационной безопасности РФ. Основными направлениями государственной политики в области обеспечения информационной безопасности. Информационная безопасность в системе национальной безопасности. Нормативно-правовые основы информационной безопасности в РФ.

Тема 3. Криптографические методы защиты информации.

Кодирование и представление информации в ПК. Измерение количества информации.
Криптографические методы защиты информации. Математическое и алгоритмическое обеспечение криптографических методов защиты информации. Симметричные и асимметричные криптосистемы.
Цифровые подписи (Электронные подписи). Инфраструктура открытых ключей. Криптографические протоколы. Создание зашифрованных файлов и криптоконтейнеров и их расшифрование. Создание защищенного канала связи средствами виртуальной частной сети.

Тема 4. Аудит информационной безопасности. Анализ информационных рисков.

Понятие аудита безопасности. Виды аудита безопасности. Проведение аудита безопасности. Основные этапы работ при проведении аудита безопасности.

4.2.Разделы и темы дисциплин, виды занятий (тематический план)

Таблица 3.1

Очно-заочная форма обучения на базе среднего профессионального образования

№	Раздел дисциплины, тема	Код компетенции	Общая трудоёмкость дисциплины		в том числе				Наименование оценочного средства
				Самостоятельная работа под контролем преподавателя НИРС	Контактная работа	Занятия лекционного типа	Занятия семинарского типа	Практическая подготовка	
		час.	час.	час.	час	час	час.	час	
1	Информационная безопасность и уровни ее	УК-1 ПК-3	40	36	4	2	2	-	вопросы для семинара

	обеспечения.								(практического занятия), коллоквиум, доклады с презентациями, контрольная работа
2	Государственная политика в обеспечении информационной безопасности.	УК-1 ПК-3	40	36	4	2	2	-	вопросы для семинара (практического занятия), коллоквиум, доклады с презентациями, контрольная работа
3	Криптографические методы защиты информации.	УК-1 ПК-3	32	30	2		2	-	вопросы для семинара (практического занятия), коллоквиум, доклады с презентациями
4	Аудит информационной безопасности. Анализ информационных рисков.	УК-1 ПК-3	32	30	2		2	-	Реферат, задания на практическую работу, коллоквиум, тестовые задания
	ВСЕГО		144	132	12	4	8		

4.3. Самостоятельное изучение студентами разделов, тем дисциплины

Таблица 4.1

Очно-заочная форма обучения на базе среднего профессионального образования

№ темы дисциплины	Вопросы, выносимые на самостоятельное изучение	Кол. часов
1	Меры защиты от утечки информации. Идентификация и аутентификация. Парольная аутентификация. Защита информации в компьютерных сетях. Объекты защиты информации в сети. Политика обеспечения конфиденциальной информации. Архивация файлов. Многотомный архив.	36
2	Национальные интересы и стратегические национальные приоритеты в соответствии с действующей Стратегией национальной безопасности Российской Федерации. Основные способы привлечения сотрудников государственных и коммерческих структур, имеющих доступ к интересующей информации.	36

3	Криптографическое преобразование информации. Электронная подпись. Использование ЭП в экономических системах. Методы шифрования с симметричным ключом и системы шифрования с открытым ключом.	30
4	Количественный подход к информационной безопасности. Оценка защищенности механизмов защиты. Формирование политики безопасности предприятия (организации).	30

4.4. Темы курсового проекта (курсовой работы)

Не предусмотрено планом

5.Учебно-методическое и информационное обеспечение дисциплины (модуля)

5.1. Учебно-методические рекомендации для студентов по изучению дисциплины (модуля)

Изучение дисциплины осуществляется в форме учебных занятий под руководством профессорско-преподавательского состава кафедры и самостоятельной подготовки обучаемых.
При проведении учебных занятий используются элементы классических и современных педагогических технологий, в том числе проблемного и проблемно-деятельностного обучения.
Предусматриваются следующие формы работы обучаемых:

- прослушивание лекционного курса;
- чтение и конспектирование рекомендованной литературы;
- проведение семинарских занятий (если предусмотрены рабочей программой) с более подробным рассмотрением ключевых проблем дисциплины;
- проведение практических занятий в компьютерных классах двумя преподавателями.

Помимо устного изложения материала, в процессе лекций предполагается использовать визуальную поддержку в виде мультимедийных презентаций содержания лекции, отражающих основные тезисы, понятия, схемы, иллюстрации, выдержки из учебных, документальных и художественных фильмов по теме лекции.
Тематика семинарских и практических занятий, а также методические указания для обучающихся, раскрывающие режим и характер проведения учебных занятий изложены в планах практических занятий по дисциплине.
При подготовке к семинарским и практическим занятиям обучаемые должны:

1. Ознакомиться с планом семинарского и практического занятия.
2. Уяснить содержание вопросов, вынесенных на обсуждение, или заданий, выполняемых на занятии.
3. Повторить содержание лекционного материала.
4. Подготовить ответы на вопросы, указанные в плане занятия.
5. Выполнить задания, обусловленные темой практического занятия.
6. Ознакомиться с кафедральными методическими рекомендациями к занятию, содержанием стендов и другими наглядными пособиями по теме занятия.
7. В целях самоконтроля ответить на вопросы, указанные в методических рекомендациях к занятию.
8. Получить консультацию у преподавателя.
9. Выполнить индивидуальные задания преподавателя.
10. Подготовить реферат или доклад (сообщение) (по согласованию с преподавателем).

Обязательным условием подготовки к занятию является выполнение в полном объеме заданий предыдущего занятия.

На занятиях рекомендуется активно использовать личный жизненный опыт, примеры из специальной литературы.
Готовясь к практическим занятиям, обучаемые должны изучить достижения естественных, гуманитарных и других наук, знание которых необходимо для разрешения практических вопросов;
На каждом занятии обучаемым необходимо иметь рабочую тетрадь, письменные принадлежности.
Рабочие тетради необходимы для конспектирования рекомендаций преподавателя по теме занятия.
При отработке пропущенных занятий обучаемые самостоятельно изучают вопросы, указанные в плане занятия. На консультации обучающиеся представляют конспекты ответов и решений задач и отвечают на вопросы преподавателя.
Контроль знаний обучающихся проводится в форме текущей и промежуточной аттестации.
Контроль текущей успеваемости обучающихся – текущая аттестация – проводится в ходе семестра с целью определения уровня усвоения обучающимися знаний; сформированности у них умений и навыков.
К контролю текущей успеваемости относятся проверка знаний, умений и навыков обучающихся:
- ✓ на занятиях;
- ✓ по результатам проведения контроля уровня усвоения знаний (с помощью тестовых заданий или контрольных вопросов);
- ✓ по результатам выполнения обучающимися индивидуальных заданий;
- ✓ по результатам проверки качества конспектов лекций и иных материалов;
- ✓ по результатам отчета обучающихся в ходе индивидуальной консультации преподавателя, проводимой в часы самоподготовки, по имеющимся задолженностям.

Контроль за выполнением обучающимися каждого вида работ может осуществляться поэтапно и служит основанием для промежуточной аттестации по дисциплине.
Промежуточная аттестация обучаемых проводится с целью выявления соответствия уровня теоретических знаний, практических умений и навыков обучаемых по дисциплине в форме дифференцированного зачета.
Для успешного освоения дисциплины студент должен изучить следующие элементы образовательного процесса:
- самостоятельное изучение разделов и тем курса по учебникам и учебным пособиям с последующей самопроверкой и решением типовых задач;
- индивидуальные консультации (очные и письменные);
- посещение практических занятий,
- сдача дифференциованного зачета по всему курсу.

Лекционные занятия (теоретический курс)

Лекции по курсу «Математические методы защиты информации» целесообразно проводить в аудитории, оснащённой проекционной аппаратурой для демонстрации заранее подготовленных компьютерных презентаций. Презентации должны содержать опорный материал для конспектирования: отражать логику изложения в виде иерархической структуры, содержать основные определения, табличный и графический иллюстрационный материал.
Методические указания студентам
Прорабатывая материал лекций, студент обязан отметить в конспекте утверждения, определения, выводы, смысл или обоснованность которых ему непонятны, и обратиться к рекомендуемой литературе за разъяснениями. Если рекомендуемая литература не содержит необходимых объяснений, необходимо обратиться к преподавателю с вопросом на семинарском занятии или во время, выделенное для индивидуальных консультаций.

Семинарские (практические) занятия

Практическое занятие является одной из форм проведения групповых занятий со студентами вузов, имеющей своими целями более глубокое усвоение обучаемыми лекционного материала,

развития у них умения целенаправленной работы с научной, учебной литературой для самостоятельного добывания новых знаний, приобретения навыков решения задач и т.д.
В ходе практического занятия во вступительном слове раскрыть теоретическую и практическую значимость темы практического занятия, определить порядок его проведения, время на выполнение каждого учебного вопроса. Целесообразно в ходе решения и обсуждения учебных вопросов задавать аудитории дополнительные и уточняющие вопросы с целью акцентирования внимания студентов на важные моменты и алгоритмы решения. Поощрять студентов, выполнивших задания качественно и раньше всех. Для наглядности и закрепления изучаемого материала преподаватель может использовать таблицы, схемы, карты, презентации.
В заключительной части практического занятия следует подвести его итоги: дать объективную оценку выступлений каждого студента и учебной группы в целом. Раскрыть положительные стороны и недостатки проведенного практического занятия. Ответить на вопросы студентов. Назвать тему очередного занятия.
При контроле знаний основное внимание уделяется способности студентов применять полученные знания на практических задачах. Поэтому при самостоятельной работе студент должен уделять внимание решению задач на ПК. При решении задач необходимо анализировать те или иные алгоритмы, которые применялись при решении подобных задач на аудиторных занятиях. Материал раздела курса можно усвоить только выполнив набор задач по данному разделу на ПК.
Рекомендации по темам:

№ п/п	Разделы (темы) дисциплины	Рекомендации
1.	Информационная безопасность и уровни ее обеспечения.	Поиск необходиомй информации по теме, создание презентации, подготовка сообщения по теме и демонстрация под управлением докладчика. Работа с лекционным материалом, изучение рекомендованной литературы, самостоятельный подбор необходимой литературы, поиск необходимой информации через Интернет. Доработка практических заданий.
2.	Государственная политика в обеспечении информационной безопасности.	Создание презентации, подготовка сообщения по теме и демонстрация под управлением докладчика. Работа с лекционным материалом, изучение рекомендованной литературы, самостоятельный подбор необходимой литературы, поиск необходимой информации через Интернет.
3.	Криптографические методы защиты информации.	Работа с лекционным материалом, изучение рекомендованной литературы. Доработка практических заданий, оформление отчетов по выполненным практическим работам.
4.	Аудит информационной безопасности. Анализ информационных рисков.	Работа с лекционным материалом. Доработка практических заданий, оформление отчетов по выполненным практическим работам, подготовка к защите. Подготовка и выполнение контрольной работы задания на практическую работу, тестовые задания, контрольное задание

Образовательные технологии, используемые для проведения семинаров в интерактивной форме:

Тестирование – контроль знаний с помощью тестов, которые состоят из условий (вопросов) и вариантов ответов для выбора (самостоятельная работа студентов).

Метод кейс-стадии – обучение, при котором студенты и преподаватели участвуют в непосредственном обсуждении деловых ситуаций или задач. При данном методе обучения студент самостоятельно вынужден принимать решение и обосновать его.

Учебно-методические рекомендации по выполнению различных форм самостоятельной работы

1) Учебно-методические рекомендации по изучению обучающимися вопросов, выносимых на самостоятельное изучение.

Виды и содержание самостоятельной работы студента по дисциплине:
- самостоятельная работа с книгой,
- самопроверка,
- выполнение упражнений (решение тестов),
- консультации

2) Учебно-методические рекомендации по выполнению отдельных форм самостоятельной работы.

Самостоятельная работа с книгой

Начинать изучение курса в целом или темы семинарского занятия необходимо с рассмотрения его содержания по программе, затем приступить к рассмотрению отдельных тем. Сначала знакомятся с содержащимися в данной теме вопросами, их последовательностью, а затем уже приступают к изучению содержания темы. При первом чтении необходимо получить общее представление об излагаемых вопросах. При повторном чтении необходимо параллельно вести конспект, в который заносить все основные понятия и закономерности рассматриваемой темы, зависимости и их выводы; впервые встретившиеся термины с краткими пояснениями их сущности. По возможности старайтесь систематизировать материал, представляйте его в виде графиков, схем, диаграмм, таблиц - это облегчает запоминание материала и позволяет легко восстановить его в памяти при повторном обращении. Не старайтесь наполнить конспект отдельными фактами и цифрами, их всегда можно отыскать в соответствующих справочных материалах. Вникайте в сущность того или иного вопроса - это способствует более глубокому и прочному усвоению материала.

Переходить к изучению новой темы следует только после полного изучения теоретических вопросов, выполнения самопроверки и выполнения заданий по предыдущей теме.

Самопроверка

Закончив изучение темы, ответьте на вопросы для самопроверки, которые акцентируют внимание на наиболее важных вопросах темы. При этом старайтесь не пользоваться конспектом или учебником. Частое обращение к конспекту показывает недостаточное усвоение основных вопросов темы. Необходимость частого обращения к учебнику показывает неумение правильно конспектировать основные понятия и закономерности темы. Внесите коррективы в конспект, который впоследствии поможет при повторении материала в период подготовки к экзамену.

Выполнение упражнений (решение тестов)

Для более прочного усвоения теоретического материала после самопроверки необходимо выполнить упражнения и ответить на вопросы тестов по пройденной теме.

Консультации

При возникновении затруднений при изучении теоретической части курса, ответов на вопросы для самопроверки или решении задач, следует обращаться за письменной или устной консультацией к преподавателю в институт. При этом необходимо точно указать вопрос, вызывающий затруднение, место в учебнике, где он разбирается.

Виды и содержание самостоятельной работы студентов по дисциплине, формы контроля.

Одним из основных видов деятельности студента является **самостоятельная работа,** которая включает в себя изучение лекционного материала, учебников и учебных пособий, первоисточников, подготовку сообщений, выступления на групповых занятиях, выполнение

индивидуальных домашних заданий.
Методика самостоятельной работы предварительно разъясняется преподавателем и в последующем может уточняться с учетом индивидуальных особенностей студентов. Время и место самостоятельной работы выбираются студентами по своему усмотрению с учетом рекомендаций преподавателя.
Самостоятельную работу над дисциплиной следует начинать с изучения программы, которая содержит основные требования к знаниям, умениям и навыкам обучаемых. Следует обязательно вспомнить рекомендации преподавателя, данные в ходе установочных занятий. Затем следует приступать к изучению отдельных разделов и тем в порядке, предусмотренном программой.
Самостоятельная работа студентов проводится в следующих формах:
А) письменные работы по заданиям, определенным в данных методических рекомендациях, а также иным заданиям, составленным преподавателем.
Б) выполнение тестовых заданий.
В) выполнение эссе.
Г) контрольные работы для студентов-заочников
Д) решение заданий в форме задач.

Особенности в организации самостоятельной работы у студентов.

Подготовительный этап. По зачислению на очередной курс следует провести подготовку к началу обучения. Эта подготовка в самом общем включает несколько необходимых пунктов.

