

Федеральное государственное бюджетное образовательное учреждение высшего образования «Тамбовский государственный университет имени Г.Р. Державина»
Институт математики, физики и информационных технологий
Кафедра математического моделирования и информационных технологий

УТВЕРЖДАЮ:
Директор института



Н. Я. Королева
«04» июля 2022 г.

РАБОЧАЯ ПРОГРАММА

по дисциплине Б1.О.19 Организационное и правовое обеспечение информационной безопасности

Направление подготовки/специальность: 10.03.01 - Информационная безопасность

Профиль/направленность/специализация: Безопасность компьютерных систем

Уровень высшего образования: бакалавриат

Квалификация: Бакалавр

год набора: 2022

Автор программы:

Кандидат педагогических наук, доцент Михайлова Елена Михайловна

Рабочая программа составлена в соответствии с ФГОС ВО по направлению подготовки 10.03.01 - Информационная безопасность (уровень бакалавриата) (приказ Министерства образования и науки РФ от «17» ноября 2020 г. № 1427).

Рабочая программа принята на заседании Кафедры математического моделирования и информационных технологий «29» июня 2022 г. Протокол № 12

Рассмотрена и одобрена на заседании Ученого совета Института математики, физики и информационных технологий, Протокол от «04» июля 2022 г. № 6.

СОДЕРЖАНИЕ

1. Цели и задачи дисциплины.....	4
2. Место дисциплины в структуре ОП бакалавра.....	5
3. Объем и содержание дисциплины.....	5
4. Контроль знаний обучающихся и типовые оценочные средства.....	14
5. Методические указания для обучающихся по освоению дисциплины (модуля).....	28
6. Учебно-методическое и информационное обеспечение дисциплины.....	29
7. Материально-техническое обеспечение дисциплины, программное обеспечение, профессиональные базы данных и информационные справочные системы.....	31

1. Цели и задачи дисциплины

1.1 Цель дисциплины – формирование компетенций:

ОПК-5 Способен применять нормативные правовые акты, нормативные и методические документы, регламентирующие деятельность по защите информации в сфере профессиональной деятельности

ОПК-6 Способен при решении профессиональных задач организовывать защиту информации ограниченного доступа в соответствии с нормативными правовыми актами, нормативными и методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю

1.2 Типы задач профессиональной деятельности, к которым готовятся обучающиеся в рамках освоения дисциплины:

- организационно-управленческий

1.3 Дисциплина ориентирована на подготовку обучающихся к профессиональной деятельности в сфере: 06 Связь, информационные и коммуникационные технологии (в сфере техники и технологии, охватывающей совокупность проблем, связанных с обеспечением защищенности объектов информатизации в условиях существования угроз в информационной сфере)

1.4 В результате освоения дисциплины у обучающихся должны быть сформированы:

Обобщенные трудовые функции / трудовые функции / трудовые или профессиональные действия (при наличии профстандарта)	Код и наименование компетенции ФГОС ВО, необходимой для формирования трудового или профессионального действия	Индикаторы достижения компетенций
	ОПК-5 Способен применять нормативные правовые акты, нормативные и методические документы, регламентирующие деятельность по защите информации в сфере профессиональной деятельности	Применяет нормативные правовые акты, нормативные и методические документы, регламентирующие деятельность по защите информации в сфере профессиональной деятельности
	ОПК-6 Способен при решении профессиональных задач организовывать защиту информации ограниченного доступа в соответствии с нормативными правовыми актами, нормативными и методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю	Организует защиту информации ограниченного доступа в соответствии с нормативными правовыми актами, нормативными и методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю

1.5 Согласование междисциплинарных связей дисциплин, обеспечивающих освоение компетенций:

ОПК-6 Способен при решении профессиональных задач организовывать защиту информации ограниченного доступа в соответствии с нормативными правовыми актами, нормативными и методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю

№ п/п	Наименование дисциплин, определяющих междисциплинарные связи	Форма обучения	
		Очная (семестр)	
		6	7
1	Аудит и аттестация объектов информатизации	+	+

2. Место дисциплины в структуре ОП бакалавриата:

Дисциплина «Организационное и правовое обеспечение информационной безопасности» относится к обязательной части учебного плана ОП по направлению подготовки 10.03.01 - Информационная безопасность.

Дисциплина «Организационное и правовое обеспечение информационной безопасности» изучается в 3 семестре.

3. Объем и содержание дисциплины

3.1. Объем дисциплины: 4 з.е.

Очная: 4 з.е.

Вид учебной работы	Очная (всего часов)
Общая трудоёмкость дисциплины	144
Контактная работа	64
Лекции (Лекции)	32
Лабораторные (Лаб. раб.)	32
Самостоятельная работа (СР)	44
Экзамен	36

3.2. Содержание курса:

№ темы	Название раздела/темы	Вид учебной работы, час.			Формы текущего контроля
		Лек ции	Лаб · раб.	СР	
		О	О	О	
3 семестр					
1	Информационная безопасность и организационные основы защиты информации	4	4	8	Собеседование

2	Организация внутриобъектного режима предприятия	4	4	8	Реферат; Тестирование
3	Организация и функции службы безопасности предприятия	6	Пп 6	8	Собеседование; Защита лабораторных работ; Практическое задание для практической подготовки
4	Организация информационно-аналитической работы	6	6	8	Собеседование
5	Организация конфиденциального делопроизводства	6	6	6	Собеседование; Тестирование
6	Организация работы с персоналом предприятия	6	Пп 6	6	Собеседование; Защита лабораторных работ; Практическое задание для практической подготовки

Тема 1. Информационная безопасность и организационные основы защиты информации (ОПК-6)

Лекция.

В лекции рассматриваются базовые вопросы информационной безопасности и организационные основы защиты информации. Информационная безопасность, виды и источники угроз информационной безопасности, методы обеспечения информационной безопасности Российской Федерации, регулирование отношений в сфере ИБ.

Организационная защита информации - это регламентация производственной деятельности и взаимоотношений исполнителей на нормативно-правовой основе, исключающей или существенно затрудняющей неправомерное овладение конфиденциальной информацией, и включает в себя организацию режима охраны, организацию работы с сотрудниками, с документами, организацию использования технических средств и работу по анализу угроз информационной безопасности.

Организационная защита информации:

- Организация работы с персоналом;
- Организация внутриобъектного и пропускного режимов и охраны;
- Организация работы с носителями сведений;
- Комплексное планирование мероприятий по защите информации;
- Организация аналитической работы и контроля.

Основные принципы организационной защиты информации:

- принцип комплексного подхода — эффективное использование сил, средств, способов и методов защиты информации для решения поставленных задач в зависимости от конкретной складывающейся ситуации и наличия факторов, ослабляющих или усиливающих угрозу защищаемой информации;

- принцип оперативности принятия управленческих решений (существенно влияет на эффективность функционирования и гибкость системы защиты информации и отражает нацеленность руководства и персонала предприятия на решение задач защиты информации);
- принцип персональной ответственности — наиболее эффективное распределение задач по защите информации между руководством и персоналом предприятия и определение ответственности за полноту и качество их выполнения.

Среди основных условий организационной защиты информации можно выделить следующие:

- непрерывность всестороннего анализа функционирования системы защиты информации в целях принятия своевременных мер по повышению ее эффективности;
- неукоснительное соблюдение руководством и персоналом предприятия установленных норм и правил защиты конфиденциальной информации.

При соблюдении перечисленных условий обеспечивается наиболее полное и качественное решение задач по защите конфиденциальной информации на предприятии.

Руководитель предприятия несет персональную ответственность за организацию и проведение необходимых мероприятий, направленных на исключение утечки сведений, отнесенных к конфиденциальной информации, и утрат носителей информации. Он обязан:

- знать фактическое состояние дел в области защиты информации, организовывать постоянную работу по выявлению и закрытию возможных каналов утечки конфиденциальной информации;
- определять обязанности и задачи должностным лицам и структурным подразделениям предприятия в этой области;
- проявлять высокую требовательность к персоналу предприятия в вопросах сохранности конфиденциальной информации;
- оценивать деятельность должностных лиц и эффективность мероприятий по защите информации.

К административному уровню информационной безопасности относятся действия общего характера, предпринимаемые руководством организации. Главная цель мер административного уровня – сформировать программу работ в области информационной безопасности и обеспечить ее выполнение, выделяя необходимые ресурсы и контролируя состояние дел.

Основой программы является политика безопасности, отражающая подход организации к защите своих информационных активов. Руководство каждой организации должно осознать необходимость поддержания режима безопасности и выделения на эти цели значительных ресурсов. Политика безопасности строится на основе анализа рисков, которые признаются реальными для информационной системы организации. Когда риски проанализированы и стратегия защиты определена, составляется программа обеспечения информационной безопасности. Под эту программу выделяются ресурсы, назначаются ответственные, определяется порядок контроля выполнения программы.

Термин "политика безопасности" отражает стратегию организации в области информационной безопасности. Для выработки стратегии и проведения ее в жизнь нужны, несомненно, политические решения, принимаемые на самом высоком уровне.

Под политикой безопасности понимаем совокупность документированных решений, принимаемых руководством организации и направленных на защиту информации и ассоциированных с ней ресурсов.

Политика безопасности

С практической точки зрения политику безопасности целесообразно рассматривать на трех уровнях детализации. К верхнему уровню можно отнести решения, затрагивающие организацию в целом. Они носят весьма общий характер и, как правило, исходят от руководства организации. Примерный список подобных решений может включать в себя следующие элементы:

- решение сформировать или пересмотреть комплексную программу обеспечения информационной безопасности, назначение ответственных за продвижение программы;
- формулировка целей, которые преследует организация в области информационной безопасности, определение общих направлений в достижении этих целей;
- обеспечение базы для соблюдения законов и правил;

- формулировка административных решений по тем вопросам реализации программы безопасности, которые должны рассматриваться на уровне организации в целом.

Для политики верхнего уровня цели организации в области информационной безопасности формулируются в терминах целостности, доступности и конфиденциальности. Если организация отвечает за поддержание критически важных баз данных, на первом плане может стоять уменьшение числа потерь, повреждений или искажений данных. Для организации, занимающейся продажей компьютерной техники, вероятно, важна актуальность информации о предоставляемых услугах и ценах и ее доступность максимальному числу потенциальных покупателей. Руководство режимного предприятия в первую очередь заботится о защите от несанкционированного доступа, то есть о конфиденциальности.

В политике должны быть определены обязанности должностных лиц по выработке программы безопасности и проведению ее в жизнь. В этом смысле политика безопасности является основой подотчетности персонала.

Политика верхнего уровня имеет дело с тремя аспектами законопослушности и исполнительской дисциплины.

Во-первых, организация должна соблюдать существующие законы.

Во-вторых, следует контролировать действия лиц, ответственных за выработку программы безопасности.

Наконец, необходимо обеспечить определенную степень исполнительности персонала, а для этого нужно выработать систему поощрений и наказаний.

К среднему уровню можно отнести вопросы, касающиеся отдельных аспектов информационной безопасности, но важные для различных эксплуатируемых организацией систем. Примеры таких вопросов – отношение к передовым (но, возможно, недостаточно проверенным) технологиям, доступ в Internet (как совместить свободу доступа к информации с защитой от внешних угроз?), использование домашних компьютеров, применение пользователями неофициального программного обеспечения и т.д.

Роли и обязанности. В "политический" документ необходимо включить информацию о должностных лицах, ответственных за реализацию политики безопасности. Например, если для использования неофициального программного обеспечения сотрудникам требуется разрешение руководства, должно быть известно, у кого и как его можно получить. Если неофициальное программное обеспечение использовать нельзя, следует знать, кто следит за выполнением данного правила.

Законопослушность. Политика должна содержать общее описание запрещенных действий и наказаний за них.

Точки контакта. Должно быть известно, куда следует обращаться за разъяснениями, помощью и дополнительной информацией. Обычно "точкой контакта" служит определенное должностное лицо, а не конкретный человек, занимающий в данный момент данный пост.

Политика безопасности нижнего уровня относится к конкретным информационным сервисам. Приведем несколько примеров вопросов, на которые следует дать ответ в политике безопасности нижнего уровня:

- кто имеет право доступа к объектам, поддерживаемым сервисом?
- при каких условиях можно читать и модифицировать данные?
- как организован удаленный доступ к сервису?

При формулировке целей политики нижнего уровня можно исходить из соображений целостности, доступности и конфиденциальности, но нельзя на этом останавливаться. Ее цели должны быть более конкретными. Например, если речь идет о системе расчета заработной платы, можно поставить цель, чтобы только сотрудникам отдела кадров и бухгалтерии позволялось вводить и модифицировать информацию. В более общем случае цели должны связывать между собой объекты сервиса и действия с ними.

Из целей выводятся правила безопасности, описывающие, кто, что и при каких условиях может делать. Чем подробнее правила, чем более формально они изложены, тем проще поддержать их выполнение программно-техническими средствами. С другой стороны, слишком жесткие правила могут мешать работе пользователей, вероятно, их придется часто пересматривать. Руководству предстоит найти разумный компромисс, когда за приемлемую цену будет обеспечен приемлемый уровень безопасности, а сотрудники не окажутся чрезмерно связаны. Обычно наиболее формально задаются права доступа к объектам ввиду особой важности данного вопроса.

На предприятиях для организации работ по защите информации могут создаваться следующие основные виды структурных подразделений:

режимно-секретные;

подразделения по технической защите информации и противодействию иностранным техническим разведкам;

подразделения криптографической защиты информации; мобилизационные;

подразделения охраны и пропускного режима.

Кроме того, защита информации организационными средствами предполагает защиту без использования технических средств. Иногда, задача решается простым удалением основных технических средств и систем (ОТСС) от границы контролируемой зоны на максимально возможное расстояние.

Так же возможен вариант размещения, например, трансформаторной подстанции и контура заземления в пределах контролируемой зоны. К организационно-техническим можно отнести так же удаление вспомогательных технических средств и систем (ВТСС), линии, которых выходят за пределы контролируемой зоны, запрещение использования ОТСС с паразитной генерацией для обработки информации, проведение специальных проверок технических средств на отсутствие закладочных устройств. Необходимо помнить, что организационно-технические меры требуют выполнения комплекса мер, предписанных нормативными документами.

Лабораторные работы.

1. Какой Государственный стандарт в области информационной безопасности является основным?
2. Какой стандарт устанавливает классификацию и перечень факторов, воздействующих на безопасность защищаемой информации?
3. Какие существуют виды угроз информационной безопасности Российской Федерации по общей направленности?
4. Что относится к внешним источникам угроз информационной безопасности Российской Федерации?
5. На какие виды разделяются общие методы обеспечения информационной безопасности Российской Федерации?
6. Кто играет основную роль в создании правовых механизмов защиты информации?
7. Функции межведомственной комиссии?
8. Какой орган формирует законодательную базу в области защиты информации?
9. Функции службы внешней разведки Российской Федерации?
10. Основные задачи ФСТЭК?

Задания для самостоятельной работы.

- подготовка к практическим занятиям, повторение изучения лекционного материала;
- подготовка к лекциям, повторение учебного материала предыдущих лекций;
- изучение материалов лекционного курса по заданиям на самостоятельную проработку, выдаваемых преподавателем на занятиях.

Тема 2. Организация внутриобъектного режима предприятия (ОПК-5)

Лекция.

Для различных объектов вводится специальный режим – внутриобъектовый. Это целый комплекс правил, который охватывает такие направления, как:

Соблюдение сотрудниками правил пожарной безопасности;

Введение четкого графика работы персонала;

Установление правил для посещения сторонними лицами;

Сборка и установка технических приспособлений для охраны объекта – ограждений, сигнализации и т.д.;

Защита территории объекта от бесконтрольного передвижения посетителей.

Для правильной организации внутриобъектового режима важна строгая отчетность. Если на объекте нет специальных цифровых носителей, то сотрудники охраны заполняют специальные журналы и бланки, в которых помимо учета рабочего времени сотрудников и регистрации посетителей отражается также ввоз и вывоз имущества, графики дежурств и прием/сдача помещений под охрану.

Лабораторные работы.

1. Кому выдаются материальные пропуска?

1) выдаются лицам, ответственным за сохранность материальных средств

2) выдаются сотрудникам при поступлении на работу на основании приказа о зачислении в штат

3) выдаются лицам, работающим временно, или прикомандированным посетителям предприятия

2. ЧТО ОТНОСИТСЯ К СРЕДСТВАМ ФИЗИЧЕСКОЙ ЗАЩИТЫ? (выберете два варианта)

1) Ограждения и запирающие устройства

2) Антивирусное ПО

3) Пароль

4) Средства физической изоляции

3. КАКОВО ВРЕМЯ ДЕЙСТВИЯ РАЗОВОГО ПРОПУСКА?

1) 30 минут со времени выдачи до входа в здание

2) Действует до выхода из здания

3) 45 минут с момента выдачи до входа в здание

4) 60 минут с момента выдачи до входа в здание

4. КАКИЕ ИЗ ПЕРЕЧИСЛЕННЫХ ВИДОВ ПРОПУСКОВ СУЩЕСТВУЮТ

1) Постоянные, временные, разовые

2) одноразовые, двухразовые

3) оба варианта верно

5. КАКИЕ ИЗ ПЕРЕЧИСЛЕННЫХ ВИДОВ ОХРАНЫ СУЩЕСТВУЮТ?