1) Следует убедиться в наличии необходимых методических указаний и программ по каждому предмету и ясного понимания требований, предъявляемых программами учебных дисциплин. При необходимости надлежит получить на кафедре необходимые указания и консультации, контрольные вопросы для изучения дисциплины.
2) Необходимо создать (рационально и эмоционально) максимально высокий уровень мотивации к последовательному и планомерному изучению дисциплины.
3) Необходимо изучить список рекомендованной основной и дополнительной литературы и убедиться в ее наличии у себя дома или в библиотеке в бумажном или электронном виде.
4) Необходимо иметь «под рукой» специальные и универсальные словари и энциклопедии, для того, чтобы постоянно уточнять значения используемых терминов и понятий. Пользование словарями и справочниками необходимо сделать привычкой. Опыт показывает, что неудовлетворительное усвоение предмета зачастую коренится в неточном, смутном или неправильном понимании и употреблении понятийного.
5) Желательно в самом начале периода обучения возможно тщательнее спланировать время, отводимое на самостоятельную работу с источниками и литературой по дисциплине, представить этот план в наглядной форме (график работы с датами) и в дальнейшем его придерживаться, не допуская срывов графика индивидуальной работы и аврала в предсессионный период. Пренебрежение этим пунктом приводит к переутомлению и резкому снижению качества усвоения учебного материала.

Общие методические рекомендации по организации самостоятельной работы студентов. (Работа с учебной литературой)
Получив представление об основном содержании раздела, темы, необходимо изучить материал с помощью учебника. Целесообразно составить краткий конспект или схему, отображающую смысл и связи основных понятий данного раздела и включенных в него тем. Обязательно следует записывать возникшие вопросы, на которые не удалось ответить самостоятельно.

Некоторые общие рекомендации по изучению литературы.

1) Всю учебную литературу желательно изучать «под конспект». Чтение литературы, не

сопровождаемое конспектированием, даже пусть самым кратким – крайне бесполезная работа. Цель написания конспекта по дисциплине – сформировать навыки по поиску, отбору, анализу и формулированию учебного материала. Эти навыки обязательны для любого специалиста с высшим образованием независимо от выбранной специальности.

2) Написание конспекта должно быть творческим – нужно не переписывать текст из источников, но пытаться кратко излагать своими словами содержание ответа, при этом максимально структурируя его и используя символы и условные обозначения. Копирование и заучивание неосмысленного текста трудоемко и по большому счету не имеет большой познавательной и практической ценности.

3) При написании конспекта используется тетрадь, поля в которой обязательны. Страницы нумеруются, каждый новый вопрос начинается с нового листа, для каждого экзаменационного вопроса отводится 1-2 страницы конспекта. Общая тетрадь позволяет создавать конспекты блоками. Поскольку часть вопросов в этих дисциплинах отчасти перекрывается, отчасти дополняя друг друга, в ряде случаев бывает достаточно сослаться на соответствующие страницы конспекта, а не переписывать их заново. На полях размещается вся вспомогательная информация – ссылки, вопросы, условные обозначения и т.д.

4) В идеале должен получиться полный конспект по программе курса, с выделенными определениями, узловыми пунктами, примерами, неясными моментами, проставленными на полях вопросами.

5) При работе над конспектом обязательно выявляются и отмечаются трудные для самостоятельного изучения вопросы, с которыми уместно обратиться к преподавателю при посещении установочных лекций и консультаций, либо в индивидуальном порядке.

6) При чтении учебной и научной литературы всегда следить за точным и полным пониманием значения терминов и содержания понятий, используемых в тексте. Постоянно следует уточнять значения по словарям или энциклопедиям, при необходимости их записывать.

7) При написании учебного конспекта обязательно указывать все прорабатываемые источники с указанием автора, названия, даты и места издания, а также с указанием использованных страниц.

Чтение учебника (учебного пособия).

Необходимо помнить, что работа с учебником – только начальный этап изучения дисциплины.

1) Учебник ориентирует в основных понятиях и категориях дисциплины, дает частичные сведения об истории их возникновения и включения в научный оборот.

2) Учебник очерчивает круг обязательных знаний по предмету, не претендуя на раскрытие и подробное доказательство логики их происхождения.

3) Учебник предназначен не для заучивания, а для ориентации в проблемном поле учебной дисциплины. Из-за краткости изложения в учебнике иногда может оказаться непонятным тот или иной раздел или пункт.

4) Отдельные пункты и даже разделы учебной программы могут отсутствовать в тексте учебника.

При чтении могут встретиться непонятные слова, термины и определения. В этих случаях следует обратиться к справочнику или соответствующему словарю. Не следует при чтении пропускать сноски и примечания, т.к. в них разъясняются отдельные места, дополняются сжато изложенные в тексте положения.

При чтении необходимо выделить основную мысль, представить прочитанное как единое целое. Это легче сделать, если студент при чтении каждого параграфа (раздела) сам себе ответит на вопросы, о чем говорится в данной части текста, чем сказанное подтверждается или поясняется.

Чтение рекомендованной дополнительной учебной и научной литературы одна из важных частей самостоятельной учебы студента, которая обеспечивает глубокое и прочное усвоение

материала по юриспруденции. Некоторые соображения:

1) Самостоятельное изучение и конспектирование рекомендованной литературы обычно приводит к знанию ответов на все вопросы, выносимые на экзамен.
2) Чтение и конспектирование литературы осуществляется не по принципу «книга за книгой», а «вопрос за вопросом» в соответствии с программой курса, при этом выделяются различные подходы к освещению одного и того же вопроса у различных авторов.
3) Изучение научной литературы должно сопровождаться поиском и фиксацией примеров, иллюстрирующих то или иное теоретическое положение.
4) При изучении дополнительной научной литературы особое внимание нужно уделить проработке проблемно ориентированных заданий семинарских (практических) занятий, включенных в программу и/или в текст учебника или пособия.

Заключительным этапом изучения учебника, книги или статьи является запись, конспектирование прочитанного. Конспект позволяет быстро восстановить в памяти содержание прочитанной книги. Кроме того, процесс конспектирования организует мысль, которая побуждает читающего к обдумыванию, к активному мышлению, улучшает качество усвоения и запоминания. Запись способствует выработке ясно, четко и лаконично формулировать и излагать мысль. Запись следует вести сжато и обязательно своими словами.

Существуют три основные формы записи прочитанного: план, тезисы, конспект.

План – самая короткая форма записи прочитанного. Различают план простой и развернутый. Простой план включает перечень заголовков или вопросов, о которых говорится в главе (параграфе или статье), расположенных в том же порядке, что и в книге. Развернутый план - это такой план, в котором каждый вопрос разбит на подвопросы.

Тезисы представляют собой запись основных положений и идей, изложенных в книге или статье, и являются более полным раскрытием плана.

Конспект – это сжатое логически связанное изложение прочитанного материала. В конспекте помещаются не только главные положения книги, но и аргументы (цифры, примеры, таблицы и т.д.).

Таким образом, самостоятельная работа студентов является одним из видов учебных занятий и она в значительной мере определяет успех обучения в институте. Самостоятельная работа способствует приобретению глубоких и прочных знаний по юриспруденции, вырабатывает умение ориентироваться в огромном потоке информации и дает навыки работы с учебной и научной литературой. Самостоятельная работа приучает делать обобщения и выводы, вырабатывает умение логично излагать изучаемый материал, формирует у студентов творческий подход, способствует использованию полученных знаний для разнообразных практических задач, развивает самостоятельность в принятии решений.

Поиск литературы можно осуществлять по электронным каталогам сайтов известных в России библиотек.

Рекомендации по выполнению тестовых заданий.

Целью выполнения тестовых заданий является формирование у студентов навыков самостоятельного выбора ответов из нескольких вариантов, определения соответствия, либо нахождения не обозначенного ответа, расположения по определенному порядку и обоснования их в соответствии со знанием системы категорий настоящей дисциплины.

Выполнение тестовых заданий должно способствовать повышению теоретической и профессиональной подготовки студентов, лучшему освоению учебного материала, углубленному рассмотрению содержания тем дисциплины. При выполнении тестовых заданий студенты, должны показать умение работать с научной литературой, делать обоснованные выводы.

Приступая к выполнению тестовых заданий, студент должен, прежде всего, уяснить суть предложенного вопроса, внимательно прочитать предлагаемые ответы, проанализировать выбранный ответ с точки зрения знаний, полученных в период обучения.

Рекомендации по подготовке презентации

Подготовительный этап

Прежде чем начинать работу над презентацией, необходимо поставить перед собой **цель** этой **презентации**. Подумайте, для чего Вы это делаете, каких результатов хотите достичь и что Вам для этого может понадобиться. После этого тщательно **изучите** всю имеющуюся у Вас **информацию** по теме презентации, отметьте те важные моменты, которые смогут послужить базой для аргументации вашей позиции. Чем большим количеством информации Вы будете владеть, тем легче Вам будет в дальнейшем. Подумайте, какие средства можно использовать, для того чтобы скрыть или *завуалировать негативные моменты* и, напротив, сделать акцент на положительных сторонах в процессе презентации. Изучите целевую аудиторию, на которую направлена Ваша презентация.

Теперь необходимо понять, в каком виде Вы будете презентовать имеющуюся у Вас информацию. Выбор формата презентации зависит от того материала, который Вам необходимо представить аудитории. Возможно понадобится и распечатанный наглядный материал. Важно отметить, что весь раздаточный материал должен выглядеть презентабельно, чтобы его было приятно взять в руки. Если вы используете цветные распечатки для презентации визуального материала, то важную роль будет играть качество распечаток, они должны правильно передавать цветовые характеристики изображения, лучше всего наклеивать цветные распечатки на плотный картон, для того чтобы материалы можно было расставить в случае необходимости.

Подготовка презентации

- Выберите **программу**, в которой вы будете работать: *Microsoft Power Point* или программы, которые позволяют сделать мультимедийную презентацию с использованием Flash-технологии.
- Набросайте **структуру** презентации, она будет отражать Вашу логику и позволит понять объем презентации. Заполняя слайды структуры, вы всегда будете понимать, сколько вам еще слайдов необходимо заполнить, какой еще материал вам необходимо найти и разместить. Продумайте о чем вы будете рассказывать в начале, середине и конце презентации. На какие моменты нужно сделать больший фокус с использованием иллюстраций и примеров, а какие можно обобщить на одном слайде и коротко перечислить.
- Составьте **план** презентации по времени на каждый смысловой блок (учитывайте временные рамки активного внимания человека) и уже после этого делайте анимацию в необходимых местах. **Анимация в презентации** имеет очень большое значение, она делает её более динамичной и интересной, помогает расставить акценты и визуально оформить логику вашего изложения. Самой большой ошибкой является чрезмерное использование анимации, которое усложняет презентацию, тормозит вас в процессе изложения и самое главное *отвлекает от основной информации*.
- Разместите материал и текстовую информацию в презентации в соответствии с вашим планом и структурой. Контекст презентации должен быть детально продуман Вами. Вспомните всю ту информацию, которую Вы изучили перед написанием презентации, и поставьте себя на место аудитории: какие вопросы по тексту презентации могут возникнуть, насколько разработанный материал или идеи соответствуют ожиданиям. Постарайтесь сами себе ответить на эти вопросы и продумайте аргументацию Вашей позиции (от самых слабых аргументов к более сильным). И помните, самой продуманной презентацией является та, где Вы готовы ответить за каждое свое слово. Если Вы используете в контексте презентации выжимки из каких-либо информационных источников, то необходимо обязательно ссылаться на них в презентации. Это *повысит доверие аудитории к информации*, которую Вы представляете.

Логическая последовательность создания презентации

1. Структуризация учебного материала.

2. Составление сценария презентации.
3. Разработкой дизайна мультимедийного пособия.
4. Подготовка медиафрагментов (аудио, видео, анимация, текст).
5. Проверка на работоспособность всех элементов презентации.

Мультимедийная презентация должна обладать следующими качествами:

1. Удобной системой навигации, позволяющей легко перемещаться по презентации.
2. Использованием мультимедийных возможностей современных компьютеров и Интернет (графических вставок, анимации, звука если необходимо и др.).
3. Разбивка занятия на небольшие логически замкнутые блоки (слайды). Каждый слайд презентации должен иметь заголовок.
4. Научностью (наличие ссылок на литературные источники, электронные библиотеки и на источники информации в сети Интернет).
5. Доступностью - быстрая загрузка, без усложнения эффектами.

При создании мультимедийной презентаций необходимо:

- Провести разбивку занятия на небольшие смысловые части – модули. Подобрать для каждого модуля соответствующую форму выражения и предъявления обучаемым заголовка раздела, текстов, рисунков, таблиц, графиков, звукового и видеоряда и т.п. (согласно содержанию);
- Моделировать познавательную деятельность обучаемых при изучении раздела и использовать результаты при его составлении (определяется основная последовательность перехода между слайдами);
- Проектировать способы закрепления знаний и навыков и осуществления обратной связи (подбор задач, контрольных вопросов, заданий для моделирования, разработка способов анализа ответов, реплик на типичные неправильные ответы, составление подсказок (help);
- Составлять тексты, разработать рисунки, таблицы, схемы, чертежи, видеоряд, согласно требованиям эргономики; скомпоновать модули каждого раздела занятия с эргономической точки зрения.

Каждый модуль по максимуму включает в себя:

- Цели изучения модуля
- Учебные вопросы
- Учебный материал
- Набор ключевых проблем по теме модуля
- Вопросы для самопроверки (желательно с ответами, комментариями и рекомендациями)
- Структурно-логическую схему модуля
- Список литературы к модулю и ссылки на сайты по тематике модуля.

Рекомендации по подготовке контрольной работы (реферата).

Написание реферата является важным средством самостоятельного изучения учебных дисциплин и формой учебной отчетности. Их выполнение способствует повышению уровня теоретических знаний и практических навыков.

Подготовка состоит из нескольких этапов:

- выбор темы и составление плана работы;
- подбор и изучение литературы;
- составление библиографии;
- набор и форматирование текста на компьютере (контрольная работа по данной учебной дисциплине представляется в распечатанном виде).

Рефераты должны быть выполнены на компьютере, оформлены в соответствии с методическими рекомендациями по оформлению письменных работ (и в *обязательном* порядке должны содержать титульный лист, рубрики: содержание (оглавление), введение, основную часть, заключение (***творческие*** выводы), список литературы (включая обязательно литературу кафедры и академии согласно УМК по учебной дисциплине), содержащий не менее трёх

наименований со *ссылками* в тексте). Объём реферата: от 10 до 15 страниц машинописного текста (гарнитура *Times New Roman*).
На все литературные источники (*учебная, научная и специальная* литература) в тексте реферата (статьи) должны быть ссылки в виде: [N], где N – номер источника в библиографии (списке литературы). На все иные источники (публицистическая, правовая, справочная, энциклопедическая и др. литература; интернет-ресурсы) – сквозные сноски внизу страниц.
Список использованной учебной, научной и специальной литературы должен соответствовать требованиям ГОСТ 7.1–2003 – «Библиографическое описание».
Студент в *обязательном порядке* должен изучить и включить в библиографию (в список литературы) соответствующую теме реферата научную и учебно-методическую литературу кафедры (включая преподавателя, ведущего учебные занятия) и академии, начиная с Рабочей программы учебной дисциплины:
Вспомогательную литературу включать в библиографию в соответствии с рекомендованным в Приложении к рабочей программе № 1 списком научной и и учебно-методической литературы.

Количество использованных источников: не менее 3 за последние 3 года.
Процедура доклада:
- устное выступление,
- презентация с последующим обсуждением.