1) Охрана с помощью технических средств

2) Комбинированная охрана

3) оба варианта верно

Задания для самостоятельной работы.

- подготовка к практическим занятиям, повторение изучения лекционного материала;
- подготовка к лекциям, повторение учебного материала предыдущих лекций;
- изучение материалов лекционного курса по заданиям на самостоятельную проработку, выдаваемых преподавателем на занятиях.

Лекция.

Служба безопасности - одна из важнейших структурных единиц на любом современном предприятии, отвечающая за обеспечение безопасности проведения производственных и прочих внутренних процессов от несанкционированных посягательств. Ознакомившись с нижеизложенной информацией, вы узнаете чем занимается служба безопасности фирмы, организации, предприятия с какими полномочиями она располагает.

Служба охраны занимается следующими задачами:

- обеспечением безопасности деятельности компании;
- организацией грамотных правовых и прочих взаимодействий;
- исключением вероятности несанкционированного доступа к информации;
- контролем соблюдения правил доступа и допуска к предметам коммерческой тайны;
- своевременным выявлением и перекрытием каналов утечки информации;
- охраной зданий, помещений, всевозможного оборудования и прочей собственности компании.

Таким образом, служба охраны отвечает за обеспечение безопасности внутри компании по всем возможным направлениям деятельности.

Лабораторные работы.

1. Организация защиты персональных данных на предприятии.
2. Основные направления, принципы и методы обеспечения информационной безопасности.
3. Правовые режимы защиты конфиденциальной информации
4. Международное законодательство в области защиты информации
5. Система организационной защиты информации

Задания для самостоятельной работы.

- подготовка к практическим занятиям, повторение изучения лекционного материала;
- подготовка к лекциям, повторение учебного материала предыдущих лекций;
- изучение материалов лекционного курса по заданиям на самостоятельную проработку, выдаваемых преподавателем на занятиях.

Тема 4. Организация информационно-аналитической работы (ОПК-5)

Лекция.

Сбор и анализ информации является важнейшим условием и исходным этапом разработки эффективного управленческого решения. На современном этапе развития общества и управления организация и технологии анализа управленческой информации приобретают исключительно высокое значение.

Особую важность это имеет применительно к практике государственного управления. Об эффективности государственного управления можно говорить, если государственные органы “вовремя обнаруживают проблемы и находят рациональные пути их решения, но еще лучше, когда эти проблемы выявляются в момент их зарождения, либо когда принимаются меры для их предупреждения”. Как правило, к управленцу поступает первичная информация, которую он обрабатывает сам и на основе этого принимает решения. “Первичная информация непригодна для обеспечения поддержки процессов принятия решения, поэтому представляется нецелесообразным, чтобы лицо, принимающее решения, осуществляло поиск информации и ее анализ”.

Эти функции в государственном управлении – прерогатива специальных отделов (информационно-аналитических служб), основное назначение которых состоит в обеспечении аналитически обработанной информацией соответствующие органы государственной власти. Существование информационно-аналитических отделов актуально в связи с тем, что есть необходимость в постоянном “получении актуальной информации, отслеживании и анализе качества получаемой информации”, выполнения таких процессов как “селекция и интерпретация информации, предоставляемой лицам, принимающим решения”.

Информационно-аналитические службы являются центрами сбора и обработки первичной информации, они осуществляют “мониторинг ситуации, ее диагностику, проводят анализ и моделируют возможное развитие событий”.

Лабораторные работы.

1. Что такое информационно-аналитическая деятельность?
2. Какие направления информационно – аналитической работы вы знаете?
3. Что предусматривает аналитическая работа с источником угрозы конфиденциальной информации?
4. Что является одним из самых важных разделов аналитической работы?
5. Что является первым этапом информационно-аналитической работы?
6. Что отражает частоту взаимодействия субъектов за определенный период времени?
7. Какие графики используются для регистрации событий?
8. Что представляют собой экспертные системы?
9. Что включает в себя обнаружение каналов НСД к конфиденциальной информации предприятия?
10. На каком этапе информационно-аналитической работы происходит выделение посторонней информации?

Задания для самостоятельной работы.

- подготовка к практическим занятиям, повторение изучения лекционного материала;
- подготовка к лекциям, повторение учебного материала предыдущих лекций;
- изучение материалов лекционного курса по заданиям на самостоятельную проработку, выдаваемых преподавателем на занятиях.

Тема 5. Организация конфиденциального делопроизводства (ОПК-5)

Лекция.

Организация конфиденциального делопроизводства означает создание необходимых условий для изготовления и получения конфиденциальных документов, организации работы с ними и предотвращения утраты и утечки документированной конфиденциальной информации.

Организация конфиденциального делопроизводства включает создание подразделения, обеспечивающего изготовление, учет, хранение, обработку и использование конфиденциальных документов, установление его статуса, структуры, численного и должностного состава, разработку положения о подразделении и должностных инструкций сотрудников, выделение для подразделения служебного помещения, обеспечение необходимых условий труда, разработку или приобретение нормативных документов и методической литературы по организации и ведению конфиденциального делопроизводства, создание постоянно действующей экспертной комиссии, оформление допуска сотрудников к коммерческой и служебной тайне и обучение их правилам работы с конфиденциальными документами.

Конфиденциальное делопроизводство в силу небольшого по сравнению с открытым делопроизводством объема документов и в целях обеспечения условий для сохранности и конфиденциальности документов должно быть централизованным, т.е. сосредоточенным в едином подразделении предприятия. Подразделение конфиденциального делопроизводства может быть самостоятельным структурным подразделением предприятия, подчиненным непосредственно руководителю предприятия, или входить в состав других подразделений, как правило, осуществляющих защиту конфиденциальной информации: службу безопасности, службу защиты информации и др. В «Положении о порядке обращения со служебной информацией ограниченного распространения» сказано: «Прием и учет (регистрация) документов, содержащих служебную информацию ограниченного распространения, осуществляются, как правило, структурными подразделениями, которым поручен прием и учет несекретной документации», однако это целесообразно лишь при незначительном объеме таких документов и при отсутствии документов, содержащих коммерческую тайну.

Лабораторные работы.

1. ЧТО ОТНОСЯТ К ОБЩЕДОСТУПНОЙ ИНФОРМАЦИИ?

- 1) Относятся общеизвестные сведения и иная информация, доступ к которой не ограничен
- 2) Личные данные
- 3) Государственные тайны
- 4) Коммерческие тайны

2. ЧТО ИЗ ПЕРЕЧИСЛЕННОГО ОТНОСИТСЯ К ГОСУДАРСТВЕННОЙ ТАЙНЕ?

- 1) Военные сведения
- 2) Паспортные данные
- 3) Сведения в области экономики, науки и техники
- 4) Всё перечисленное

3. ВЫБЕРЕТЕ ВЕРНЫЕ ПРИЗНАКИ КОНФИДЕЦИАЛЬНОЙ ИНФОРМАЦИИ

- 1) Информация неизвестна третьим лицам
- 2) К ней нет свободного доступа на законном основании
- 3) К ней есть свободный доступ
- 4) Всё перечисленное неверно

4. ЧТО ОТНОСЯТ К ОСНОВНЫМ УГРОЗАМ КОНФИДЕЦИАЛЬНОЙ ИНФОРМАЦИИ?

- 1) Разглашение
- 2) Уточка
- 3) Оба варианта верны

5. ВЫБЕРЕТЕ ВЕРНЫЕ ВАРИАНТЫ О ТАКТИЧЕСКИХ ПРИЕМУЩЕСТВАХ СЭД

- 1) Освобождение офисных площадей
- 2) Возможность коллективной работы над документацией
- 3) Сохранность документов, удобство их применения
- 4) Снижение затрат на ресурсы

Задания для самостоятельной работы.

- подготовка к практическим занятиям, повторение изучения лекционного материала;
- подготовка к лекциям, повторение учебного материала предыдущих лекций;
- изучение материалов лекционного курса по заданиям на самостоятельную проработку, выдаваемых преподавателем на занятиях.

Тема 6. Организация работы с персоналом предприятия (ОПК-6)

Лекция.

Управление персоналом – это процесс системного, планомерно организованного с помощью взаимосвязанных организационных, экономических и социальных механизмов управления, воздействия на персонал организации с целью как обеспечения эффективного функционирования операционного процесса, так и удовлетворения потребностей персонала в их профессиональном и личностном развитии.

Понятие «управление персоналом» (его синонимы – «менеджмент персонала», «управление человеческими ресурсами», «экономика персонала») подразумевает три аспекта: функциональный, организационный, образовательный.

В функциональном отношении под управлением персоналом подразумеваются все задачи и решения, связанные с деятельностью в сфере персонала (например, подбор персонала, введение в работу, использование персонала, повышение квалификации, оплата труда и увольнение работников).

В организационном отношении это понятие охватывает всех лиц и все службы на

предприятия, которые несут ответственность за работу с персоналом (например, линейных менеджеров, отдел персонала, совет работников предприятия).

В качестве учебной и научной дисциплины менеджмент персонала является важной составной дисциплиной науки об управлении организацией.

Сущностью управления персоналом является системное, планомерно организованное воздействие с помощью взаимосвязанных организационно-экономических и социальных мер на процесс формирования, распределения, перераспределения рабочей силы на уровне предприятия, на создание условий для использования трудовых качеств работника (рабочей силы) в целях обеспечения эффективного функционирования предприятия и всестороннего развития занятых на нем работников.

Лабораторные работы.

1. Комплексное обеспечение информационной безопасности при реализации угрозы попытки доступа в удаленную систему.
2. Правила хранения паролей для доступа удалённой системы.
3. Обеспечение инвентаризации установленного ПО для доступа удалённой системы.
4. Проанализировать всевозможные варианты доступа в удаленную систему в организации.
5. Изучить методы борьбы с доступом удаленных систем.

Задания для самостоятельной работы.

- подготовка к практическим занятиям, повторение изучения лекционного материала;
- подготовка к лекциям, повторение учебного материала предыдущих лекций;
- изучение материалов лекционного курса по заданиям на самостоятельную проработку, выдаваемых преподавателем на занятиях.

4. Контроль знаний обучающихся и типовые оценочные средства

4.1. Распределение баллов:

3 семестр

- посещаемость – 10 баллов
- текущий контроль – 48 баллов
- контрольные срезы – 2 среза по 6 баллов каждый
- премиальные баллы – 20 баллов
- ответ на экзамене: не более 30 баллов

Распределение баллов по заданиям:

№ темы	Название темы / вид учебной работы	Формы текущего контроля / срезы	Мах. кол-во баллов	Методика проведения занятия и оценки

1.	Информационная безопасность и организационные основы защиты информации	Собеседование	5	<p>Собеседование предполагает организацию беседы преподавателя со студентами по вопросам практического занятия с целью более обстоятельного выявления их знаний по определенному разделу, теме, проблеме и т.п. Устный опрос может применяться в различных формах: фронтальный, индивидуальный, комбинированный. Основные качества устного ответа подлежащего оценке:</p> <ul style="list-style-type: none"> - правильность ответа по содержанию; - полнота и глубина ответа; - сознательность ответа; - логика изложения материала; - рациональность использованных приемов и способов решения поставленной учебной задачи; - своевременность и эффективность использования наглядных пособий и технических средств при ответе; - использование дополнительного материала; - рациональность использования времени, отведенного на задание. <p>5 баллов – студент умеет сопоставить полученную при подготовке к практическому занятию информацию, сравнивать разные точки зрения на анализируемую проблему, уметь четко формулировать свои вопросы и отвечать на задаваемые ему вопросы</p> <p>2 балла - студент умеет применять полученную при подготовке к практическому занятию информацию, отвечать на большинство вопросов, вести дискуссию .</p> <p>Если студент не владеет проблематикой практического занятия, не может отвечать на вопросы, зачитывает ответ по напечатанному тексту – ответ баллами не оценивается</p>
2.	Организация внутриобъектного режима предприятия	Реферат	3	<p>3 балла – реферат выполнен обучающимся самостоятельно, в полном объеме, с соблюдением необходимых технических параметров; стиль изложения отвечает специфике жанра научной работы; во введении логично, объективно и аргументировано характеризуется научная проблема; содержание реферата включает самостоятельное исследование, а заключение содержат выводы, логично вытекающие из содержания основной части; список литературы оформлен в соответствии с правилами ГОСТа</p> <p>2 балла – во введении четко сформулированы основные позиции реферата, а содержание соответствует теме реферата; в содержании реферата логично, связно, но недостаточно полно излагается теоретическая или практическая часть; заключение содержит выводы, логично вытекающие из содержания основной части; стиль изложения соответствует специфике жанра научной работы; в оформлении списка литературы встречаются незначительные погрешности</p> <p>1 балл – во введении основные позиции реферата сформулированы нечетко или не вполне соответствуют теме исследования; в основной части реферата (теоретической и эмпирической главах) исследование выполнено недостаточно логично (убедительно) и последовательно; выводы в заключение отражают содержание глав не полностью или неточно; в оформлении списка литературы нет единообразия; стиль изложения не отвечает специфике жанра научной работы</p> <p>0 баллов – текст реферата представляет несамостоятельное (компиляция; плагиат) научное исследование; реферат написан с несоблюдением технических и научных требований</p>

		Тестирование(контрольный срез)	6	<p>Оценка теста по текущему разделу или теме дисциплины</p> <p>6 баллов – студент правильно отвечает на 50-100% вопросов в тесте.</p> <p>3 балла - студент правильно отвечает на 25-50% вопросов в тесте.</p>
3.	Организация и функции службы безопасности предприятия	Собеседование	5	<p>Собеседование предполагает организацию беседы преподавателя со студентами по вопросам практического занятия с целью более обстоятельного выявления их знаний по определенному разделу, теме, проблеме и т.п. Устный опрос может применяться в различных формах: фронтальный, индивидуальный, комбинированный. Основные качества устного ответа подлежащего оценке:</p> <ul style="list-style-type: none"> - правильность ответа по содержанию; - полнота и глубина ответа; - сознательность ответа; - логика изложения материала; - рациональность использованных приемов и способов решения поставленной учебной задачи; - своевременность и эффективность использования наглядных пособий и технических средств при ответе; - использование дополнительного материала; - рациональность использования времени, отведенного на задание. <p>5 баллов – студент умеет сопоставить полученную при подготовке к практическому занятию информацию, сравнивать разные точки зрения на анализируемую проблему, уметь четко формулировать свои вопросы и отвечать на задаваемые ему вопросы</p> <p>2 балла - студент умеет применять полученную при подготовке к практическому занятию информацию, отвечать на большинство вопросов, вести дискуссию .</p> <p>Если студент не владеет проблематикой практического занятия, не может отвечать на вопросы, зачитывает ответ по напечатанному тексту – ответ баллами не оценивается</p>
		Защита лабораторных работ	8	<p>Лабораторные работы выполняются по текущему разделу или теме дисциплины.</p> <p>8 баллов – лабораторная работа выполнена в полном объеме, студент свободно владеет материалом, демонстрирует глубокие, систематизированные знания, свободно отвечает на вопросы, используя профессиональную терминологию.</p> <p>4 балла – лабораторная работа выполнена, но имеет некоторые неточности выполнения, студент владеет представленным материалом, отвечает на заданные вопросы.</p> <p>2 балла - лабораторная работа в целом выполнена, однако в процессе выполнения лабораторной работы допущены существенны ошибки, студент слабо владеет информацией по теме, при ответе использует заготовленный текст, затрудняется с ответами на задаваемые вопросы.</p>

		Практическое задание для практической подготовки	2	<p>Практические задания выполняются по тематике практических занятий.</p> <p>2 баллов – практическое задание выполнено в полном объеме, студент свободно владеет материалом, демонстрирует глубокие, систематизированные знания, свободно отвечает на вопросы используя профессиональную терминологию</p> <p>1 балла – практическое задание выполнено, но имеет некоторые неточности выполнения, студент владеет представленным материалом, отвечает на заданные вопросы</p>
4.	Организация информационно-аналитической работы	Собеседование	5	<p>Собеседование предполагает организацию беседы преподавателя со студентами по вопросам практического занятия с целью более обстоятельного выявления их знаний по определенному разделу, теме, проблеме и т.п. Устный опрос может применяться в различных формах: фронтальный, индивидуальный, комбинированный. Основные качества устного ответа подлежащего оценке:</p> <ul style="list-style-type: none"> - правильность ответа по содержанию; - полнота и глубина ответа; - сознательность ответа; - логика изложения материала; - рациональность использованных приемов и способов решения поставленной учебной задачи; - своевременность и эффективность использования наглядных пособий и технических средств при ответе; - использование дополнительного материала; - рациональность использования времени, отведенного на задание. <p>5 баллов – студент умеет сопоставить полученную при подготовке к практическому занятию информацию, сравнивать разные точки зрения на анализируемую проблему, уметь четко формулировать свои вопросы и отвечать на задаваемые ему вопросы</p> <p>2 балла - студент умеет применять полученную при подготовке к практическому занятию информацию, отвечать на большинство вопросов, вести дискуссию .</p> <p>Если студент не владеет проблематикой практического занятия, не может отвечать на вопросы, зачитывает ответ по напечатанному тексту – ответ баллами не оценивается</p>