Контрольные вопросы для самоподготовки:

1. Понятие информации, информационной сферы, безопасности информации и информационной безопасности субъекта.
2. Основные составляющие национальных интересов в информационной сфере (на примере Российской Федерации).
3. Виды и источники угроз информационной безопасности страны (на примере Российской Федерации).
4. Принципы государственной политики обеспечения информационной безопасности страны (на примере Российской Федерации).
5. Защита информации. Комплексный подход к защите информации.
6. Классификация методов защиты информации.
7. Понятие и виды каналов утечки информации ограниченного доступа.
8. Условия и факторы, способствующие утечке информации ограниченного доступа.
9. Основные угрозы безопасности информации. Общая характеристика технических средств несанкционированного получения информации и технологий их применения.
10. Основные направления инженерно-технической защиты информации: физическая защита, скрытие информации, поиск и нейтрализация источников утечки.
11. Распространённые способы блокирования каналов утечки информации и виды специальных технических средств защиты.
12. Уязвимость компьютерных систем. Понятие несанкционированного доступа. Классы и виды несанкционированного доступа.
13. Уязвимость компьютерных систем. Модель злоумышленника.
14. Понятие «идентификации пользователя». Задача идентификации пользователя. Использование идентификации в защите информационных процессов.
15. Методы и средства защиты данных от несанкционированного доступа.
16. Основные методы несанкционированного доступа при физическом контакте с компьютером.
17. Классический алгоритм поведения злоумышленника при удаленном несанкционированном доступе в компьютерную систему.
18. Основные причины утечки информации с охраняемых объектов.

19. Разграничение доступа к информации. Идентификация и аутентификация.
20. Криптографические методы защиты данных.
21. Основные угрозы безопасности информации в компьютерных системах.
22. Угрозы безопасности современных информационно-вычислительных и телекоммуникационных сетей. Классификация угроз безопасности.

Содержание тем семинарских (практических) занятий.

Тема1. Информационная безопасность и уровни ее обеспечения.

Направления обеспечения безопасности вообще рассматриваются как нормативно-правовые категории, определяющие комплексные меры защиты информации на государственном уровне, на уровне предприятия и организации, на уровне отдельной личности.

Система защиты информации как любая система должна иметь определенные виды собственного обеспечения, опираясь на которые она будет выполнять свою целевую функцию. С учетом этого СЗИ может иметь:

– правовое обеспечение. Сюда входят нормативные документы, положения, инструкции, руководства, требования которых являются обязательными в рамках сферы их действий;

– организационное обеспечение. Имеется в виду, что реализация защиты информации осуществляется определенными структурными единицами – такими, как служба защиты документов; служба режима, допуска, охраны; служба защиты информации техническими средствами; информационно-аналитическая деятельность и др.;

– аппаратное обеспечение. Предполагается широкое использование технических средств как для защиты информации, так и для обеспечения деятельности собственно СЗИ;

– информационное обеспечение. Оно включает в себя сведения, данные, показатели, параметры, лежащие в основе решения задач, обеспечивающих функционирование системы. Сюда могут входить как показатели доступа, учета, хранения, так и системы информационного обеспечения расчетных задач различного характера, связанных с деятельностью службы обеспечения безопасности;

– программное обеспечение. К нему относятся различные информационные, учетные, статистические и расчетные программы, обеспечивающие оценку наличия и опасности различных каналов утечки и 11 путей несанкционированного проникновения к источникам конфиденциальной информации;

– математическое обеспечение. Предполагает использование математических методов для различных расчетов, связанных с оценкой опасности технических средств злоумышленников, зон и норм необходимой защиты;

– лингвистическое обеспечение. Совокупность специальных языковых средств общения специалистов и пользователей в сфере защиты информации;

– нормативно-методическое обеспечение. Сюда входят нормы и регламенты деятельности органов, служб, средств, реализующих функции защиты информации, различного рода методики, обеспечивающие деятельность пользователей при выполнении своей работы в условиях жестких требований защиты информации.

Удовлетворить современные требования по обеспечению безопасности предприятия и защиты его конфиденциальной информации может только система безопасности.

Под системой безопасности будем понимать организованную совокупность специальных органов, служб, средств, методов и мероприятий, обеспечивающих защиту жизненно важных интересов личности, предприятия и государства от внутренних и внешних угроз. Кроме этого, защитные действия, ориентированные на обеспечение информационной безопасности, могут быть охарактеризованы целым рядом параметров, отражающих, помимо направлений, ориентацию на объекты защиты, характер угроз, способы действий, их распространенность, охват и масштабность.

Так, по характеру угроз защитные действия ориентированы на защиту информации от разглашения, утечки и несанкционированного доступа. По способам действий их можно подразделить на предупреждение, выявление, обнаружение, пресечение и восстановление

ущерба или иных убытков. По охвату защитные действия могут быть ориентированы на территорию, здание, помещение, аппаратуру или отдельные элементы аппаратуры. Масштабность защитных мероприятий характеризуется как объектовая, групповая или индивидуальная защита.

Архивация файлов. Архиваторы.

Архивация (упаковка) — помещение (загрузка) исходных файлов в архивный файл в сжатом или несжатом виде.

Архивация предназначена для создания резервных копий используемых файлов, на случай потери или порчи по каким-либо причинам основной копии (невнимательность пользователя, повреждение магнитного диска, заражение вирусом и т.д.).

Для архивации используются специальные программы, архиваторы, осуществляющие упаковку и позволяющие уменьшать размер архива, по сравнению с оригиналом, примерно в два и более раз.

Архиваторы позволяют защищать созданные ими архивы паролем, сохранять и восстанавливать структуру подкаталогов, записывать большой архивный файл на несколько дисков (многотомный архив).

Сжиматься могут как один, так и несколько файлов, которые в сжатом виде помещаются в так называемый архивный файл или архив.

Программы большого объема, распространяемые на дискетах, также находятся на них в виде архивов.

Архивный файл — это специальным образом организованный файл, содержащий в себе один или несколько файлов в сжатом или несжатом виде и служебную информацию об именах файлов, дате и времени их создания или модификации.

Выигрыш в размере архива достигается за счет замены часто встречающихся в файле последовательностей кодов на ссылки к первой обнаруженной последовательности и использования алгоритмов сжатия информации.

Степень сжатия зависит от используемой программы, метода сжатия и типа исходного файла. Наиболее хорошо сжимаются файлы графических образов, текстовые файлы и файлы данных, для которых степень сжатия может достигать 5 - 40%, меньше сжимаются файлы исполняемых программ и загрузочных модулей — 60 - 90%. Почти не сжимаются архивные файлы. Программы для архивации отличаются используемыми методами сжатия, что соответственно влияет на степень сжатия.

Для того чтобы воспользоваться информацией, запакованной в архив, необходимо архив раскрыть или распаковать. Это делается либо той же программой-архиватором, либо парной к ней программой-разархиватором.

Разархивация (распаковка) — процесс восстановления файлов из архива в первоначальном виде. При распаковке файлы извлекаются из архива и помещаются на диск или в оперативную память.

Самораспаковывающийся архивный файл — это загрузочный, исполняемый модуль, который способен к самостоятельной разархивации находящихся в нем файлов без использования программы-архиватора.

Самораспаковывающийся архив получил название SFX-архив (SelF-eXtracting). Архивы такого типа в обычно создаются в форме *.EXE-файла.*

Архиваторы, служащие для сжатия и хранения информации, обеспечивают представление в едином архивном файле одного или нескольких файлов, каждый из которых может быть при необходимости извлечен в первоначальном виде.

В оглавлении архивного файла для каждого содержащегося в нем файла хранится следующая информация:

- имя файла;
- сведения о каталоге, в котором содержится файл;
- дата и время последней модификации файла;

- размер файла на диске и в архиве;
- код циклического контроля для каждого файла, используемый для проверки целостности архива.

Архиваторы имеют следующие функциональные возможности:

1. Уменьшение требуемого объема памяти для хранения файлов от 20% до 90% первоначального объема.
2. Обновление в архиве только тех файлов, которые изменялись со времени их последнего занесения в архив, т.е. программа-упаковщик сама следит за изменениями, внесенными пользователем в архивируемые файлы, и помещает в архив только новые и измененные файлы.
3. Объединение группы файлов с сохранением в архиве имен директорий с именами файлов, что позволяет при разархивации восстанавливать полную структуру директорий и файлов.
4. Написания комментариев к архиву и файлам в архиве.
5. Создание саморазархивируемых архивов, которые для извлечения файлов не требуют наличия самого архиватора.
6. Создание многотомных архивов – последовательности архивных файлов. Многотомные архивы предназначены для архивации больших комплексов файлов.

Тема 2. Государственная политика обеспечения информационной безопасности РФ

Под ***информационной безопасностью*** Российской Федерации понимается **состояние защищенности** основных интересов личности, общества и государства в информационной сфере, связанных с поиском, получением, передачей, распространением, производством, обработкой, хранением и использованием информации.

Интересы личности в информационной сфере на современном этапе состоят в реальном обеспечении конституционных прав человека и гражданина на доступ к информации, на использование информации в интересах осуществления не запрещенной законом деятельности, а также в защите информации, обеспечивающей личную безопасность.

Интересы общества в информационной сфере заключаются в защите интересов личности в этой сфере, обеспечении реализации конституционных прав и свобод человека и гражданина в целях упрочения демократии, достижения поддержания общественного согласия, повышении созидательной активности населения, духовного возрождения России.

Интересы государства в информационной сфере состоят в создании условий для гармоничного развития российской информационной инфраструктуры, для реализации прав и свобод человека и гражданина, в целях укрепления конституционного строя, упрочения суверенитета и сохранения территориальной целостности России, для установления политической и социальной стабильности, экономического процветания, а также в защите государственной тайны, безусловном исполнении законодательства и поддержании правопорядка, развитии международного сотрудничества на основе партнерства и интересов России.

Совокупность основных интересов личности, общества и государства определяет основные интересы Российской Федерации в информационной сфере. На их основе формируются стратегические текущие задачи внутренней и внешней политики государства в области обеспечения информационной безопасности.

Информационная безопасность играет ключевую роль в обеспечении жизненно важных интересов РФ. Являясь самостоятельной составляющей национальной безопасности, информационная безопасность в то же время оказывает непосредственное влияние на защищенность интересов РФ в различных сферах жизни общества.

Государственная политика обеспечения информационной безопасности Российской Федерации определяет основные направления деятельности федеральных органов государственной власти и органов государственной власти субъектов Российской Федерации в этой области, порядок закрепления их обязанностей по защите интересов Российской

Федерации в информационной сфере в рамках направлений их деятельности и базируется на соблюдении баланса интересов личности, общества и государства в информационной сфере.
Государственная политика обеспечения информационной безопасности Российской Федерации основывается на следующих **основных принципах:**
- соблюдение Конституции Российской Федерации, законодательства Российской Федерации, общепризнанных принципов и норм международного права при осуществлении деятельности по обеспечению информационной безопасности Российской Федерации;
- открытость в реализации функций федеральных органов государственной власти, органов государственной власти субъектов Российской Федерации и общественных объединений, предусматривающая информирование общества об их деятельности с учетом ограничений, установленных законодательством Российской Федерации;
- правовое равенство всех участников процесса информационного взаимодействия вне зависимости от их политического, социального и экономического статуса, основывающееся на конституционном праве граждан на свободный поиск, получение, передачу, производство и распространение информации любым законным способом;
- приоритетное развитие отечественных современных информационных и телекоммуникационных технологий, производство технических и программных средств, способных обеспечить совершенствование национальных телекоммуникационных сетей, их подключение к глобальным информационным сетям в целях соблюдения жизненно важных интересов Российской Федерации.
Государственная политика является открытой и предусматривает информированность общества о деятельности государственных органов и общественных институтов в области информационной безопасности с учётом ограничений, предусмотренных действующим законодательством.
Государственная политика исходит из принципа безусловного правового равенства всех участников процесса информационного взаимодействия вне зависимости от их политического, социального и экономического статуса. Она основывается на обязательном обеспечении прав граждан и организаций на свободное создание, поиск, получение и распространение информации любым законным способом. В этих целях государство совершенствует существующее и разрабатывает новое законодательство и нормативно-правовую базу информационных отношений в обществе, а также осуществляет контроль за безусловным их исполнением.
Государство исходит из того, что информационные ресурсы являются объектом собственности, способствует введению их в хозяйственный оборот при соблюдении законных интересов собственников, владельцев и распорядителей информационных ресурсов.
Государство считает приоритетным развитие современных информационных и телекоммуникационных технологий и технических средств, способных обеспечить создание национальных телекоммуникационных сетей и включение России в глобальные информационные сети и системы мониторинга.
Исходя из принципа разделения ответственности между органами федеральной, региональной власти и местного самоуправления, государственная политика предусматривает согласованность организационных и технических решений, принимаемых этими органами для обеспечения информационной безопасности в рамках единого информационного пространства России.

Государственная информационная политика. Информационная безопасность в системе национальной безопасности.

Государство должно играть ведущую роль в формировании концепции государственной политики и в ряде других вопросов, но вместе с тем некоторые вопросы обеспечения информационной безопасности должны развиваться гражданами России, объединениями и т. д. и должен финансироваться за счет средств негосударственных структур.
Правовые методы предусматривают разработку правовых актов, регламентирующих отношения в информационной сфере, нормативно-методических документов по вопросам

обеспечения информационной безопасности. Наиболее важными направлениями этой деятельности являются:
— внесение изменений и дополнений в действующее законодательство, регулирующее отношения в области обеспечения информационной безопасности в целях создания и совершенствования федеральной системы обеспечения информационной безопасности, устранения внутренних противоречий федерального законодательства, внутренних противоречий, связанных с международными соглашениями, к которым присоединилась РФ, а также в целях конкретизации норм ответственности за правонарушения в области обеспечения информационной безопасности,
— законодательное разграничение полномочий в области обеспечения информационной безопасности между федеральными органами государственной власти и органами субъектов РФ, определение целей, задач, механизмов, участие в этой деятельности общественных объединений, организаций и граждан,
— разработка и принятие нормативно-правовых актов, устанавливающих ответственность физических и юридических лиц за несанкционированный доступ к информации, ее противоправное копирование, искажение, противозаконное использование, преднамеренное распространение недостоверной информации, противоправное раскрытие конфиденциальной информации, использование в преступных целях служебной информации, содержащей коммерческую тайну,
— уточнение в интересах РФ правового статуса иностранных информационных агентств, СМИ и журналистов, а также инвесторов при привлечении иностранных инвестиций для развития информационной инфраструктуры России,
— законодательное закрепление приоритета развития национальных сетей связи отечественного производства, космических спутников связи,
— определение правового статуса организаций, предоставляющих услугу глобальных информационно-телекоммуникационных сетей на территории РФ и правовое регулирование этих организаций,
— создание правовой базы для формирования в РФ региональных структур обеспечения информационной безопасности.
Организационно-технические методы предусматривают создание и совершенствование федеральной системы обеспечения информационной безопасности, правоприменительную деятельность исполнительных и судебных органов государственной власти, разработку, совершенствование и использование средств защиты информации, методов контроля эффективности этих средств; создание системы средств предотвращения несанкционированного доступа к обрабатываемой информации специальных воздействий; выявление вредных технических устройств и программ; предотвращения перехвата информации по техническим каналам; сертификацию средств защиты информации; лицензирование деятельности в области защиты государственной тайны и области защиты информации, стандартизацию способов и средств защиты информации.
Экономические методы предусматривают разработку программ обеспечения информационной безопасности, определение порядка их финансирования, совершенствование структуры финансирования работ, связанных с реализацией правовых и организационно-технических методов защиты информации, создание системы страхования информационных рисков физических и юридических лиц.
Компетенция основных элементов организационной основы системы обеспечения информационной безопасности РФ, ее подсистема определяется федеральными законами, нормативно-правовыми актами Президента Правительства РФ.
Система обеспечения информационной безопасности является частью системы национальной безопасности. Эту систему составляют: Президент РФ, Совет Безопасности РФ, Федеральное Собрание РФ, Правительство РФ, федеральные органы исполнительной власти и органы государственной власти субъектов РФ, органы местного самоуправления, предприятия, учреждения, организации независимо от формы собственности, осуществляющие работы

использованием сведений, отнесенных к государственной тайне или специализирующиеся на проведении работ в области защиты информации.
В настоящее время разработка государственной политики по обеспечению информационной безопасности выдвигается в разряд приоритетных явлений национальной безопасности. Четкая государственная политика в области обеспечения информационной безопасности по предотвращению актуальных угроз позволит обеспечить развитие отечественной индустрии информации на мировом уровне и достичь необходимого уровня обеспечения безопасности информационных и телекоммуникационных систем как развернутых, так и создаваемых на территории России.