5.	Организация конфиденциаль- ного делопроизводс- тва	Собеседо- вание	5	<p>Собеседование предполагает организацию беседы преподавателя со студентами по вопросам практического занятия с целью более обстоятельного выявления их знаний по определенному разделу, теме, проблеме и т.п. Устный опрос может применяться в различных формах: фронтальный, индивидуальный, комбинированный. Основные качества устного ответа подлежащего оценке:</p> <ul style="list-style-type: none"> - правильность ответа по содержанию; - полнота и глубина ответа; - сознательность ответа; - логика изложения материала; - рациональность использованных приемов и способов решения поставленной учебной задачи; - своевременность и эффективность использования наглядных пособий и технических средств при ответе; - использование дополнительного материала; - рациональность использования времени, отведенного на задание. <p>5 баллов – студент умеет сопоставить полученную при подготовке к практическому занятию информацию, сравнивать разные точки зрения на анализируемую проблему, уметь четко формулировать свои вопросы и отвечать на задаваемые ему вопросы</p> <p>2 балла - студент умеет применять полученную при подготовке к практическому занятию информацию, отвечать на большинство вопросов, вести дискуссию .</p> <p>Если студент не владеет проблематикой практического занятия, не может отвечать на вопросы, зачитывает ответ по напечатанному тексту – ответ баллами не оценивается</p>
		Тестиров- ание(кон- трольный срез)	6	<p>Оценка теста по текущему разделу или теме дисциплины</p> <p>6 баллов – студент правильно отвечает на 50-100% вопросов в тесте.</p> <p>3 балла - студент правильно отвечает на 25-50% вопросов в тесте.</p>

6.	Организация работы с персоналом предприятия	Собеседование	5	<p>Собеседование предполагает организацию беседы преподавателя со студентами по вопросам практического занятия с целью более обстоятельного выявления их знаний по определенному разделу, теме, проблеме и т.п. Устный опрос может применяться в различных формах: фронтальный, индивидуальный, комбинированный. Основные качества устного ответа подлежащего оценке:</p> <ul style="list-style-type: none"> - правильность ответа по содержанию; - полнота и глубина ответа; - сознательность ответа; - логика изложения материала; - рациональность использованных приемов и способов решения поставленной учебной задачи; - своевременность и эффективность использования наглядных пособий и технических средств при ответе; - использование дополнительного материала; - рациональность использования времени, отведенного на задание. <p>5 баллов – студент умеет сопоставить полученную при подготовке к практическому занятию информацию, сравнивать разные точки зрения на анализируемую проблему, уметь четко формулировать свои вопросы и отвечать на задаваемые ему вопросы</p> <p>2 балла - студент умеет применять полученную при подготовке к практическому занятию информацию, отвечать на большинство вопросов, вести дискуссию .</p> <p>Если студент не владеет проблематикой практического занятия, не может отвечать на вопросы, зачитывает ответ по напечатанному тексту – ответ баллами не оценивается</p>
		Защита лабораторных работ	8	<p>Лабораторные работы выполняются по текущему разделу или темы дисциплины.</p> <p>8 баллов – лабораторная работа выполнена в полном объеме, студент свободно владеет материалом, демонстрирует глубокие, систематизированные знания, свободно отвечает на вопросы, используя профессиональную терминологию.</p> <p>4 балла – лабораторная работа выполнена, но имеет некоторые неточности выполнения, студент владеет представленным материалом, отвечает на заданные вопросы.</p> <p>2 балла - лабораторная работа в целом выполнена, однако в процессе выполнения лабораторной работы допущены существенны ошибки, студент слабо владеет информацией по теме, при ответе использует заготовленный текст, затрудняется с ответами на задаваемые вопросы.</p>
		Практическое задание для практической подготовки	2	<p>Практические задания выполняются по тематике практических занятий.</p> <p>2 балла – практическое задание выполнено в полном объеме, студент свободно владеет материалом, демонстрирует глубокие, систематизированные знания, свободно отвечает на вопросы используя профессиональную терминологию</p> <p>1 балл – практическое задание выполнено, но имеет некоторые неточности выполнения, студент владеет представленным материалом, отвечает на заданные вопросы</p>

7.	Посещаемость	10	<p>10 баллов – стопроцентное посещение занятий студентом</p> <p>7-9 баллов – посещаемость студента составляет не менее 80 % занятий</p> <p>4-6 баллов – посещаемость студента составляет не менее 50 % занятий</p> <p>1-3 балла – посещаемость студента составляет не менее 25 % занятий</p>
8.	Премияльные баллы	20	<p>Дополнительные премияльные баллы могут быть начислены:</p> <ul style="list-style-type: none"> - за проект, выполненный по заказу работодателя и реализованный на практике – 20 баллов; - постоянная активность во время практических занятий – 10 баллов; - полностью подготовленная к публикации статья по тематике в рамках дисциплины – 10 баллов; - участие с докладом во всероссийской олимпиаде по тематике изучаемой дисциплины – 20 баллов; - участие в выставке по тематике изучаемой дисциплины – 20 баллов; - публикация статьи по тематике изучаемой дисциплины в сборнике студенческих работ / материалах всероссийской конференции / журнале из перечня ВАК – 10 / 15 / 20
9.	Ответ на экзамене	30	<p>Оценка «удовлетворительно»- студент имеет достаточный минимальный объем знаний по дисциплине; студентом усвоена основная литература, рекомендованная учебной программой; студент умеет ориентироваться в основных теориях, концепциях и направлениях по дисциплине и давать им оценку; студент умеет делать выводы без существенных ошибок;</p> <p>Оценка «хорошо» – «достаточно полные и систематизированные знания по дисциплине;» умение ориентироваться в основном теориях, концепциях и направлениях дисциплины и давать им критическую оценку; использование научной терминологии, лингвистически и логически правильное изложение ответа на вопросы, умение делать обоснованные выводы; владение инструментарием по дисциплине, умение его использовать в постановке и решении научных и профессиональных задач; усвоение основной и дополнительной литературы, рекомендованной учебной программой по дисциплине; самостоятельная работа на практических занятиях, участие в групповых обсуждениях, высокий уровень культуры исполнения заданий; средний уровень сформированности заявленных в рабочей программе компетенций.</p> <p>- Оценка «отлично» – систематизированные и полные знания по всем разделам дисциплины, а также по основным вопросам, выходящим за пределы учебной программы; точное использование научной терминологии систематически грамотное и логически правильное изложение ответа на вопросы; безупречное владение инструментарием учебной дисциплины, умение его эффективно использовать в постановке научных и практических задач; выраженная способность самостоятельно и творчески решать сложные проблемы и нестандартные ситуации; полное и глубокое усвоение основной и дополнительной литературы, рекомендованной учебной программой по дисциплине; умение ориентироваться в теориях, концепциях и направлениях дисциплины и давать им критическую оценку, используя научные достижения других дисциплин; творческая самостоятельная работа; активное участие в групповых обсуждениях.</p>

10.	Индивидуальные задания, с помощью которых можно набрать дополнительные баллы	10	<p>Доклад студента предполагает организацию совместной дискуссии автора, преподавателя и студентов по вопросам, связанных с определенным разделом, проблеме или способе реализации т.п. После доклада все члены группы активно участвуют в обсуждении, добавляют информацию, задают вопросы и делают замечания докладчику.</p> <p>Основные качества доклада подлежащего оценке:</p> <p>10 баллов – четко сформулированы проблемы, соответствующая теме доклада; полнота раскрытия материала темы доклада; в основной части логично, связно и полно рассмотрены решения проблемы; деление презентации на введение, основную часть и заключение; заключение содержит выводы, логично вытекающие из содержания основной части; нет замечаний по презентационному материалу; правильно используются и приведены авторитетные источники информации; выполнена задача заинтересованности слушателей в группе, активная дискуссия среди студентов при обсуждении доклада.</p> <p>8 баллов – четко сформулированы проблемы, соответствующая теме доклада; достаточно раскрыта тема доклада; в основной части полно рассмотрены решения проблемы; деление презентации на введение, основную часть и заключение; заключение содержит выводы, логично вытекающие из содержания основной части; есть замечания по презентационному материалу; выполнена задача заинтересованности слушателей в группе, активная дискуссия среди студентов при обсуждении доклада.</p> <p>6 баллов - четко сформулированы проблемы, соответствующая теме доклада; достаточно раскрыта тема доклада; недостаточно полно рассмотрены решения проблемы; деление презентации на введение, основную часть и заключение; есть замечания по презентационному материалу; слабо выполнена задача заинтересованности слушателей в группе.</p>
11.	Итого за семестр	100	

Итоговая оценка по экзамену выставляется в 100-балльной шкале и в традиционной четырехбалльной шкале. Перевод 100-балльной рейтинговой оценки по дисциплине в традиционную четырехбалльную осуществляется следующим образом:

100-балльная система	Традиционная система
85 - 100 баллов	Отлично
70 - 84 баллов	Хорошо
50 - 69 баллов	Удовлетворительно
Менее 50	Неудовлетворительно

4.2 Типовые оценочные средства текущего контроля

Защита лабораторных работ

Тема 3. Организация и функции службы безопасности предприятия

1. Организация защиты персональных данных на предприятии.
2. Основные направления, принципы и методы обеспечения информационной безопасности.
3. Правовые режимы защиты конфиденциальной информации
4. Международное законодательство в области защиты информации

5. Система организационной защиты информации

Тема 6. Организация работы с персоналом предприятия

1. Разработка комплекса режимных мероприятий по сохранности конфиденциальной информации на предприятии.
2. Создайте учетные записи двух пользователей.
3. Предусмотрите возможность обработки личных конфиденциальных документов в собственных папках.
4. Создайте требуемые папки, установите разрешения.
5. Создайте от имени пользователя папку и в ней файл.
6. Запретите доступ к файлу администраторам системы.
7. Зарегистрируйтесь администратором, получите доступ к файлу.

Практическое задание для практической подготовки

Тема 3. Организация и функции службы безопасности предприятия

1. Комплексная защита информации на предприятии .
2. Выбрать угрозы, действие которых может быть направлено на ресурс.
3. Указать, через какие уязвимости реализуются выбранные угрозы.
4. Рассчитать риск ИБ для ресурса для двух вариантов работы алгоритма.
5. Разработайте политику разграничения доступа произвольной организации.

Тема 6. Организация работы с персоналом предприятия

1. Комплексное обеспечение информационной безопасности при реализации угрозы попытки доступа в удаленную систему.
2. Правила хранения паролей для доступа удалённой системы.
3. Обеспечение инвентаризации установленного ПО для доступа удалённой системы.
4. Проанализировать всевозможные варианты доступа в удаленную систему в организации.
5. Изучить методы борьбы с доступом удаленных систем.

Реферат

Тема 2. Организация внутриобъектного режима предприятия

1. Комплексная защита информации на предприятии .
2. Комплексное обеспечение информационной безопасности при реализации угрозы попытки доступа в удаленную систему.
3. Организация защиты персональных данных на предприятии.
4. Основные направления, принципы и методы обеспечения информационной безопасности.
5. Разработка комплекса режимных мероприятий по сохранности конфиденциальной информации на предприятии.

Собеседование

Тема 1. Информационная безопасность и организационные основы защиты информации

1. Какой Государственный стандарт в области информационной безопасности является основным?
2. Какой стандарт устанавливает классификацию и перечень факторов, воздействующих на безопасность защищаемой информации?
3. Какие существуют виды угроз информационной безопасности Российской

Федерации по общей направленности?

4. Что относится к внешним источникам угроз информационной безопасности Российской Федерации?
5. На какие виды разделяются общие методы обеспечения информационной безопасности Российской Федерации?
6. Кто играет основную роль в создании правовых механизмов защиты информации?
7. Функции межведомственной комиссии?
8. Какой орган формирует законодательную базу в области защиты информации?
9. Функции службы внешней разведки Российской Федерации?
10. Основные задачи ФСТЭК?

Тема 3. Организация и функции службы безопасности предприятия

1. Что такое служба безопасности предприятия?
2. Кто принимает решение о создании системы безопасности?
3. Что такое кризисная ситуация?
4. Какие задачи решает анти-кризисная группа?
5. Что в себя включает инженерно-техническая защита информации?
6. Что относится к организационным мероприятиям по защите информации?
7. Что необходимо делать для пресечения несанкционированного доступа (НСД) к информационным системам?
8. Основными способами несанкционированного доступа к ИС являются?
9. Чему должна отводиться основная роль в деятельности службы безопасности предприятия?

Тема 4. Организация информационно-аналитической работы

1. Что такое информационно-аналитическая деятельность?
2. Какие направления информационно – аналитической работы вы знаете?
3. Что предусматривает аналитическая работа с источником угрозы конфиденциальной информации?
4. Что является одним из самых важных разделов аналитической работы?
5. Что является первым этапом информационно-аналитической работы?
6. Что отражает частоту взаимодействия субъектов за определенный период времени?
7. Какие графики используются для регистрации событий?
8. Что представляют собой экспертные системы?
9. Что включает в себя обнаружение каналов НСД к конфиденциальной информации предприятия?
10. На каком этапе информационно-аналитической работы происходит выделение посторонней информации?

Тема 5. Организация конфиденциального делопроизводства

1. Что является угрозой внутренней ИТ?
2. На какие два типа делятся документы?
3. Перечислить сведения, которые составляют гос.тайну?
4. Сколько дается времени должностным лицам на оценку поступивших предложений?
5. Перечислить степени секретности информации?

6. Конфиденциальность информации-это?
7. Какая информация содержится в законе «О коммерческой тайне»?
8. Какая статья ГК определяет секрет производства (ноу-хау)?
9. Перечислить угрозы конфиденциальной информации?
10. ЭДО-это?

Тема 6. Организация работы с персоналом предприятия

1. В чём заключается сложность персонала как объекта защиты?
2. Под обеспечением безопасности деятельности предприятия понимается?
3. Какова цель кадровой политики?
4. Кто является источником получения конфиденциальной информации?
5. Какие определяются сложности в работе с персоналом?
6. Метод поиска кандидатов внутри компании позволяет?
7. Как проводятся плановые полиграфные проверки?
8. Как проводятся внеплановые полиграфные проверки?
9. Как проводятся целевые полиграфные проверки?
10. Что представляет собой обязательство о неразглашении конфиденциальных сведений представляет собой?

Тестирование

Тема 2. Организация внутриобъектного режима предприятия

1. Кому выдаются материальные пропуска?

1) выдаются лицам, ответственным за сохранность материальных средств

2) выдаются сотрудникам при поступлении на работу на основании приказа о зачислении в штат

3) выдаются лицам, работающим временно, или прикомандированным посетителям предприятия

2. ЧТО ОТНОСИТСЯ К СРЕДСТВАМ ФИЗИЧЕСКОЙ ЗАЩИТЫ? (выберете два варианта)

- 1) Ограждения и запирающие устройства
- 2) Антивирусное ПО
- 3) Пароль
- 4) Средства физической изоляции

3. КАКОВО ВРЕМЯ ДЕЙСТВИЯ РАЗОВОГО ПРОПУСКА?

- 1) 30 минут со времени выдачи до входа в здание
- 2) Действует до выхода из здания
- 3) 45 минут с момента выдачи до входа в здание
- 4) 60 минут с момента выдачи до входа в здание

4. КАКИЕ ИЗ ПЕРЕЧИСЛЕННЫХ ВИДОВ ПРОПУСКОВ СУЩЕСТВУЮТ

- 1) Постоянные, временные, разовые
- 2) одноразовые, двухразовые
- 3) оба варианта верно

5. КАКИЕ ИЗ ПЕРЕЧИСЛЕННЫХ ВИДОВ ОХРАНЫ СУЩЕСТВУЮТ?

- 1) Охрана с помощью технических средств

- 2) Комбинированная охрана
- 3) Оба варианта верно

Тема 5. Организация конфиденциального делопроизводства

1. ЧТО ОТНОСЯТ К ОБЩЕДОСТУПНОЙ ИНФОРМАЦИИ?

- 1) Относятся общеизвестные сведения и иная информация, доступ к которой не ограничен
- 2) Личные данные
- 3) Государственные тайны
- 4) Коммерческие тайны

2. ЧТО ИЗ ПЕРЕЧИСЛЕННОГО ОТНОСИТСЯ К ГОСУДАРСТВЕННОЙ ТАЙНЕ?

- 1) Военные сведения
- 2) Паспортные данные
- 3) Сведения в области экономики, науки и техники
- 4) Всё перечисленное

3. ВЫБЕРЕТЕ ВЕРНЫЕ ПРИЗНАКИ КОНФИДЕЦИАЛЬНОЙ ИНФОРМАЦИИ

- 1) Информация неизвестна третьим лицам
- 2) К ней нет свободного доступа на законном основании
- 3) К ней есть свободный доступ
- 4) Всё перечисленное неверно

4. ЧТО ОТНОСЯТ К ОСНОВНЫМ УГРОЗАМ КОНФИДЕЦИАЛЬНОЙ ИНФОРМАЦИИ?