Тема 3. Криптографические методы защиты информации.

Криптографическое преобразование информации.

Шифрование данных (криптография) – это преобразование информации в другую форму или код таким образом, что доступ к ней сможет получить только тот пользователь, у которого есть секретный ключ,
В настоящее время шифрование данных является одним из самых популярных и эффективных методов защиты. Существуют три основных типа шифрования:
Симметричное шифрование: стороннему лицу может быть известен алгоритм шифрования, но неизвестна небольшая часть секретной информации - ключа, одинакового для отправителя и получателя сообщения.
Асимметричное шифрование: стороннему лицу может быть известен алгоритм шифрования, и, возможно, открытый ключ, но неизвестен закрытый ключ, известный только получателю сообщения.
Сквозное - способ передачи данных, в котором только пользователи, участвующие в общении, имеют доступ к сообщениям.
Цель шифрования – обеспечение конфиденциальности цифровых данных. Поскольку вся информация хранится на компьютерах и передается по сети Интернет, она уязвима к различного рода атакам. Ранее для шифрования использовался метод DES, разработанный в 70-ых годах, сейчас он считается устаревшим. На смену ему пришли более сложные современные алгоритмы.
Асимметричное шифрование, или криптографическая система с открытым ключом, представляет собой криптографическую систему, использующую открытые (public key) и закрытые (private key) ключи для шифрования и расшифровки данных. Эти ключи образуют так называемую ключевую пару и представляют собой большие числа, которые связаны некоторой зависимостью, но отличаются друг от друга.
Открытый ключ передается по незащищенным каналам связи и известен всем. С помощью открытого ключа осуществляется шифрование данных и проверка электронной подписи документов (ЭП).
Для расшифровки данных используется закрытый ключ, который хранится в тайне. Таким образом, главным преимуществом асимметричного шифрования по сравнению с симметричным шифрованием является возможность сторон связываться и обмениваться данными друг с другом без использования секретных каналов связи.
В симметричном шифровании используется всего один пароль (или как его еще называют ключ). Рассмотрим как все происходит. Есть некоторый математический алгоритм шифрования, которому на вход подается пароль и текст. На выходе получается зашифрованный текст. Чтобы получить исходный текст, используется этот же пароль, но с алгоритмом дешифрования (иногда он может совпадать).
Другими словами, стоит кому-либо узнать этот пароль, как безопасность тут же нарушается. Поэтому если используется симметричное шифрование, немалое внимание должно придаваться вопросу создания и сохранения в безопасности самого пароля. Он не должен передаваться в открытом виде, неважно сеть это или же листочек, прикрепленный к монитору. Пароль должен

быть достаточно сложным, чтобы его нельзя было получить простым перебором. Если пароль используется несколькими людьми, то должен быть продуман безопасный метод его распространения, а так же систему оповещения на случай, если пароль станет известен кому-либо еще.

Несмотря на свои ограничения, симметричное шифрование имеет большое распространение. В основном из-за простоты понимания всего процесса (один пароль) и технической нагрузки (обычно, такие алгоритмы быстрые).

Сквозное шифрование (также оконечное шифрование; англ. end-to-end encryption) — способ передачи данных, в котором только пользователи, участвующие в общении, имеют доступ к сообщениям. Таким образом, использование сквозного шифрования не позволяет получить доступ к криптографическим ключам со стороны третьих лиц.

Защита информации путем преобразования, исключающего ее прочтение посторонним лицом, является одним из наиболее действенных методов обеспечения информационной безопасности.

Для обеспечения защиты информации в настоящее время не существует единого технического приема или средства, однако общим в решении многих проблем безопасности является использование криптографии и криптоподобных преобразований информации. Защита конфиденциальной информации, основанная на криптографической защите информации, шифрует данные при помощи семейства обратимых преобразований, каждое из которых описывается параметром, именуемым «ключом» и порядком, определяющим очередность применения каждого преобразования.

Криптографические преобразования имеют цель обеспечить недоступность информации для лиц, не имеющих ключа, и поддержание с требуемой надежностью обнаружения несанкционированных искажений.

В криптографии используются следующие основные алгоритмы шифрования:

- алгоритм замены (подстановки) – символы шифруемого текста заменяются символами того же или другого алфавита в соответствии с заранее обусловленной схемой замены;
- алгоритм перестановки – символы шифруемого текста переставляются по определенному правилу в пределах некоторого блока этого текста;
- гаммирование – символы шифруемого текста складываются с символами некоторой случайной последовательности;
- аналитическое преобразование – преобразование шифруемого текста по некоторому аналитическому правилу (формуле).

Современная криптография включает в себя четыре крупных раздела:

- Симметричные криптосистемы.
- Криптосистемы с открытым ключом.
- Системы электронной подписи.
- Управление ключами.

Основные направления использования криптографических методов:

- передача конфиденциальной информации по каналам связи;
- установление подлинности передаваемых сообщений;
- хранение информации в зашифрованном виде.

Шифрование. Основные понятия

Алфавит – конечное множество используемых для кодирования информации знаков.

Дешифрование – процесс преобразования шифрованного текста в открытый с помощью ключа шифрования.

Ключ – конкретное секретное состояние некоторых параметров алго- ритма криптографического преобразования данных, обеспечивающее выбор только одного варианта из всех возможных для данного алгоритма, т.е. информация, необходимая для беспрепятственного шифрования и дешифрования текстов.

Кодирование – (не относится к криптографии) – система условных обозначений, применяемых при передаче информации. Применяется для увеличения качества передачи информации, сжатия информации и для уменьшения стоимости хранения и передачи.
Криптоанализ – наука о методах раскрытия и модификации данных без знания ключей. Занимается вскрытием шифра без знания ключа (проверка устойчивости шифра).
Криптография – наука о методах защиты информации на основе ее преобразования с сохранением достоверности содержания. Обеспечивает сокрытие смысла сообщения с помощью шифрования и открытия его расшифрованием (дешифрованием), которые выполняются по специальным алгоритмам с помощью ключей.
Текст – упорядоченный набор из элементов (символов) алфавита.
Шифрование – процесс, при котором исходный (открытый) текст сообщения заменяется шифрованным текстом.
Процессы шифрования и дешифрования осуществляются в рамках некоторой криптосистемы.
Для **симметричной** криптосистемы характерно применение одного и того же ключа как при шифровании, так и при дешифровании сообщений.
В **асимметричных** криптосистемах для шифрования данных используется один (общедоступный) ключ, а для дешифрования – другой (секретный) ключ.

Тема 4. Аудит информационной безопасности – основа эффективной защиты предприятия.

Сегодня информационные системы (ИС) играют ключевую роль в обеспечении эффективности работы коммерческих и государственных предприятий. Повсеместное использование ИС для хранения, обработки и передачи информации делает актуальными проблемы их защиты, особенно учитывая глобальную тенденцию к росту числа информационных атак, приводящих к значительным финансовым и материальным потерям. Для эффективной защиты от атак компаниям необходима объективная оценка уровня безопасности ИС - именно для этих целей и применяется аудит безопасности.

Что такое аудит безопасности?

Определение аудита безопасности еще не устоялось, но в общем случае его можно описать как процесс сбора и анализа информации об ИС для качественной или количественной оценки уровня ее защищенности от атак злоумышленников. Существует множество случаев, когда целесообразно проводить аудит безопасности. Это делается, в частности, при подготовке технического задания на проектирование и разработку системы защиты информации и после внедрения системы безопасности для оценки уровня ее эффективности. Возможен аудит, направленный на приведение действующей системы безопасности в соответствие требованиям российского или международного законодательства. Аудит может также предназначаться для систематизации и упорядочения существующих мер защиты информации или для расследования произошедшего инцидента, связанного с нарушением информационной безопасности.

Как правило, для проведения аудита привлекаются внешние компании, которые предоставляют консалтинговые услуги в области информационной безопасности. Инициатором процедуры аудита может стать руководство предприятия, служба автоматизации или служба информационной безопасности. В ряде случаев аудит также проводится по требованию страховых компаний или регулирующих органов. Аудит безопасности выполняется группой экспертов, численность и состав которой зависит от целей и задач обследования, а также от сложности объекта оценки.

Виды аудита безопасности.

Можно выделить следующие основные виды аудита информационной безопасности:

- экспертный аудит безопасности, в ходе которого выявляются недостатки в системе мер защиты информации на основе опыта экспертов, участвующих в процедуре обследования;

- оценка соответствия рекомендациям международного стандарта ISO 17799, а также требованиям руководящих документов ФСТЭК (Гостехкомиссии);
- инструментальный анализ защищенности ИС, направленный на выявление и устранение уязвимостей программно-аппаратного обеспечения системы;
- комплексный аудит, включающий в себя все вышеперечисленные формы проведения обследования.

Любой из перечисленных видов аудита может проводиться по отдельности или в комплексе, в зависимости от тех задач, которые решает предприятие. В качестве объекта аудита может выступать как ИС компании в целом, так и ее отдельные сегменты, в которых обрабатывается информация, подлежащая защите.

Основные этапы работ при проведении аудита безопасности.

На первом этапе совместно с заказчиком разрабатывается регламент, устанавливающий состав и порядок проведения работ. Основная задача регламента - определить границы, в рамках которых будет проводиться обследование. Регламент позволяет избежать взаимных претензий по завершении аудита, поскольку четко определяет обязанности сторон. Как правило, регламент содержит следующую основную информацию:

- состав рабочих групп от исполнителя и заказчика для проведения аудита;
- список и местоположение объектов заказчика, подлежащих аудиту;
- перечень информации, которая будет предоставлена исполнителю;
- перечень ресурсов, которые рассматриваются в качестве объектов защиты (информационные, программные, физические ресурсы и т. д.);
- модель угроз информационной безопасности, на основе которой проводится аудит;
- категории пользователей, которые рассматриваются в качестве потенциальных нарушителей;
- порядок и время проведения инструментального обследования ИС заказчика.

На втором этапе, в соответствии с согласованным регламентом, собирается исходная информация. Методы сбора информации включают интервьюирование сотрудников заказчика, заполнение опросных листов, анализ предоставленной организационно-распорядительной и технической документации, использование специализированных инструментальных средств.

Третий этап работ предполагает анализ собранной информации с целью оценки текущего уровня защищенности ИС предприятия. По результатам проведенного анализа на четвертом этапе разрабатываются рекомендации по повышению уровня защищенности ИС от угроз информационной безопасности.

Рассмотрим этапы аудита, связанные со сбором информации, ее анализом и разработкой рекомендаций по повышению уровня защиты ИС.

Сбор исходных данных

Качество аудита безопасности во многом зависит от полноты и точности информации, полученной в процессе сбора исходных данных. Поэтому в нее необходимо включить следующее: организационно-распорядительную документацию, касающуюся вопросов информационной безопасности, сведения о программно-аппаратном обеспечении ИС, информацию о средствах защиты, установленных в ИС, и т. д. Более подробный перечень исходных данных представлен в табл.

Таблица Перечень исходных данных, необходимых для аудита безопасности

Тип информации	**Состав исходных данных**
Организационно-распорядительная документация по вопросам информационной безопасности	• политика информационной безопасности ИС; руководящие документы (приказы, распоряжения, инструкции) по вопросам хранения, порядка доступа и передачи информации; • регламенты работы пользователей с информационными ресурсами ИС
Информация об аппаратном	• перечень серверов, рабочих станций и коммуникационного

обеспечении хостов	оборудования, установленного в ИС; • аппаратные конфигурации серверов и рабочих станций; • сведения о периферийном оборудовании
Информация об общесистемном ПО	• сведения об ОС, установленных на рабочих станциях и серверах; • сведения о СУБД, установленных в ИС
Информация о прикладном ПО	• перечень прикладного ПО общего и специального назначения, установленного в ИС; • описание функциональных задач, решаемых с помощью прикладного ПО
Информация о средствах защиты, установленных в ИС	• производитель средства защиты; • конфигурационные настройки средства защиты; • схема установки средства защиты
Информация о топологии ИС	• карта локальной вычислительной сети, включая схему распределения серверов и рабочих станций по сегментам сети; • типы каналов связи, используемых в ИС; • используемые в ИС сетевые протоколы; • схема информационных потоков ИС

Как уже отмечалось выше, для сбора исходных данных применяются следующие методы.

Интервьюирование сотрудников заказчика, обладающих необходимой информацией. Интервью обычно проводятся как с техническими специалистами, так и с представителями руководящего звена компании. Перечень вопросов, которые планируется обсудить в процессе интервью, согласовывается заранее.

Предоставление опросных листов по определенной тематике, которые сотрудники заказчика заполняют самостоятельно. В тех случаях, когда представленные материалы не полностью отвечают на необходимые вопросы, проводится дополнительное интервьюирование.

Анализ организационно-технической документации, используемой заказчиком.

Использование специализированного ПО, которое позволяет получить необходимую информацию о составе и настройках программно-аппаратного обеспечения ИС предприятия. Например, с помощью систем анализа защищенности (security scanners) можно провести инвентаризацию сетевых ресурсов и выявить уязвимости в них. В качестве примеров таких систем можно назвать Internet Scanner компании ISS и XSpider компании Positive Technologies.

Оценка уровня безопасности ИС

После сбора необходимой информации проводится ее анализ с целью оценки текущего уровня защищенности системы. В процессе такого анализа определяются риски информационной безопасности, которым подвержена компания. Фактически риск представляет собой интегральную оценку того, насколько эффективно существующие средства защиты способны противостоять информационным атакам.

Обычно выделяют две основные группы методов расчета рисков безопасности. Первая группа позволяет установить уровень риска путем оценки степени соответствия определенному набору требований к информационной безопасности. В качестве источников таких требований могут выступать:

- нормативно-правовые документы предприятия, касающиеся вопросов информационной безопасности (политика безопасности, регламенты, приказы, распоряжения);
- требования действующего российского законодательства - руководящие документы ФСТЭК (Гостехкомиссии), СТР-К, требования ФСБ РФ, ГОСТы и т. д.;
- рекомендации международных стандартов - ISO 17799, OCTAVE, CoBIT, BS 7799-2 и т. д.;
- рекомендации компаний-производителей программного и аппаратного обеспечения - Microsoft, Oracle, Cisco и т. д.

Вторая группа методов оценки рисков информационной безопасности базируется на определении вероятности реализации атак, а также уровней их ущерба. Значение риска вычисляется отдельно для каждой атаки и в общем случае представляется как произведение вероятности проведения атаки а на величину возможного ущерба от этой атаки - Риск (а) = Р(а) . Ущерб (а). Значение ущерба определяется собственником информационного ресурса, а вероятность атаки вычисляется группой экспертов, проводящих процедуру аудита. Вероятность в данном случае рассматривается как мера того, что в результате проведения атаки нарушители достигли своих целей и нанесли ущерб компании.

Методы обеих групп могут использовать количественные или качественные шкалы для определения величины риска информационной безопасности. В первом случае для риска и всех его параметров берутся численные выражения. Например, при использовании количественных шкал вероятность проведения атаки Р(а) может выражаться числом в интервале [0,1], а ущерб от атаки - задаваться в виде денежного эквивалента материальных потерь, которые может понести организация в случае успешной атаки. При использовании качественных шкал числовые значения заменяются на эквивалентные им понятийные уровни. Каждому понятийному уровню в этом случае будет соответствовать определенный интервал количественной шкалы оценки. Количество уровней может варьироваться в зависимости от применяемых методик оценки рисков. В таблицах приведены примеры качественных шкал оценки рисков информационной безопасности, в которых для оценки уровней ущерба и вероятности атаки используется пять понятийных уровней.

Таблица. Качественная шкала оценки уровня ущерба

Уровень ущерба	**Описание**
Малый	Незначительные потери материальных активов, которые быстро восстанавливаются, или незначительные последствия для репутации компании
Умеренный	Заметные потери материальных активов или умеренные последствия для репутации компании
Средней тяжести	Существенные потери материальных активов или значительный урон репутации компании
Большой	Большие потери материальных активов и большой урон репутации компании
Критический	Критические потери материальных активов или полная потеря репутации компании на рынке, что делает невозможным ее дальнейшую деятельность

Таблица. Качественная шкала оценки вероятности проведения атаки

Вероятность атаки	**Описание**
Очень низкая	Атака практически никогда не будет проведена. Соответствует числовому интервалу вероятности [0, 0,25)
Низкая	Вероятность проведения атаки достаточно низкая. Соответствует числовому интервалу вероятности [0,25, 0,5)
Средняя	Вероятность проведения атаки приблизительно равна 0,5
Высокая	Атака скорее всего будет проведена. Соответствует числовому интервалу вероятности (0,5, 0,75]
Очень высокая	Атака почти наверняка будет проведена. Соответствует числовому интервалу вероятности (0,75, 1]

Для вычисления уровня риска по качественным шкалам применяются специальные таблицы, в которых в первом столбце задаются понятийные уровни ущерба, а в первой строке - уровни вероятности атаки. Ячейки же таблицы, расположенные на пересечении соответствующих

строк и столбцов, содержат уровень риска безопасности. Размерность таблицы зависит от количества концептуальных уровней вероятности атаки и ущерба.

Таблица. Определение уровня риска информационной безопасности по качественной шкале

	Вероятность атаки				
Ущерб	очень низкая	низкая	средняя	высокая	очень высокая
Малый	Низкий риск	Низкий риск	Низкий риск	Средний риск	Средний риск
Умеренный	Низкий риск	Низкий риск	Средний риск	Средний риск	Высокий риск
Средней тяжести	Низкий риск	Средний риск	Средний риск	Средний риск	Высокий риск
Большой	Средний риск	Средний риск	Средний риск	Средний риск	Высокий риск
Критический	Средний риск	Высокий риск	Высокий риск	Высокий риск	Высокий риск

При расчете значений вероятности атаки, а также уровня возможного ущерба используют статистические методы, экспертные оценки или элементы теории принятия решений. Статистические методы предполагают анализ уже накопленных данных о реально случавшихся инцидентах, связанных с нарушением информационной безопасности. На основе результатов такого анализа строятся предположения о вероятности проведения атак и уровнях ущерба от них в других ИС. Однако статистические методы не всегда удается применить из-за недостатка статистических данных о ранее проведенных атаках на ресурсы ИС, аналогичной той, которая выступает в качестве объекта оценки.

При использовании аппарата экспертных оценок анализируются результаты работы группы экспертов, компетентных в области информационной безопасности, которые на основе имеющегося у них опыта определяют количественные или качественные уровни риска. Элементы теории принятия решений позволяют применять для вычисления значения риска безопасности более сложные алгоритмы обработки результатов работы группы экспертов.

Результаты аудита безопасности

На последнем этапе аудита информационной безопасности разрабатываются рекомендации по совершенствованию организационно-технического обеспечения защиты на предприятии. Такие рекомендации могут включать в себя различные типы действий, направленных на минимизацию выявленных рисков.

Уменьшение риска за счет дополнительных организационных и технических средств защиты, позволяющих снизить вероятность проведения атаки или уменьшить возможный ущерб от нее. Так, установка межсетевых экранов в точке подключения ИС к Интернету существенно снижает вероятность проведения успешной атаки на общедоступные информационные ресурсы ИС - такие, как Web-серверы, почтовые серверы и т. д.

Уклонение от риска путем изменения архитектуры или схемы информационных потоков ИС, что позволяет исключить проведение той или иной атаки. Например, физическое отключение от Интернета сегмента ИС, в котором обрабатывается конфиденциальная информация, позволяет избежать внешних атак на конфиденциальную информацию.

Изменение характера риска в результате принятия мер по страхованию. В качестве примеров изменения характера риска можно привести страхование оборудования ИС от пожара или страхование информационных ресурсов от возможного нарушения их конфиденциальности, целостности или доступности. В настоящее время ряд российских компаний уже предлагают услуги страхования информационных рисков.

Принятие риска, если он уменьшен до того уровня, на котором уже не представляет опасности для ИС.

Обычно рекомендации направлены не на полное устранение всех выявленных рисков, а лишь на их уменьшение до приемлемого уровня. При выборе мер для повышения уровня защиты ИС учитывается одно принципиальное ограничение - стоимость реализации этих мер не должна превышать стоимости защищаемых информационных ресурсов, а также убытков компании от возможного нарушения конфиденциальности, целостности или доступности информации.

В завершение процедуры аудита его результаты оформляются в виде отчетного документа, который предоставляется заказчику. В общем случае этот документ состоит из следующих основных разделов:

- описание границ, в рамках которых проводился аудит безопасности;
- описание структуры ИС заказчика;
- методы и средства, которые использовались в процессе проведения аудита;
- описание выявленных уязвимостей и недостатков, включая уровень их риска;
- рекомендации по совершенствованию комплексной системы обеспечения информационной безопасности;
- предложения к плану реализации первоочередных мер, направленных на минимизацию выявленных рисков.

Аудит информационной безопасности - один из наиболее эффективных сегодня инструментов для получения независимой и объективной оценки текущего уровня защищенности предприятия от угроз информационной безопасности. Кроме того, результаты аудита дают основу для формирования стратегии развития системы обеспечения информационной безопасности организации. Однако необходимо понимать, что аудит безопасности - не разовая процедура, он должен проводиться на регулярной основе. Только в этом случае аудит будет приносить реальную отдачу и способствовать повышению уровня информационной безопасности компании.

Методические рекомендации для обучающихся с ограниченными возможностями здоровья и инвалидами по освоению дисциплины (модуля)

Для освоения образовательной программы лицами с ограниченными возможностями здоровья предусматриваются организация учебного процесса с использованием специальных методов обучения и дидактических материалов, составленных с учетом особенностей психофизического развития, индивидуальных возможностей и состояния здоровья таких обучающихся (обучающегося),

В целях освоения образовательной программы инвалидами и лицами с ограниченными возможностями здоровья обеспечивается (в случае наличия таких обучающихся);

1) для инвалидов и лиц с ограниченными возможностями здоровья по зрению:

предоставление альтернативных форматов используемых методических материалов (крупный шрифт или аудиофайлы);

присутствие ассистента, оказывающего обучающемуся необходимую помощь; преимущественное использование индивидуальных и групповых заданий, контроль выполнения которых осуществляется в устной форме;

на лекционном занятии рекомендуется использовать звукозаписывающие устройства и компьютеры, как способ конспектирования;

2) для инвалидов и лиц с ограниченными возможностями здоровья по слуху: надлежащие звуковые средства воспроизведения информации; наглядность при подаче материала; преимущественное использование заданий, проверка решения которых осуществляется в письменной форме либо тестовом режиме,

3) для инвалидов и лиц с ограниченными возможностями здоровья, имеющих нарушения опорно-двигательного аппарата: возможность беспрепятственного доступа обучающихся в учебные помещения.

Образование обучающихся с ограниченными возможностями здоровья может быть организовано как совместно с другими обучающимися, так и в отдельных группах или индивидуально. При его реализации предусматривается использование технических средств, необходимых им в связи с их индивидуальными особенностями.

Учебно-методические материалы для самостоятельной работы обучающихся из числа инвалидов и лиц с ограниченными возможностями здоровья предоставляются в формах, адаптированных к ограничениям их здоровья и восприятия информации.

В освоении образовательной программы инвалидами и лицами с ограниченными возможностями здоровья большое значение имеет индивидуальная работа. Индивидуальная работа может проводиться в аудиовизуальной, либо в текстовой форме. Освоение образовательной программы инвалидами и лицами с ограниченными возможностями здоровья осуществляется с использованием средств обучения общего и специального назначения, включая:

- лекционная аудитория - мультимедийное оборудование;
- учебная аудитория для практических занятий (семинаров) мультимедийное оборудование;
- учебная аудитория для самостоятельной работы - стандартные рабочие места с персональными компьютерами; рабочее место с персональным компьютером, с программой экранного доступа, программой экранного увеличения для студентов с нарушением зрения.

В целях освоения учебной программы дисциплины инвалидами и лицами с ограниченными возможностями здоровья возможно:

- использование специальных технических и иных средств индивидуального пользования, рекомендованных врачом-специалистом;
- присутствие ассистента, оказывающего обучающемуся необходимую помощь.

На занятиях рекомендуется использовать звукозаписывающие устройства и компьютеры, как способ конспектирования. Для освоения дисциплины (в т.ч. подготовки к занятиям, при самостоятельной работе) лицами с ограниченными возможностями здоровья, предоставляется возможность использования учебной литературы в виде электронного документа в электронно-библиотечной системе Book.ru имеющей специальную версию для слабовидящих; обеспечивается доступ к учебно-методическим материалам посредством СЭО «Фемида»; доступ к информационным и библиографическим ресурсам посредством сети «Интернет».

Учебно-методические материалы для самостоятельной работы обучающихся из числа инвалидов и лиц с ограниченными возможностями здоровья предоставляются в формах, адаптированных к ограничениям их здоровья и восприятия информации:

Категории студентов	**Формы**
С нарушением слуха	в печатной форме; в форме электронного документа;
С нарушением зрения	в печатной форме увеличенным шрифтом; в форме электронного документа; в форме аудиофайла;
С нарушением опорно-двигательного аппарата	в печатной форме; в форме электронного документа; в форме аудиофайла;

5.2. Перечень нормативных правовых актов, актов высших судебных организаций, материалы судебной практики:

1. Федеральный закон «О банках и банковской деятельности» от 02.12.1990 №395-1 (ред. от 30.12.2020 №495-ФЗ, с изм. от 27.10.2008)
2. Федеральный закон "О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма" от 07.08.2001 N 115-ФЗ (ред. от 02.07.2021 №355-ФЗ)
3. Федерального закона № 63ФЗ 06.04.2011 «Об электронной подписи»
4. Положение ЦБ РФ «Об индентификации кредитными организациями клиентов, представителей клиентов, выгодоприобретателей и бенефициарных владельцев в целях

противодействия легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма» от 15.10.2015 № 499

5. Положение ЦБ РФ «О требованиях к правилам внутреннего контроля кредитной организации в целях противодействия легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма» от 02.03.2012 № 375

5.3.Информационное обеспечение изучения дисциплины

Информационные, в том числе электронные ресурсы Университета, а также иные электронные ресурсы, необходимые для изучения дисциплины

Информационные ресурсы Университета:

№ п/п	Наименование	Адрес в сети Интернет	Условия доступа
1.	ЭБС «ZNANIUM.COM»	https://znanium.com/ Основная коллекция Коллекция издательства Статут Znanium.com. Discovery для аспирантов	Зарегистрированному пользователю по логину и паролю
2.	ЭБС «ЮРАЙТ»	https://urait.ru/	Зарегистрированному пользователю по логину и паролю
3.	ЭБС «BOOK.ru»	https://www.book.ru/ коллекция издательства Проспект Юридическая литература; коллекции издательства Кнорус Право, Экономика и Менеджмент	Зарегистрированному пользователю по логину и паролю
4.	East View Information Services	www.ebiblioteka.ru Универсальная база данных периодики (электронные журналы)	Зарегистрированному пользователю по логину и паролю
5.	НЦР РУКОНТ	http://rucont.ru/ Раздел Ваша коллекция – РГУП периодика (электронные журналы)	Зарегистрированному пользователю по логину и паролю
6.	Электронный каталог РГУП	http://biblioteka.raj.ru/MegaPro/Web	Зарегистрированному пользователю по логину и паролю
7.	Информационно-образовательный потенциал РГУП	http://op.raj.ru/ электронные версии учебных, научных и научно-практических изданий РГУП	Зарегистрированному пользователю по логину и паролю
8.	Система электронного обучения «Фемида»	https://femida.raj.ru Учебно-методические комплексы, Рабочие программы по направлению подготовки	Зарегистрированному пользователю по логину и паролю
9.	Система электронного обучения «Фемида»	Гарант, Консультант	По ip-адресу в университете
10.	Национальная электронная библиотека (НЭБ)	https://rusneb.ru/	По ip-адресу в университете

6. Материально-техническое обеспечение дисциплины

В целях освоения учебной программы дисциплины необходимы следующие материально-технические и программные средства:
Лекционные занятия: комплект электронных презентаций/слайдов, аудитория, оснащенная презентационной техникой (проектор, экран, компьютер/ноутбук).
Практические занятия: презентационная техника (проектор, экран, компьютер/ноутбук), пакеты ПО общего назначения (текстовые редакторы, графические редакторы, системы управления базами данных).
Прочее:
рабочее место преподавателя, оснащенное компьютером с доступом в Интернет;
рабочие места студентов в компьютерном классе, в библиотеке РГУП, в аудиториях для практических занятий, оснащенные компьютерами с доступом в Интернет, предназначенные для работы в электронной образовательной среде.

№ п/п	Наименование дисциплины (модуля), в соответствии с учебным планом	Наименование специальных помещений и помещений для самостоятельной работы
1	Математические методы защиты информации	Аудитория № 107 - для проведения занятий лекционного типа, занятий семинарского типа, курсового проектирования (выполнения курсовых работ), групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации (либо аналог)

7. Карта обеспеченности литературой

Кафедра правовой информатики, информационного права и естественнонаучных дисциплин
Направление подготовки (специальность): 38.03.02 «Менеджмент»
Профиль: управление недвижимостью
Дисциплина: Математические методы защиты информации
Курс: 3

Наименование, Автор или редактор, Издательство, Год издания, кол-во страниц	ЭБС (указат
1	
Основная литература	
Пилиди, В. С. Математические основы зашиты информации : учебное пособие / В. С. Пилиди ; Южный федеральный университет. - Ростов-на-Дону ; Таганрог : Издательство Южного федерального университета, 2019. - 308 с. - ISBN 978-5-9275-3363-3. - Текст : электронный. - URL: https://znanium.com/catalog/product/1088209 (дата обращения: 24.03.2023). – Режим доступа: по подписке.	https:// og/pro
Клименко, И. С. Информационная безопасность и защита информации: модели и методы управления : монография / И.С. Клименко. — Москва : ИНФРА-М, 2022. — 180 с. — (Научная мысль). — DOI 10.12737/monography_5d412ff13c0b88.75804464. - ISBN 978-5-16-015149-6. - Текст : электронный. - URL: https://znanium.com/catalog/product/1862651 (дата обращения: 24.03.2023). – Режим доступа: по подписке.	https:// ocument
Дополнительная литература	
Криптографическая защита информации : учебное пособие / С.О. Крамаров, О.Ю. Митясова, С.В. Соколов [и др.] ; под ред. С.О. Крамарова. — Москва : РИОР : ИНФРА-М, 2023. — 321 с. — (Высшее образование). — DOI: https://doi.org/10.12737/1716-6. - ISBN 978-5-369-01716-6. - Текст : электронный. - URL: https://znanium.com/catalog/product/1899016 (дата обращения: 24.03.2023). – Режим доступа: по подписке.	https:// ocume
Ищейнов, В. Я., Информационная безопасность и защита информации: словарь терминов и понятий : словарь / В. Я. Ищейнов. — Москва : Русайнс, 2022. — 226 с. — ISBN 978-5-4365-9298-5. — URL: https://book.ru/book/944006 (дата обращения: 24.05.2023). — Текст : электронный.	https://
Внуков, А. А. Защита информации : учебное пособие для вузов / А. А. Внуков. — 3-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2023. — 161 с. — (Высшее образование). — ISBN 978-5-534-07248-8. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/512268 (дата обращения: 24.05.2023).	https:// informa
Дополнительная литература для углубленного изучения дисциплины	
Щеглов, А. Ю. Защита информации: основы теории : учебник для вузов / А. Ю. Щеглов, К. А. Щеглов. — Москва : Издательство Юрайт, 2023. — 309 с. — (Высшее образование). — ISBN 978-5-534-04732-5. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/511998 (дата обращения: 24.05.2023).	https:// informa 511998

Зам. зав. библиотекой _____

Зам. зав. кафедрой _____

8. Фонд оценочных средств
8.1.Паспорт фонда оценочных средств по дисциплине (модулю).