- 1) Разглашение
- 2) Утечка
- 3) Оба варианта верны

5. ВЫБЕРЕТЕ ВЕРНЫЕ ВАРИАНТЫ О ТАКТИЧЕСКИХ ПРИЕМУЩЕСТВАХ СЭД

- 1) Освобождение офисных площадей
- 2) Возможность коллективной работы над документацией
- 3) Сохранность документов, удобство их применения
- 4) Снижение затрат на ресурсы

4.3 Промежуточная аттестация по дисциплине проводится в форме экзамена

Типовые вопросы экзамена (ОПК-5, ОПК-6)

1. Законодательные основы организационной защиты информации
2. Определение информационной безопасности, виды и источники угроз информационной безопасности.
3. Документы, регламентирующие организационную защиту информации
4. Организация охраны объектов предприятия, организация инженерно-технической защиты
5. Охрана объекта в условиях чрезвычайных ситуаций
6. Направления и методы информационно-аналитической работы
7. Конфиденциальная информация, угрозы конфиденциальной информации
8. Электронный документооборот, классификация систем электронного документооборота
9. Организация работы с персоналом предприятия. Подбор и подготовка кадров, методы добывания ценной информации у персонала
10. Технология подбора персонала для работы с конфиденциальными документами

Типовые задания для экзамена (ОПК-5, ОПК-6)

1. Внутриобъектный режим – это:
 - a) установленный на предприятии (организации) порядок выполнения правил внутреннего трудового распорядка, направленных на обеспечение комплексной безопасности, сохранения материальных средств и защиты конфиденциальной информации.;
 - b) это установленный на предприятии (организации) порядок выполнения правил внутреннего трудового распорядка;
 - c) сохранения материальных средств и защиты конфиденциальной информации;
2. Перечислите виды пропусков:
 - a) одноразовые и многоразовые
 - b) постоянные и непостоянные
 - c) **разовые, временные постоянные**
 - d) всё выше перечисленное
3. Кому выдаются материальные пропуска?
 - a) **выдаются лицам, ответственным за сохранность материальных средств**
 - b) выдаются сотрудникам при поступлении на работу на основании приказа о зачислении в штат
 - c) выдаются лицам, работающим временно, или прикомандированным
 - d) посетителям предприятия
4. В течении скольких минут действителен разовый пропуск ?
 - a) 15 минут
 - b) **30 минут;**
 - c) 90 минут
 - d) 120 минут
5. Физические средства защиты объектов можно разделить на:
 - a) **средства предупреждения, обнаружения и ликвидации угроз**
 - b) средства расследования компьютерных инцидентов
 - c) средства анализа межсетевого трафика и антивирусной защиты

4.4. Шкала оценивания промежуточной аттестации

Оценка	Компетенции	Дескрипторы (уровни) – основные признаки освоения (показатели достижения результата)
	ОПК-5	<p>Демонстрирует высокий уровень теоретических знаний основных нормативных правовых актов, нормативных и методических документов, регламентирующих деятельность по защите информации.</p> <p>Способен эффективно использовать нормативные правовые акты в профессиональной деятельности.</p> <p>Демонстрирует высокие навыки организации технологического процесса защиты информации в соответствии с правовыми нормативными актами и нормативными методическими документами.</p>

«отлично» (85 - 100 баллов)	ОПК-6	<p>Демонстрирует высокий уровень теоретических знаний основных нормативных правовых документов и актов, регламентирующих действия по организации защиты информации ограниченного доступа.</p> <p>Демонстрирует высокие навыки организации технологического процесса защиты информации в соответствии с правовыми нормативными актами и нормативными методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю.</p> <p>Способен продемонстрировать навыки организации обеспечения защиты информации.</p>
«хорошо» (70 - 84 баллов)	ОПК-5	<p>Демонстрирует достаточный уровень теоретических знаний основных нормативных правовых актов, нормативных и методических документов, регламентирующих деятельность по защите информации.</p> <p>Способен использовать нормативные правовые акты в профессиональной деятельности.</p> <p>Демонстрирует достаточные навыки организации технологического процесса защиты информации в соответствии с правовыми нормативными актами и нормативными методическими документами.</p>
	ОПК-6	<p>Демонстрирует достаточный уровень теоретических знаний основных нормативных правовых документов и актов, регламентирующих действия по организации защиты информации ограниченного доступа.</p> <p>Демонстрирует достаточные навыки организации технологического процесса защиты информации в соответствии с правовыми нормативными актами и нормативными методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю.</p> <p>Способен частично продемонстрировать навыки организации обеспечения защиты информации.</p>
«удовлетворительно» (50 - 69 баллов)	ОПК-5	<p>Демонстрирует низкий уровень теоретических знаний основных нормативных правовых актов, нормативных и методических документов, регламентирующих деятельность по защите информации.</p> <p>Демонстрирует низкие навыки организации технологического процесса защиты информации в соответствии с правовыми нормативными актами и нормативными методическими документами.</p>
	ОПК-6	<p>Демонстрирует низкий уровень теоретических знаний основных нормативных правовых документов и актов, регламентирующих действия по организации защиты информации ограниченного доступа.</p> <p>Демонстрирует низкие навыки организации технологического процесса защиты информации в соответствии с правовыми нормативными актами и нормативными методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю.</p>

«неудовлетворительно» (менее 50 баллов)	ОПК-5	Не имеет знаний об основных нормативных правовых документах и актах. Не ориентируется в необходимых нормативных правовых актах и информационно-правовых нормах в системе действующего законодательства.
	ОПК-6	Не имеет знаний основных нормативных правовых документов и актов, регламентирующих действия по организации защиты информации ограниченного доступа. Не способен продемонстрировать навыки организации технологического процесса защиты информации в соответствии с правовыми нормативными актами и нормативными методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю. Не способен продемонстрировать навыки организации обеспечения защиты информации.

5. Методические указания для обучающихся по освоению дисциплины (модуля)

5.1 Методические указания по организации самостоятельной работы обучающихся:

Приступая к изучению дисциплины, в первую очередь обучающимся необходимо ознакомиться содержанием рабочей программы дисциплины (РПД), которая определяет содержание, объем, а также порядок изучения и преподавания учебной дисциплины, ее раздела, части.

Для самостоятельной работы важное значение имеют разделы «Объем и содержание дисциплины», «Учебно-методическое и информационное обеспечение дисциплины» и «Материально-техническое обеспечение дисциплины, программное обеспечение, профессиональные базы данных и информационные справочные системы».

В разделе «Объем и содержание дисциплины» указываются все разделы и темы изучаемой дисциплины, а также виды занятий и планируемый объем в академических часах.

В разделе «Учебно-методическое и информационное обеспечение дисциплины» указана рекомендуемая основная и дополнительная литература.

В разделе «Материально-техническое обеспечение дисциплины, программное обеспечение, профессиональные базы данных и информационные справочные системы» содержится перечень профессиональных баз данных и информационных справочных систем, необходимых для освоения дисциплины.

5.2 Рекомендации обучающимся по работе с теоретическими материалами по дисциплине

При изучении и проработке теоретического материала необходимо:

- просмотреть еще раз презентацию лекции в системе MOODLe, повторить законспектированный на лекционном занятии материал и дополнить его с учетом рекомендованной дополнительной литературы;
- при самостоятельном изучении теоретической темы сделать конспект, используя рекомендованные в РПД источники, профессиональные базы данных и информационные справочные системы;
- ответить на вопросы для самостоятельной работы, по теме представленные в пункте 3.2 РПД.
- при подготовке к текущему контролю использовать материалы фонда оценочных средств (ФОС).

5.3 Рекомендации по работе с научной и учебной литературой

Работа с основной и дополнительной литературой является главной формой самостоятельной работы и необходима при подготовке к устному опросу на семинарских занятиях, к дебатам, тестированию, экзамену. Она включает проработку лекционного материала и рекомендованных источников и литературы по тематике лекций.

Конспект лекции должен содержать реферативную запись основных вопросов лекции, в том числе с опорой на размещенные в системе MOODLe презентации, основных источников и литературы по темам, выводы по каждому вопросу. Конспект может быть выполнен в рамках распечатки выдачи презентаций лекций или в отдельной тетради по предмету. Он должен быть аккуратным, хорошо читаемым, не содержать не относящуюся к теме информацию или рисунки.

Конспекты научной литературы при самостоятельной подготовке к занятиям должны содержать ответы на каждый поставленный в теме вопрос, иметь ссылку на источник информации с обязательным указанием автора, названия и года издания используемой научной литературы. Конспект может быть опорным (содержать лишь основные ключевые позиции), но при этом позволяющим дать полный ответ по вопросу, может быть подробным. Объем конспекта определяется самим студентом.

В процессе работы с основной и дополнительной литературой студент может:

- делать записи по ходу чтения в виде простого или развернутого плана (создавать перечень основных вопросов, рассмотренных в источнике);
- составлять тезисы (цитирование наиболее важных мест статьи или монографии, короткое изложение основных мыслей автора);
- готовить аннотации (краткое обобщение основных вопросов работы);
- создавать конспекты (развернутые тезисы).

5.4. Рекомендации по подготовке к отдельным заданиям текущего контроля

Собеседование предполагает организацию беседы преподавателя со студентами по вопросам практического занятия с целью более обстоятельного выявления их знаний по определенному разделу, теме, проблеме и т.п. Все члены группы могут участвовать в обсуждении, добавлять информацию, дискутировать, задавать вопросы и т.д.