№ п/п	Раздел дисциплины, тема	Код компетенции	Наименование оценочного средства
1.	Информационная безопасность и уровни ее обеспечения.	УК-1 ПК-3	вопросы для семинара (практического занятия), коллоквиум, доклады с презентациями, контрольная работа
2.	Государственная политика в обеспечении информационной безопасности.	УК-1 ПК-3	вопросы для семинара (практического занятия), коллоквиум, доклады с презентациями, контрольная работа
3.	Криптографические методы защиты информации.	УК-1 ПК-3	вопросы для семинара (практического занятия), коллоквиум, доклады с презентациями
4 .	Аудит информационной безопасности. Анализ информационных рисков.	УК-1 ПК-3	Реферат, задания на практическую работу, коллоквиум, тестовые задания

Проверка и оценка результатов выполнения заданий

Контрольные материалы для проведения **текущего контроля** оцениваются в баллах:

Форма текущего контроля	Баллы
Тесты (за 10 вопросов)	8-10 правильных ответов – 3 балла, 5-7 правильных ответов – 2 балла, 2-4 правильных ответов – 1 балл 0-1 правильных ответов – 0 баллов
Контрольная работа	соответствие заявленной теме-1 балл логичность и последовательность изложения материала-2 балла способность к работе с информационными источниками-1 балл способность к анализу-3 балла умение формулировать выводы-3 балла Итого: максимум -10 баллов
Практическая работа	Выполняет работу верно – 3 балла, Выполняет работу с незначительными неточностями – 2 балла Выполняет работу с ошибками, которые при дополнительных

	вопросах исправляет – 1 балл Не может выполнить работу – 0 баллов
Коллоквиум	Отвечает верно – 3 балла, Отвечает с незначительными неточностями – 2 балла Отвечает с ошибками, которые при дополнительных вопросах исправляет – 1 балл Не может ответить – 0 баллов
Доклад-презентация	Критерии оценивания: - соответствие заявленной теме – 1 балл, - логичность и последовательность изложения материала – 2 балла, - способность к работе с информационными источниками – 1 балл, - способность к анализу – 3 балла, - умение формулировать выводы – 3 балла. Итого: максимум 10 баллов

8.2.Оценочные средства

Тестовые задания
Содержание банка тестовых заданий

V1: Математические методы защиты информации

I:
S: Меры каких уровней необходимо принимать при обеспечении защиты интересов субъектов информационных отношений?
-: социального;
-: законодательного;
-: исполнительного;
-: административного;
-: экономического;
-: процедурного;
-: функционального;
-: программно-технического;
-: программно-аппаратного.

I:
S: Что относится к основным составляющим информационной безопасности?
-: защита информации;
-: компьютерная безопасность;
-: экологическая безопасность;
-: защищенность информации и поддерживающей инфраструктуры;
-: защита от информации;
-: защищенность потребностей граждан.

I:
S: Что относится к первоочередным задачам защиты информации?
-: обеспечение качества информационных ресурсов;
-: обеспечение целостности информационных ресурсов;
-: обеспечение доступности информационных ресурсов;
-: обеспечение надежности информационных ресурсов;
-: обеспечение конфиденциальности информационных ресурсов.

I:
S: Обозначьте основные направления деятельности на законодательном уроне в сфере обеспечения информационной безопасности?
-: разработка новых законов с учетом интересов всех категорий субъ- ектов информационных отношений;
-: ориентация на созидательные законы;
-: ориентация на карательные законы;
-: создание уникальных стандартов и сертификационных нормативов, актуальных только в России;
-: интеграция в мировое правовое пространство;
-: учет современного состояния информационных технологий;
-: использование исключительно собственного опыта при создании нормативно-правовой базы в области информационной безопасности.

I:

S: Выделите основные группы процедурных мер, направленных на обеспечение информационной безопасности
-: программная защита;
-: управление персоналом;
-: управление ресурсами;
-: аппаратная защита;
-: физическая защита;
-: поддержание работоспособности;
-: реагирование на нарушения режима безопасности;
-: обеспечение стабильности;
-: планирование восстановительных работ.

I:
S: На чем основывается политика информационной безопасности в организации?
-: на выявлении всех возможных угроз информационной безопасности организации;
-: на поиске уязвимостей информационной системы организации;
-: на анализе рисков, признанных реальными для информационной системы организации;
-: на закупке оборудования, предотвращающего утечку информации по техническим каналам;
-: на регистрации всех действий персонала при работе с защищаемой информацией.

I:
S: Уполномоченными лицами считаются …
-: собственники информации;
-: владельцы информации;
-: пользователи информации;
-: пользователи, получившие право работы с информацией от ее владельца;
-: государственные служащие;
-: работники силовых структур.

I:
S: Уязвимость — это …
-: наличие узких мест в системе защиты информации;
-: слабость системы информационной безопасности;
-: незащищенность или ошибка в объекте, которая может привести к возникновению угрозы;
-: наличие угроз информационной безопасности;
-: незащищенность объектов информационной системы.

I:
S: Неумышленное происшествие с деструктивным воздействием на объект — это …
-: ошибка;
-: катастрофа;
-: авария;
-: повреждение;
-: поломка.

I:
S: Для чего предназначены информационные способы работы с информационными потоками?
-: сбор информации;
-: качественное, своевременное и достоверное удовлетворение информационных потребностей пользователей;
-: перераспределение информации;
-: передача информации;

-: уничтожение информации.

I:
S: Основные компоненты информатизации включают в себя …
-: оборудование;
-: вычислительные сети;
-: информационные системы;
-: каналы связи;
-: информационные ресурсы.

I:
S: Информационные ресурсы — это…
-: документ, входящий в информационную систему;
-: массивы документов;
-: файлы, хранящиеся в памяти компьютера;
-: документы и массивы документов в разных формах и видах, содержащие информацию по всем направлениям жизнедеятельности общества;
-: все существующие знания.

I:
S: Что из нижеперечисленного относится к свойствам информации
-: неотрывность от языка носителя;
-: дискретность;
-: периодичность;
-: независимость от создателей;
-: латентность.

I:
S: Фиксированные информационные ресурсы — это…
-: некоторые сведения, которые не могут менять свое содержание со временем;
-: информация, закрепленная на каком-нибудь физическом носителе;
-: набор символов, имеющий смысл и определенную размерность;
фиксированный массив документов, необходимый для удовлетворения информационных -: потребностей общества в определенной сфере деятельности;
-: документы определенного вида.

I:
S: Информация — это…
-: входные данные;
-: фиксированный набор символов естественного языка;
-: сведения о лицах, предметах, событиях, явлениях и процессах, хранящиеся в памяти ЭВМ;
-: сведения о лицах, предметах, событиях, явлениях и процессах, отраженные на материальных
-: носителях, используемые в целях получения знаний и практических решений;
-: признаковая структура объектов.

I:
S: Чем определяется ценность информации*?*
-: рыночной стоимостью;
-: обеспечением возможности достижения цели, поставленной перед получателем;
-: стоимостью носителя;
-: степенью доверия к источнику;
-: количеством заинтересованных в ней лиц.

I:
S: Что такое защита информации?
-: создание защищенных банков данных конфиденциальной информации
-: комплекс мероприятий по обеспечению конфиденциальности, целостности, доступности, учета и неотрекаемости информации;
-: набор аппаратных и программных средств для обеспечения конфиденциальности, целостности, доступности, учета и неотрекаемости информации;
-: комплекс мероприятий по обеспечению сохранности, доступности и конфиденциальности данных в компьютерных сетях;
-: обеспечение кодирования информации, передаваемой в локальной сети организации.

I:
S: Возможность за приемлемое время получить требуемую информационную услугу определяет …
-: отказоустойчивость информационной системы;
-: время отклика системы;
-: пропускную способность канала;
-: качество сервиса;
-: степень доступности информации.

I:
S: Что подразумевается под комплексом организационных, технических и технологических мер по защите информации от неавторизованного доступа, разрушения, модификации, раскрытия и задержек в доступе?
-: информационная защищенность;
-: информационная стабильность;
-: стойкость информационной системы;
-: национальная безопасность;
-: информационная безопасность.

I:
S: Что такое «угроза»?
-: возможность реализации несанкционированных действий в отношении информационной системы;
-: невосполнимый ущерб, нанесенный государственной организации;
-: предотвращенное деструктивное воздействие на информационную систему;
-: непоправимый вред, наносимый окружающей среде;
-: уязвимость информационной системы.

I:
S: Назовите основные средства защиты информации
-: электромеханические;
-: физические;
-: аппаратные;
-: виброакустические;
-: программные;
-: криптографические;
-: идентификационные.

I:
S: Назовите свойство данных сохранять ценность для потребителя с течением времени, т.е. не

подвергаться моральному старению:
-: актуальность;
-: значимость;
-: неизменность;
-: срочность;
-: постоянность.

I:
S: Что понимается под совокупностью документированных управленческих решений, направленных на защиту информации и ассоциированных с ней ресурсов?
-: информационная политика;
-: безопасность информации;
-: политика безопасности;
-: регламентация доступа;
-: организация защиты.

I:
S: Какие механизмы безопасности необходимо использовать в рамках современных информационных систем ?
-: квотирование;
-: идентификация и аутентификация пользователей;
-: управление доступом;
-: резервное копирование;
-: протоколирование и аудит;
-: обеспечение высокой производительности системы;
-: обновление;
-: криптография;
-: межсетевое экранирование;
-: обеспечение высокой доступности.

I:
S: Перечислите основные группы мер, которые необходимо реализовывать на законодательном уровне для обеспечения информационной безопасности меры, направленные на увеличение количества аппаратно- программных продуктов иностранного производства на отечественном рынке;
-: меры, направленные на создание и поддержание в обществе негативного отношения к нарушениям и нарушителям информационной безопасности;
-: меры, направленные на снижение использования средств вычислительной техники (СВТ) во всех сферах человеческой деятельности;
-: меры, направленные на ограничение доступа рядовых граждан к механизмам информационной безопасности;
-: меры, способствующие повышению образованности общества в области информационной безопасности, помогающие в разработке и распространении средств обеспечения информационной безопасности.

I:
S: Фиксация и анализ всех действий уполномоченных лиц, выполняемых ими в рамках, контролируемых системой информационной безопасности — это …
-: контроль;
-: учет;
-: база знаний;
-: слежка;

-: регистрация.

I:
S: Попытка практической реализации угрозы — это …
-: взлом;
-: атака;
-: кража;
-: нападение;
-: удаленная атака.

I:
S: Каким свойством обладают данные, характеризующие текущую ситуацию?
-: адаптивность;
-: корректность;
-: непротиворечивость;
-: целостность;
-: актуальность.

I:
S: Субъект, преследующий корыстные или деструктивные цели, противоречащие целям системы, — это …
-: вредитель;
-: хакер;
-: агент конкурирующей системы;
-: правонарушитель;
-: злоумышленник.

I:
S: Что понимается под истинностью данных?
-: свойство данных не иметь скрытых случайных ошибок;
-: свойство данных постоянно соответствовать текущей ситуации;
-: свойство данных противостоять деструктивному воздействию;
-: свойство данных не иметь явных ошибок;
-: свойство данных не иметь преднамеренные искажения человеком — источником сведений или -: искажения, вносимые средствами обработки информации.

I:
S: Что представляет собой объективно значимые потребности личности, общества и государства в обеспечении их защищенности и устойчивого развития в части, касающейся информационной сферы?
-: государственная информационная политика;
-: информационная безопасность Российской Федерации;
-: национальные интересы Российской Федерации в информационной сфере;
-: информационные интересы Российской Федерации;
-: национальная безопасность Российской Федерации в информационной сфере.

I:
S: Что представляет собой совокупность условий и факторов, создающих опасность жизненно важным интересам личности, общества и государства?
-: мировую экологическую обстановку;
-: злоумышленные действия вражеской разведки;
-: потенциальный вред;

-: угрозу;
-: промышленный шпионаж с привлечением разведывательных и специальных служб.

I:
S: Что можно отнести к важнейшим принципам деятельности государственных органов по обеспечению информационной безопасности?
-: законность общественных отношений в информационной сфере и правовое равенство всех участников таких отношений;
-: предоставление гражданам информации по работе государственных органов на всех уровнях;
-: конструктивное взаимодействие государственных органов, организаций и граждан при решении задач по обеспечению информационной без- опасности;
-: соблюдение баланса между потребностью граждан в свободном обмене информацией и ограничениями;
-: развитие систем массовой информации Российской Федерации.

I:
S: Что является стратегической целью обеспечения информационной безопасности в области обороны страны согласно Доктрине информационной безопасности Российской Федерации?
-: защита суверенитета;
-: поддержание обороноспособности Российской Федерации;
-: защита жизненно важных интересов личности, общества и государства от внутренних и внешних угроз, связанных с применением информационных технологий в военно-политических целях;
-: поддержание территориальной целостности Российской Федерации;
-: обеспечение основных прав и свобод человека и гражданина.

I:
S: Перечислите организации, которые входят в состав организационной основы системы обеспечения информационной безопасности Российской Федерации
-: ФСБ России;
-: Совет Федерации Федерального Собрания РФ;
-: Совет Безопасности Российской Федерации;
-: ФСТЭК России;
-: Государственная Дума Федерального Собрания РФ;
-: МВД России;
-: Правительство РФ.

I:
S: Что относится к основной деятельности Минобороны России в области обеспечения информационной безопасности?
-: разработка криптографических средств защиты информации;
-: организация деятельности по обеспечению информационной безопасности, защите государственной тайны в Вооруженных Силах РФ;
-: организационно-техническое обеспечение деятельности Межведомственной комиссии по защите государственной тайны;
-: организация деятельности государственной системы противодействия техническим разведкам на федеральном уровне;
-: техническая защита информации в аппаратах федеральных органов государственной власти.

I:
S: К угрозам информационной безопасности для личности можно отнести …
-: препятствия в построении информационного общества;

-: манипулирование массовым сознанием;
-: лишение права граждан на неприкосновенность частной жизни;
-: противодействие защите интересов личности и общества;
-: нарушение права граждан на защиту своего здоровья от неосознаваемой человеком вредной информации.

I:
S: К угрозам информационной безопасности для государства можно отнести …
-: лишение права граждан на неприкосновенность частной жизни;
-: противодействие защите интересов личности и общества;
-: посягательства на объекты интеллектуальной собственности;
-: противодействие защите единого информационного пространства страны;
-: противодействие построению правового государства.

I:
S: Национальными интересами Российской Федерации в информационной сфере являются :
-: защита государственных информационных ресурсов от несанкционированного доступа;
-: развитие в Российской Федерации отрасли информационных технологий и электронной промышленности;
-: обеспечение свободного сбора, хранения, использования и распространения информации о частной жизни граждан Российской Федерации;
-: обеспечение и защита конституционных прав и свобод человека и гражданина в части, касающейся получения и использования информации;
-: содействие формированию системы международной информационной безопасности, направленной на противодействие угрозам использования информационных технологий в целях нарушения стратегической стабильности.