Устный опрос может применяться в различных формах: фронтальный, индивидуальный, комбинированный. Основные качества устного ответа подлежащего оценке:

- правильность ответа по содержанию;
- полнота и глубина ответа;
- сознательность ответа;
- логика изложения материала;
- рациональность использованных приемов и способов решения поставленной учебной задачи;
- своевременность и эффективность использования наглядных пособий и технических средств при ответе;
- использование дополнительного материала;
- рациональность использования времени, отведенного на задание.

Устный опрос может сопровождаться презентацией, которая подготавливается по одному из вопросов практического занятия. При выступлении с презентацией необходимо обращать внимание на такие моменты как:

- содержание презентации: актуальность темы, полнота ее раскрытия, смысловое содержание, соответствие заявленной темы содержанию, соответствие методическим требованиям (цели, ссылки на ресурсы, соответствие содержания и литературы), практическая направленность, соответствие содержания заявленной форме, адекватность использования технических средств учебным задачам, последовательность и логичность презентуемого материала;
- оформление презентации: объем (оптимальное количество), дизайн (читаемость, наличие и соответствие графики и анимации, звуковое оформление, структурирование информации, соответствие заявленным требованиям), оригинальность оформления, эстетика, использование возможности программной среды, соответствие стандартам оформления;
- личностные качества: ораторские способности, соблюдение регламента, эмоциональность, умение ответить на вопросы, систематизированные, глубокие и полные знания по всем разделам программы;
- содержание выступления: логичность изложения материала, раскрытие темы, доступность изложения, эффективность применения средств ИКТ, способы и условия достижения результативности и эффективности для выполнения задач своей профессиональной или учебной деятельности, доказательность принимаемых решений, умение аргументировать свои заключения, выводы.

6. Учебно-методическое и информационное обеспечение дисциплины

6.1 Основная литература:

1. Тамб. гос. ун-т им. Г.Р. Державина Организационная защита информации : электронное учебное пособие. - [Тамбов]: [Б.и.], 2012. - 1 электрон. опт. диск (CD-ROM)
2. Аверченков, В. И., Рытов, М. Ю. Организационная защита информации : учебное пособие для вузов. - Весь срок охраны авторского права; Организационная защита информации. - Брянск: Брянский государственный технический университет, 2012. - 184 с. - Текст : электронный // IPR BOOKS [сайт]. - URL: <http://www.iprbookshop.ru/7002.html>
3. Аверченков, В. И., Рытов, М. Ю. Служба защиты информации. Организация и управление : учебное пособие для вузов. - Весь срок охраны авторского права; Служба защиты информации. Организация и управление. - Брянск: Брянский государственный технический университет, 2012. - 186 с. - Текст : электронный // IPR BOOKS [сайт]. - URL: <http://www.iprbookshop.ru/7008.html>
4. Кармановский, Н. С., Михайличенко, О. В., Прохожев, Н. Н. Организационно-правовое и методическое обеспечение информационной безопасности : учебное пособие. - 2022-10-01; Организационно-правовое и методическое обеспечение информационной безопасности. - Санкт-Петербург: Университет ИТМО, 2016. - 169 с. - Текст : электронный // IPR BOOKS [сайт]. - URL: <http://www.iprbookshop.ru/67452.html>

6.2 Дополнительная литература:

1. Загинайлов Ю. Н. Теория информационной безопасности и методология защиты информации : учебное пособие. - Москва|Берлин: Директ-Медиа, 2015. - 253 с. - Текст : электронный // ЭБС «Университетская библиотека онлайн» [сайт]. - URL: <http://biblioclub.ru/index.php?page=book&id=276557>
2. Лапина, М. А., Ревин, А. Г., Лапин, В. И. Информационное право : учебное пособие для студентов вузов, обучающихся по специальности 021100 «юриспруденция». - 2021-02-20; Информационное право. - Москва: ЮНИТИ-ДАНА, 2015. - 335 с. - Текст : электронный // IPR BOOKS [сайт]. - URL: <http://www.iprbookshop.ru/52038.html>
3. Корниенко С. А. Основы государственного регулирования использования радиочастотного спектра в Российской Федерации : учебное пособие. - Ставрополь: Северо-Кавказский Федеральный университет (СКФУ), 2016. - 154 с. - Текст : электронный // ЭБС «Университетская библиотека онлайн» [сайт]. - URL: <http://biblioclub.ru/index.php?page=book&id=459067>
4. Аверченков В. И., Ерохин В. В., Голембиовская О. М. История развития системы государственной безопасности России : учебное пособие. - 3-е изд., стер.. - Москва: Флинта, 2016. - 192 с. - Текст : электронный // ЭБС «Университетская библиотека онлайн» [сайт]. - URL: <http://biblioclub.ru/index.php?page=book&id=93267>
5. Аверченков В. И., Рытов М. Ю. Служба защиты информации: организация и управление : учебное пособие для вузов. - 3-е изд., стер.. - Москва: Флинта, 2016. - 186 с. - Текст : электронный // ЭБС «Университетская библиотека онлайн» [сайт]. - URL: <http://biblioclub.ru/index.php?page=book&id=93356>

6.3 Иные источники:

1. Федеральный закон от 27 июля 2006 г. N 152-ФЗ «О персональных данных.» -
2. Федеральный закон от 27 июля 2006 г. N 149-ФЗ «Об информации, информационных технологиях и о защите информации.» -
3. Закон Российской Федерации от 21 июля 1993 г. N 5485-1 «О государственной тайне.» -
4. Указ Президента Российской Федерации от 17 марта 2008 г. N 351 «О мерах по обеспечению информационной безопасности Российской Федерации при исполъз -
5. Указ Президента Российской Федерации от 30 ноября 1995 г. N 1203 «Об утверждении Перечня сведений, отнесенных к государственной тайне.» -
6. Указ Президента Российской Федерации от 6 марта 1997 г. N 188 «Об утверждении Перечня сведений конфиденциального характера.» -
7. Указ Президента РФ от 31 декабря 2015 г. N 683 "О Стратегии национальной безопасности Российской Федерации" -

8. Указ Президента РФ от 05 декабря 2016 г. N 646 "Об утверждении Доктрины информационной безопасности Российской Федерации" -

7. Материально-техническое обеспечение дисциплины, программное обеспечение, профессиональные базы данных и информационные справочные системы

Для проведения занятий по дисциплине необходимо следующее материально-техническое обеспечение: учебные аудитории для проведения занятий лекционного и семинарского типа, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации, помещения для самостоятельной работы.

Учебные аудитории и помещения для самостоятельной работы укомплектованы специализированной мебелью и техническими средствами обучения, служащими для представления учебной информации большой аудитории.

Помещения для самостоятельной работы укомплектованы компьютерной техникой с возможностью подключения к сети "Интернет" и обеспечением доступа в электронную информационно-образовательную среду Университета.

Для проведения занятий лекционного типа используются наборы демонстрационного оборудования, обеспечивающие тематические иллюстрации (проектор, ноутбук, экран/ интерактивная доска).

Лицензионное и свободно распространяемое программное обеспечение:

Kaspersky Endpoint Security для бизнеса - Стандартный Russian Edition. 1500-2499 Node 1 year Educational Renewal Licence

Операционная система Microsoft Windows 10

Adobe Reader XI (11.0.08) - Russian Adobe Systems Incorporated 10.11.2014 187,00 MB 11.0.08

7-Zip 9.20

Microsoft Office Профессиональный плюс 2007

Профессиональные базы данных и информационные справочные системы:

1. Электронный каталог Фундаментальной библиотеки ТГУ. – URL: <http://biblio.tsutmb.ru/elektronnyij-katalog>
2. Университетская библиотека онлайн: электронно-библиотечная система. – URL: <https://biblioclub.ru>
3. Консультант студента. Гуманитарные науки: электронно-библиотечная система. – URL: <https://www.studentlibrary.ru>
4. Научная электронная библиотека eLIBRARY.ru. – URL: <https://elibrary.ru>
5. Российская национальная библиотека. – URL: <http://nlr.ru>
6. Российская государственная библиотека. – URL: <https://www.rsl.ru>
7. Президентская библиотека имени Б.Н. Ельцина. – URL: <https://www.prilib.ru>
8. Научная электронная библиотека Российской академии естествознания. – URL: <https://www.monographies.ru>
9. Электронная библиотека РФФИ. – URL: <https://www.rfbr.ru/rffi/ru/library>

Электронная информационно-образовательная среда

https://auth.tsutmb.ru/authorize?response_type=code&client_id=moodle&state=xyz

Взаимодействие преподавателя и студента в процессе обучения осуществляется посредством мультимедийных, гипертекстовых, сетевых, телекоммуникационных технологий, используемых в электронной информационно-образовательной среде университета.