I:
S: Какие бывают уровни воздействия информационной безопасности?
-: для личности;
-: для организации;
-: для государства;
-: для предприятия;
-: для общества;
-: для субъекта РФ.

I:
S: Что можно отнести к важнейшим задачам государственных органов в рамках деятельности по обеспечению информационной безопасности?
-: организация разведывательной деятельности для обеспечения информационной безопасности личности, общества и государства;
-: обеспечение защиты прав и законных интересов граждан и организаций в информационной сфере;
-: оценка состояния информационной безопасности, прогнозирование и обнаружение -: информационных угроз, определение приоритетных направлений их предотвращения и ликвидации последствий их проявления;
-: государственная поддержка разработки, производства и эксплуатации средств информационного взаимодействия;
-: планирование, осуществление и оценка эффективности комплекса мер по обеспечению информационной безопасности.

I:

S: Создание помех для нормальной работы канала передачи связи, то есть нарушение работоспособности канала связи возникает:
-: со стороны злоумышленника;
-: со стороны законного отправителя сообщения;
-: со стороны законного получателя сообщения.

I:
S: Какие алгоритмы используют один и тот же ключ для шифрования и дешифровки?
-: асимметричный;
-: симметричный;
-: правильного ответа нет.

I:
S: Процесс нахождения открытого сообщения соответственно заданному закрытому при неизвестном криптографическом преобразовании называется:
-: шифрование;
-: дешифровка;
-: расшифровка.

I:
S: В каких основных форматах существует симметричный алгоритм?
-: блока и строки;
-: потока и блока;
-: потока и данных

I:
S: Открытым текстом в криптографии называют:
-: расшифрованный текст;
-: любое послание;
-: исходное послание.

I:
S: Какой ключ известен только приемнику?
-: открытый;
-: закрытый.

I:
S: Наука, занимающаяся защитой информации, путем преобразования этой информации это:
-: криптография;
-: криптология;
-: криптоанализ.

I:
S: В каких шифрах результат шифрования очередного блока зависит только от него самого и не зависит от других блоков шифруемого массива данных?
-: в потоковых;
-: в блочных.

I:
S: Шифр, который заключается в перестановках структурных элементов шифруемого блока данных – битов, символов, цифр – это:
-: шифр функциональных преобразований;

-: шифр замен;
-: шифр перестановок.

I:
S: Функция, предназначенная для выработки блока данных, используемого для модификации шифруемого блока, из инварианта и ключевого элемента называется:
-: функция шифрования шага преобразования;
-: инвариант стандартного шага шифрования.

I:
S: Шифрование-это:
-: процесс создания алгоритмов шифрования;
-: процесс сжатия информации;
-: процесс криптографического преобразования информации к виду, когда ее смысл полностью теряется.

I:
S: В каком случае построение цифровой подписи не требует наличия в системе третьего лица – арбитра, занимающегося аутентификацией?
-: при шифровании с помощью асимметричного алгоритма;
-: при шифровании с помощью симметричного алгоритма;
-: арбитр необходим всегда.

I:
S: Можно ли отнести слабую аутентификацию к проблемам безопасности?
-: нет;
-: да;
-: в редких случаях.

I:
S: Возможно ли расшифровывать информацию без знания ключа?
-: нет;
-: да;
-: в редких случаях.

I:
S: Возможно ли вычислить закрытый ключ ассиметричного алгоритма, зная открытый?
-: нет;
-: да;
-: в редких случаях.

I:
S: Аутентификацией называют:
-: процесс регистрации в системе;
-: способ защиты системы;
-: процесс распознавания и проверки подлинности заявлений о себе пользователей и процессов.

I:
S: Аутентификация бывает:
-: статическая;
-: устойчивая;
-: постоянная;

-: все варианты правильные;
-: правильного варианта нет.

I:
S: Стойкость ключа характеризуется…..
-: длинной;
-: непредсказуемостью;
-: все варианты правильные;
-: правильного варианта нет.

I:
S: К угрозам информационной безопасности для общества можно отнести …
-: нарушение права граждан на защиту своего здоровья от неосознаваемой человеком вредной информации;
-: препятствия в построении информационного общества;
-: манипулирование массовым сознанием;
-: препятствие формированию институтов общественного контроля органов государственной власти;
-: противодействие защите государственных информационных систем и государственных информационных ресурсов.

I:
S: По происхождению угрозы информационной безопасности бывают …
-: сторонние;
-: внезапные;
-: внутренние;
-: ожидаемые;
-: внешние.

I:
S: Какая информация подлежит защите?
-: информация, которая не подлежит разглашению;
-: секретная информация;
-: важная информация;
-: оперативная информация;
-: конфиденциальная информация.

I:
S: Базовый федеральный закон, регулирующий информационные отношения — это Федеральный закон:
-: «Об информации, информационных технологиях и защите информации»;
-: «О коммерческой тайне»;
-: «Об архивном деле в Российской Федерации»;
-: «О связи».

I:
S: Информация ограниченного доступа — это …
-: информация, доступ к которой ограничен федеральными законами;
-: информация, доступ к которой ограничен законами субъекта РФ;
-: информация, доступ к которой ограничен в силу указа Президента Рф
-: информация, доступ к которой ограничен Конституцией РФ.

I:
S: Термин криптология применяется для обозначения...
-: процесса дешифрования зашифрованного текста
-: процесса шифрования текста
-: специальных методов раскрытия шифров
-: всей области секретной связи

I:
S: В криптосистемах с секретным ключом последний по защищенному каналу передается…
-: в дешифратор
-: в шифратор
-: в источник сообщений
-: в источник ключа

I:
S: Назначение электронной подписи
-: защита данных от несанкционированного копирования
-: удостоверение подлинности сведений
-: выявление закономерностей построения производственных процессов
-: ограничение доступа к информационным массивам
-: защита программ от нелегального использования

I:
S: Криптографическое преобразование
-: многократное использование данных
-: секретное копирование
-: один из наиболее эффективных методов защиты информации
-: простота внесения изменений

I:
S: Криптографическое преобразование повышает безопасность
-: передачи и хранения данных, находящихся в удаленных устройствах памяти
-: использования ключевой дискеты
-: информации при обмене между удаленными объектами

I:
S: Методы защитных криптографических преобразований
-: перестановки
-: замены (подстановки)
-: аппаратные
-: механические
-: аддитивные
-: комбинированные

Критерии оценки тестов (из 50 тестовых заданий)

Критерии	**Баллы**
45-50 правильных ответов	«отлично»
37-44 правильных ответов	«хорошо»
25-36 правильных ответов	«удовлетворительно»
Менее 25 правильных ответов	«неудовлетворительно»

Критерии оценки тестов (из 50 тестовых вопросов)

Критерии	Баллы
45-50 правильных ответов	3 балла
37-44 правильных ответов	2 балла
25-36 правильных ответов	1 балл
Менее 25 правильных ответов	0 баллов

Критерии оценки тестов (за 10 тестовых вопросов):

8-10 правильных ответов	3 балла
5-7 правильных ответов	2 балла
2-4 правильных ответов	1 балл
0-1 правильных ответов	0 баллов

Критерии оценки уровня сформированности компетенций при решении тестовых заданий

1. Определение бинарного признака правильности ответа (решения), дихотомическая оценка – 1 (правильно/ да), 0 – (неправильно/ нет).
2. ***«Повышенный уровень освоения компетенций»*** – студент за отведенное время правильно решил более 80% тестовых заданий.
3. ***«Пороговый уровень освоения компетенций»*** – студент за отведенное время правильно решил от 50 до 80% тестовых заданий.
4. ***«Незачтено»*** – студент за отведенное время правильно решил менее 50% тестовых заданий.
5. Количество выставляемых студенту баллов связано с количеством тестов. При повышенном уровне освоения компетенций рекомендуем выставлять от 0,6 до 0,8 балла, при пороговом от 0,2 до 0,5 баллов. Если студент разрешил менее половины заданий, ему выставляется 0 баллов.

Темы для подготовки докладов-презентаций

Тема	Код компетенции (части) компетенции
1. Обеспечение информационной безопасности. Подсистемы системы информационной безопасности. 2. Основные методы и средства защиты информации, применяемые в корпоративных экономических информационных системах. 3. Потенциальные угрозы безопасности в корпоративных вычислительных сетях. 4. Защита информации в компьютерных сетях. Объекты защиты информации в сети. 5. Формирование политики безопасности предприятия (организации). 6. Важность и сложность проблемы информационной безопасности. 7. Виды угроз безопасности информации. 8. Особенности зарубежного законодательства в области информационной безопасности. 9. Текущее состояние российского законодательства в области информационной безопасности. 10. Основные угрозы государственной и общественной безопасности. 11. Виды и источники угроз информационной безопасности страны (на примере Российской Федерации). 12. Принципы государственной политики обеспечения информационной безопасности страны (на примере Российской Федерации). 13. Защита информации. Комплексный подход к защите информации. 14. Классификация методов защиты информации. 15. Понятие и виды каналов утечки информации ограниченного доступа. 16. Условия и факторы, способствующие утечке информации ограниченного доступа. 17. Основные угрозы безопасности информации. Общая характеристика технических средств несанкционированного получения информации и технологий их применения. 18. Основные направления инженерно-технической защиты информации: физическая защита, скрытие информации, поиск и нейтрализация источников утечки. 19. Уязвимость компьютерных систем. Модель злоумышленника. 20. Понятие «идентификации пользователя». Задача идентификации пользователя. Использование идентификации в защите информационных процессов. 21. Методы и средства защиты данных от несанкционированного доступа. 22. Основные методы несанкционированного доступа при физическом контакте с компьютером.	УК-1 ПК-3

23. Основные причины утечки информации с охраняемых объектов. 24. Разграничение доступа к информации. Идентификация и аутентификация. 25. Основные угрозы безопасности информации в компьютерных системах. **26.** Угрозы безопасности современных информационно-вычислительных и телекоммуникационных сетей. Классификация угроз безопасности.	

Критерии оценивания:

Критерии	**Баллы**
Соответствие заявленной теме	1
Логичность и последовательность изложения материала	2
Способность к работе с информационными источниками	1
Способность к анализу	3
Умение формулировать выводы	3
Итого:	10

Вопросы по темам/разделам дисциплины для коллоквиума

ВОПРОСЫ	**Код компетенции (части) компетенции**
Тема 1. **Информационная безопасность и уровни ее обеспечения.**	УК-1 ПК-3
1. Классификация информации. Виды данных и носителей. 2. Ценность информации. Цена информации. 3. Количество и качество информации. 4. Виды защищаемой информации. 5. Демаскирующие признаки объектов защиты. 6. Классификация источников и носителей информации. 7. Мероприятия по управлению доступом к информации. 8. Методы синтеза информации. 9. Что понимается под доступностью? 10. Что понимают под целостностью информационных ресурсов? 11. Что такое конфиденциальность? Конфиденциальная информация. Угрозы конфиденциальной информации. 12. Утечка информации. Каналы утечки информации. 13. Меры защиты от утечки информации.	
Тема 2. **Государственная политика в обеспечении информационной безопасности.**	УК-1 ПК-3
1. Дайте определение понятию «национальная безопасность Российской Федерации». 2. Перечислите организационные, нормативно-правовые и информационные основы реализации действующей Стратегией национальной безопасности Российской Федерации. Перечислите и охарактеризуйте виды безопасности, предусмотренные Конституцией РФ и законодательством РФ. 3. Руководящие документы гостехкомиссии России в области информационной безопасности. 4. Основные федеральные законы в области защиты информации. 5. Государственные органы власти, обеспечивающие защиту информации в России. 6. Сформулируйте основные угрозы государственной и общественной безопасности. 7. Каковы стратегические цели обеспечения национальной безопасности в области науки, технологий и образования? 8. Какие мероприятия необходимо реализовать в целях обеспечения государственной и общественной безопасности? 9. Анализ статей Уголовного кодекса, касающихся нарушений информационной безопасности. Федеральные Законы и руководящие документы Федеральной службы по экспортному и техническому контролю по вопросам информационной безопасности.	
Тема 3. **Криптографические методы защиты информации.**	УК-1 ПК-3
1. Какие существуют единицы измерения информации?	

2. Дайте определение понятию машинного кода, машинного слова. 3. Шифрование. Требования к системам криптографической защиты. 4. Способы шифрования. 5. Проверка подлинности. Проверка целостности сообщений. Шифры замены и перестановки. 6. Программирование алгоритмов криптосистем с открытом ключом. 7. Криптологические меры защиты информации. 8. Что такое симметричная и асимметричная криптография? 9. Цифровая подпись (ЭП) и асимметричное шифрование. 10. Что такое криптография? 11. Что такое алгоритм шифрования? 12. Как с помощью шифрования защищаются данные? 13. Какой алгоритм шифрования самый стойкий? 14. Что такое ключ шифрования? 15. Какие бывают алгоритмы шифрования?	
Тема 4. **Аудит информационной безопасности. Анализ информационных рисков.**	УК-1 ПК-3
1. Управление рисками информационной безопасности 2. Современные методы и средства анализа и управление рисками информационных систем компаний 3. Роль и место аудита в системе сервисов безопасности организации. 4. Процесс оценки информационной безопасности. 5. Мониторинг и аудит, контроль целостности информации. 6. Управление рисками информационной безопасности 7. Современные методы и средства анализа и управление рисками информационных систем компаний 8. Роль и место аудита в системе сервисов безопасности организации. 9. Процесс оценки информационной безопасности. 10. Мониторинг и аудит, контроль целостности информации.	

Критерии оценивания:

Критерии	Баллы
Отвечает верно	3 балла
Отвечает с незначительными неточностями	2 балла
Отвечает с ошибками, которые при дополнительных вопросах исправляет	1 балл
Не может ответить	0 баллов

Задания для выполнения практических работ

Практическая работа по теме № 1 «Информационная безопасность и уровни ее обеспечения».

Перечень компетенций, проверяемых с помощью практической работы

Индекс	Формулировка компетенции
УК-1	способен осуществлять поиск, критический анализ и синтез информации, применять истемный подход для решения поставленных задач
ПК-3	владение навыками стратегического анализа, разработки и осуществления стратегии организации, направленной на обеспечение конкурентоспособности

Цель работы: повторение теоретической части учебного материала по теме курса, закрепление навыков создания презентаций в приложении MS Power Point.
Объем работы 10 – 15 слайдов, включая титульный слайд, слайд с оглавлением, слайды-приложения с диаграммами и таблицами, список литературы.
Форма отчетности. Презентация должна иметь: титульный лист, оглавление с гиперссылками на разделы и подразделы, текст работы, состоящий из введения, рассматриваемых вопросов и заключения, список литературы. Каждый слайд должен иметь управляющие кнопки для перехода к оглавлению.
Форма отчетности предусматривает демонстрацию презентации. Демонстрация презентации проходит под управлением докладчика в полноэкранном режиме, при этом докладчик должен полностью контролировать ход демонстрации. Наименование тем для подготовки презентаций приведены в таблице.

Практическая работа.
Цель работы: Работа с архиваторами.
Задание: Создайте новую папку на рабочем столе. Найдите в своём компьютере файлы с расширениями jpg, txt, doc, xls, mp3, avi, zip, rar и скопируйте по одному из них в свою папку. Создайте архивный файл, содержащий вашу папку и все находящиеся в ней файлы. Преобразуйте его в самораспаковывающийся архив. Защитите архив паролем. Извлеките файлы из архива. Создайте многотомный архив. Перенесите его в свой каталог на сервере.
Последовательность выполнения работы:
1. На рабочем столе создайте папку «Архивы» (Archives).
2. Найдите в своём компьютере файлы с расширением **jpg, doc**, **txt**, **xls**, **mp3**, **avi**, **zip**, **rar** и скопируйте их (по одному каждого формата) в свою папку на рабочем столе.
3. Для запуска поиска файлов выполните команду **Пуск ◊ Найти ◊ Файлы и папки** и в поле «**Искать имена файлов и папок**» введите: *.**jpg, *.doc, *.txt, *.xls, *.mp3, *.avi, *.zip, *.rar**. Нажмите на кнопку **Найти**.
4. Заархивируйте свою папку на рабочем столе программой WinRar.
- *Наведите указатель мыши на папку, нажмите правую клавишу и выберите команду «**Добавить в** …».*

5. Откройте созданный архивный файл в программе WINRAR и оцените степень сжатия папки. Запишите эти данные в отчет.
- *Наведите указатель мыши на архив и выполните двойной щелчок. Можно вызвать контекстное меню правой клавишей мыши и выбрать команду «**Открыть**».*
- *Степень сжатия папки в целом можно определить, выполнив команду «**Показать информацию**» (нажав кнопку «**Info**»)*

6. Закройте программу WinRar, удалите исходную папку с файлами и извлеките файлы из архива (файла с расширением **rar**).
- *Для того чтобы извлечь файлы из архива, можно вызвать для файла – архива контекстное меню и выбрать одну из команд «**Извлечь** …»*
- *Можно открыть архив в программе WinRar и выполнить щелчок мышью по кнопке «**Извлечь**».*

7. Создайте самораспаковывающийся архив на основе несжатой папки.

- *Наведите указатель мыши на вашу папку, вызовите контекстное меню и выполните команду «**Упаковать в архив** ...»*
- *В группе команд «**Параметры архивации**» выберите команду (установите флажок ⎷ в строке) «**Создать SFX – архив**». Будет создан файл с расширением **.exe**, для распаковки которого программа WinRar уже не нужна.*

8. Закройте программу WinRar, удалите исходную папку с файлами и извлеките файлы из SFX-архива.

- *Для извлечение файлов просто выполните двойной щелчок по файлу-архиву и при необходимости укажите папку назначения, т.е. ту, в которую распакуются файлы. Процесс распаковки архива начнётся при нажатии кнопки «**Извлечь**».*

9. Удалите исходную папку с файлами и извлеките из архива один-два файла.
10. Защитите архив паролем.

- *Паролем можно защитить только вновь создаваемый архив. Поэтому извлеките все файлы из архива, удалите старый архив.*
- *Выполните щелчок правой клавишей мыши по папке, которую собираетесь заархивировать, выберите команду «**Добавить в архив**».*
- *В окне «**Имя и параметры архива**» на вкладке «**Общие**» установите следующие параметры архивации:*
- *Удалить файлы после упаковки;*
- *Создать SFX – архив (для создания самораспаковывающегося архива);*
- *Создать непрерывный архив (такой архив занимает меньше места);*
- *Добавить информацию для восстановления (такой архив занимает больше места, но зато обладает некоторой избыточностью, что позволяет восстанавливать его при незначительных повреждениях);*
- *Протестировать файлы после упаковки.*
- *На вкладке «Дополнительно» нажмите кнопку «Установить пароль», введите пароль 2 раза и установите флажок «Шифровать имена файлов». При выборе этой опции скрывается содержимое архива, т.е. не будет видно даже названий сжатых файлов.*
- *Нажмите «ОК» в окне «Архивация с паролем» и снова «ОК» в окне «Имя и параметры архива».*

11. Извлеките файлы из архива, защищенного паролем.

- Создайте многотомный архив. *Для создания многотомного архива укажите размер его отдельных томов в поле «Разделить на тома размером (в байтах)» или выберите нужный из предлагаемого списка:*

12. Скопируйте в свой каталог на Сервере SFX – архив и многотомный архив. Со своего компьютера удалите все файлы и папки, созданные в этой работе.

Практическая работа №2 по теме «Государственная политика в обеспечении информационной безопасности».

Перечень компетенций, проверяемых с помощью практической работы

Индекс	Формулировка компетенции
УК-1	способен осуществлять поиск, критический анализ и синтез информации, применять истемный подход для решения поставленных задач

Темы для подготовки докладов-презентаций по теме №2

1.Особенности зарубежного законодательства в области информационной безопасности.

2.Текущее состояние российского законодательства в области информационной безопасности.

3.Основные угрозы государственной и общественной безопасности.
4.Основные угрозы государственной и общественной безопасности.
5.Виды и источники угроз информационной безопасности страны (на примере Российской Федерации).
6.Текущее состояние российского законодательства в области информационной безопасности.
7.Формирование политики безопасности предприятия (организации).
8.Принципы государственной политики обеспечения информационной безопасности страны (на примере Российской Федерации).

Цель работы: повторение теоретической части учебного материала по теме курса, закрепление навыков создания презентаций в приложении MS Power Point.

Объем работы 10 – 15 слайдов, включая титульный слайд, слайд с оглавлением, слайды-приложения с диаграммами и таблицами, список литературы.

Форма отчетности. Презентация должна иметь: титульный лист, оглавление с гиперссылками на разделы и подразделы, текст работы, состоящий из введения, рассматриваемых вопросов и заключения, список литературы. Каждый слайд должен иметь управляющие кнопки для перехода к оглавлению.

Форма отчетности предусматривает демонстрацию презентации. Демонстрация презентации проходит под управлением докладчика в полноэкранном режиме, при этом докладчик должен полностью контролировать ход демонстрации. Наименование тем для подготовки презентаций приведены в таблице.

Практическая работа №3 по теме: «Криптографические методы защиты информации».

Перечень компетенций, проверяемых с помощью практической работы

Индекс	Формулировка компетенции
ПК-3	владение навыками стратегического анализа, разработки и осуществления стратегии организации, направленной на обеспечение конкурентоспособности

Цель работы: Исследование основных методов криптографической зашиты информации

1. Шифры перестановки
2. Шифры простой замены
3. Шифры сложной замены

Практическая работа №4. Аудит информационной безопасности. Анализ информационных рисков.

Перечень компетенций, проверяемых с помощью практической работы

Индекс	Формулировка компетенции
УК-1	способен осуществлять поиск, критический анализ и синтез информации, применять истемный подход для решения поставленных задач
ПК-3	владение навыками стратегического анализа, разработки и осуществления стратегии организации, направленной на обеспечение конкурентоспособности

***Цель работы*:** Выявить риски информационной безопасности предприятия, проанализировать их и предложить наиболее эффективные меры по их минимизации.

Теоретические сведения

Оценка рисков нарушения информационной безопасности компьютерных систем является одной из важнейших составляющих процесса управления информационной безопасностью.

Риск – это потенциальная опасность нанесения ущерба организации в результате реализации некоторой угрозы с использованием уязвимостей актива или группы активов. Риск определяется как сочетание вероятности события и его последствий.

Анализ рисков представляет собой процедуры выявления факторов рисков и оценки их значимости, по сути, анализ вероятности того, что произойдут определенные нежелательные события и отрицательно повлияют на достижение целей проекта. Анализ рисков включает оценку рисков и методы снижения рисков или уменьшения связанных с ним неблагоприятных последствий, т.е. идентификацию и вычисление уровней (мер) рисков на основе оценок, присвоенных ресурсам, угрозам и уязвимостям ресурсов.

Назначение анализа рисков – дать потенциальным партнерам необходимые данные для принятия решений о целесообразности участия в проекте и выработки мер по защите от возможных финансовых потерь.

Анализ рисков можно подразделить на два взаимно дополняющих друг друга вида: качественный и количественный. *Качественный анализ* имеет целью определить (идентифицировать) факторы, области и виды рисков. *Количественный анализ* рисков должен дать возможность численно определить размеры отдельных рисков и риска проекта в целом.

Контроль рисков состоит в идентификации и выборе контрмер, позволяющих снизить риски до приемлемого уровня.

Целью ***оценки рисков*** является выявление следующих положений: приемлемость существующих рисков;

- определение неприемлемых рисков, которые в первую очередь нуждаются в уменьшении;
- определение защитных средств, экономически целесообразных для уменьшения неприемлемых рисков.

Ход выполнения работы:

1. Проанализировать систему информационной безопасности конкретной организации (рассмотреть имеющиеся средства и методы защиты информации).
2. Произвести оценку рисков существующей системы безопасности, результаты свести в таблицу.

Таблица – Оценка рисков существующей системы безопасности организации

Наименование угрозы	**Вероятность наступления**	**Ущерб от реализации**	**Риск**
Стихийные бедствия, аварии, пожары и пр.		3	
Непреднамеренные ошибки пользователей		2	
Перебои электропитания		2	
Вредоносное программное обеспечение		3	

Халатность пользователей		2	
Другое			
Сумма рисков:			

1. Проставить в таблице коэффициент вероятности наступления и коэффициент ущерба от реализации угрозы по 3х балльной шкале.
2. Произведение этих составляющих позволят **определить риск.**
Рассчитать общую **сумму** рисков.
На основе полученных данных выделить три типа риска: низкий (1,2), средний (3,4), высокий (от 5…).
Построить диаграмму оценки рисков по категориям.
Сделать выводы.

Критерии оценки:

Критерии	Баллы
Выполняет работу верно	3 балла
Выполняет работу с незначительными неточностями	2 балла
Выполняет работу с ошибками, которые при дополнительных вопросах исправляет	1 балла
Не может выполнить работу	0 баллов

Типовые контрольные задания, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций в процессе освоения образовательной программы.

Примерный перечень вопросов по закреплению теоретических знаний, умений и практических навыков, предусмотренных компетенциями:

Индекс	Формулировка компетенции
УК-1	способен осуществлять поиск, критический анализ и синтез информации, применять истемный подход для решения поставленных задач
ПК-3	владение навыками стратегического анализа, разработки и осуществления стратегии организации, направленной на обеспечение конкурентоспособности

Темы контрольной работы

1. Построение системы защиты информации в информационной системе.
2. Методы несанкционированного доступа к информации.
3. Использование биометрических данных. Управление доступом.
4. Потенциальные каналы утечки информации.
5. Электронный документ, электронная подпись, владелец сертификата ключа подписи, средства электронной подписи, сертификат средств электронной подписи.

6. Закрытый ключ электронной цифровой подписи, открытый ключ электронной подписи, сертификат ключа подписи, подтверждение подлинности электронной подписи в электронном документе.
7. Понятие «идентификации пользователя». Задача идентификации пользователя. Использование идентификации в защите информационных процессов.
8. Методы и средства защиты данных от несанкционированного доступа.
9. Основные понятия и определения информационной безопасности. Особенности защиты информации в социально-экономических информационных системах.
10. Основные методы и средства защиты информации, применяемые в корпоративных экономических информационных системах.
11. Правовые меры обеспечения информационной безопасности в социальноэкономических информационных системах.
12. Законодательные и нормативные акты Российской Федерации в области защиты информации.
13. Использование электронных ключей для организации информационной безопасности.
14. Организационно-административные методы защиты, применяемые в социальноэкономических информационных системах.
15. Идентификация пользователей, аутентификация пользователей и авторизация пользователей (назначение и способы реализации).
16. Криптографические методы защиты информации. Математическое и алгоритмическое обеспечение криптографических методов защиты информации.
17. Симметричные и асимметричные криптосистемы.
18. Потенциальные угрозы безопасности в Интернет (и в частности в электронной коммерции). Методы защиты информации в сети Интернет.
19. Аудит информационной безопасности.
20. Управление информационными рисками.

Критерии оценивания:

Критерии	**Баллы**
Соответствие заявленной теме	1
Логичность и последовательность изложения материала	2
Способность к работе с информационными источниками	1
Способность к анализу	3
Умение формулировать выводы	3
Итого:	10

Федеральное государственное бюджетное образовательное учреждение высшего образования
«РОССИЙСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ПРАВОСУДИЯ»
Вопросы для дифференцируемого зачета

1. Основные понятия и определения информационной безопасности. Особенности защиты информации в социально-экономических информационных системах.
2. Основные методы и средства защиты информации, применяемые в корпоративных экономических информационных системах.
3. Правовые меры обеспечения информационной безопасности в социально-экономических информационных системах.
4. Законодательные и нормативные акты Российской Федерации в области защиты информации.
5. Использование электронных ключей для организации информационной безопасности.
6. Принципы и показатели эффективности криптографической защиты информации
7. Организационно-административные методы защиты, применяемые в социально-экономических информационных системах.
8. Формирование политики безопасности предприятия (организации).
9. Идентификация пользователей, аутентификация пользователей и авторизация пользователей (назначение и способы реализации).
10. Криптографические методы защиты информации. Математическое и алгоритмическое обеспечение криптографических методов защиты информации.
11. Симметричные и асимметричные криптосистемы.
12. Электронная подпись. Использование электронной подписи в экономических системах.
13. Защита информации в компьютерных сетях. Объекты защиты информации в сети.
14. Потенциальные угрозы безопасности в Интернет. Методы защиты информации в сети Интернет.
15. Количественный подход к информационной безопасности. Оценка защищенности механизмов защиты.
16. Аудит информационной безопасности.
17. Управление информационными рисками.
18. Проведение анализа информационной системы. Выявление угроз и уязвимостей, каналов утечки информации
19. Построение системы защиты информации в информационной системе.
20. Этапы разработки мер по предотвращению угроз утечки информации.

Зам. зав. кафедрой Галяутдинова Л.Р., к.ф-м..н, доцент

_____/ __Галяутдинова Л.Р._____
(подпись) (ФИО)

Критерии оценивания дифференцированного зачета:

Критерии	Баллы

ДКЗ выполнено и/или классная контрольная летучка выполнена с оценкой «удовлетворительно».	21 – 40 (допуск к зачету)
ДКЗ не выполнено или выполнено с оценкой «неудовлетворительно» и/или классная контрольная летучка выполнена с оценкой «неудовлетворительно».	0 – 20 (недопуск к зачету)
На зачете на теоретические вопросы даны практически полные ответы и в решении практической задачи ошибок не допущено (51 – 60 баллов).	80 – 100 (отлично)
На зачете на теоретические вопросы даны неполные ответы (не менее 59 баллов) и в решении практической задачи допущено не более одной ошибок (41 – 50 баллов).	59 – 79 (хорошо)
На зачете на теоретические вопросы даны неполные ответы и в решении практической задачи допущено не более двух ошибок (16 – 40 баллов) .	37 – 58 (удовлетворительно)
Не получен ответ хотя бы на один из теоретических вопросов или на теоретические вопросы даны неполные ответы (не более 36 баллов) или в решении практической задачи допущено более двух ошибок (0 – 15 баллов).	0 – 36 (неудовлетворительно)

Уровни сформированности компетенций			
ниже порога	***пороговый***	***базовый***	***продвинутый***
«2»	***«3»***	***«4»***	***«5»***
Не зачтено	***зачтено***		
Компетенция не сформирована. Отсутствие знаний и уровня самостоятельности практического навыка.	Компетенция сформирована. Демонстрируется недостаточный уровень самостоятельности практического навыка.	Компетенция сформирована. Демонстрируется достаточный уровень самостоятельности устойчивого практического навыка.	Компетенция сформирована. Демонстрируется высокий уровень самостоятельности, высокая адаптивность практического навыка.

Федеральное государственное бюджетное образовательное учреждение высшего образования
«РОССИЙСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ПРАВОСУДИЯ»

Билет № __

Дисциплина: **Математические методы защиты информации**

1. Основные методы и средства защиты информации, применяемые в корпоративных экономических информационных системах.
2. Количественный подход к информационной безопасности. Оценка защищенности механизмов защиты.

Зам. зав. кафедрой Галяутдинова Л.Р., к.ф-м..н, доцент

_____/ __Галяутдинова Л.Р._____
(подпись) (ФИО)