

Документ подписан простой электронной подписью

Информация о владельце:

ФИО: Таныгин Максим Олегович

Должность: и.о. декана факультета фундаментальной информатики и информатических технологий

Дата подписания: 06.10.2022 10:25:54

Уникальный программный идентификатор:

65ab2aa0d384efe8480e6a4c688eddbc475e411a

## **Аннотация к рабочей программе**

### **дисциплины «Организация и управление службой защиты информации»**

#### **Цель преподавания дисциплины**

Целью преподавания дисциплины «Организация и управление службой защиты информации» является изучение структуры, логической организации и системы управления службой защиты информации как основного звена систем защиты информации.

#### **Задачи изучения дисциплины**

Основными обобщенными задачами дисциплины являются:

- определение места службы защиты информации в системе безопасности предприятия; объяснение функций службы защиты информации;
- обоснование оптимальной структуры и штатного состава службы защиты информации в зависимости от решаемых задач и выполняемых функций;
- установление организационных основ и принципов деятельности службы защиты информации;
- разрешение общих и специфических вопросов подбора, расстановки и обучения кадров, организации труда сотрудников службы защиты информации; раскрытие принципов, методов и технологии управления службой защиты информации

#### **Компетенции, формируемые в результате освоения дисциплины**

Способен организовать работы по выполнению требований защиты информации ограниченного доступа в телекоммуникационных системах и сетях (ПК-8).

#### **Разделы дисциплины**

Структура службы информационной безопасности. Функции основных групп службы безопасности. Цели и задачи службы информационной безопасности.

Организационные основы и принципы деятельности службы информационной безопасности. Лицензирование видов деятельности службы безопасности. Управление службой защиты информации. Организация информационно-аналитической работы. Организация работы с персоналом предприятия.

МИНОБРНАУКИ РОССИИ  
Юго-Западный государственный университет

УТВЕРЖДАЮ:

Декан факультета

фундаментальной и прикладной

*(наименование ф-та полностью)*

информатики



М.О. Таныгин

*(подпись, инициалы, фамилия)*

« 31 » 08 2021 г

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Организация и управление службой защиты информации

*(наименование дисциплины)*

ОПОП ВО

10.05.02 Информационная безопасность

*шифр и наименование направление подготовки (специальности)*

телекоммуникационных систем

Управление безопасностью телекоммуникационных систем и сетей

*наименование направленности (профиля, специализации)*

Рабочая программа дисциплины составлена в соответствии с ФГОС ВО – специалитет по специальности 10.05.02 Информационная безопасность телекоммуникационных систем на основании учебного плана ОПОП ВО 10.04.01 Информационная безопасность, специализация «Управление безопасностью телекоммуникационных систем и сетей», одобренного Ученым советом университета (протокол №6 «20» 02 20 21 г.).


Рабочая программа дисциплины обсуждена и рекомендована к реализации в образовательном процессе для обучения студентов по ОПОП ВО 10.05.02 Информационная безопасность телекоммуникационных систем на основании учебного плана ОПОП ВО 10.05.02 Информационная безопасность телекоммуникационных систем, специализация «Управление безопасностью телекоммуникационных систем и сетей» на заседании кафедры информационной безопасности №1 «30» 08 20 21 г.

Зав. кафедрой \_\_\_\_\_  Таныгин М.О.

Разработчик программы  
к.т.н., доцент \_\_\_\_\_  Таныгин М.О.  
(ученая степень и ученое звание, Ф.И.О.)

/Директор научной библиотеки \_\_\_\_\_  Макаровская В.Г.

Рабочая программа дисциплины пересмотрена, обсуждена и рекомендована к реализации в образовательном процессе на основании учебного плана ОПОП ВО 10.05.02 Информационная безопасность телекоммуникационных систем на основании учебного плана ОПОП ВО 10.04.01 Информационная безопасность, специализация «Управление безопасностью телекоммуникационных систем и сетей», одобренного Ученым советом университета протокол № 6 «26» 02 20 21 г., на заседании кафедры ИБ, протокол №1 от 30.06.2022 г. .  
(наименование кафедры, дата, номер протокола)

Зав. кафедрой М.В. Лавкина 

Рабочая программа дисциплины пересмотрена, обсуждена и рекомендована к реализации в образовательном процессе на основании учебного плана ОПОП ВО 10.05.02 Информационная безопасность телекоммуникационных систем на основании учебного плана ОПОП ВО 10.04.01 Информационная безопасность, специализация «Управление безопасностью телекоммуникационных систем и сетей», одобренного Ученым советом университета протокол №\_\_ «\_\_» 20\_\_ г., на заседании кафедры \_\_\_\_\_ .  
(наименование кафедры, дата, номер протокола)

Зав. кафедрой \_\_\_\_\_

## 1. Цель и задачи дисциплины. Перечень планируемых результатов обучения по дисциплине, соотнесенных с планируемыми результатами освоения основной профессиональной образовательной программы

### 1.1. Цель дисциплины

Целью преподавания дисциплины «Организация и управление службой защиты информации» является изучение структуры, логической организации и системы управления службой защиты информации как основного звена систем защиты информации.

### 1.2. Задачи дисциплины

Основными обобщенными задачами дисциплины являются:

- определение места службы защиты информации в системе безопасности предприятия; объяснение функций службы защиты информации;
- обоснование оптимальной структуры и штатного состава службы защиты информации в зависимости от решаемых задач и выполняемых функций;
- установление организационных основ и принципов деятельности службы защиты информации;
- разрешение общих и специфических вопросов подбора, расстановки и обучения кадров, организации труда сотрудников службы защиты информации; раскрытие принципов, методов и технологии управления службой защиты информации

### 1.3 Перечень планируемых результатов обучения по дисциплине, соотнесенных с планируемыми результатами освоения основной профессиональной образовательной программы

<i>Планируемые результаты освоения основной профессиональной образовательной программы (компетенции, закрепленные за практикой)</i>		<i>Код и наименование индикатора достижения компетенции, закрепленного за практикой</i>	<i>Планируемые результаты обучения по практике, соотнесенные с индикаторами достижения компетенций</i>
<i>код компетенции</i>	<i>наименование компетенции</i>		
ПК-8	Способен организовать работы по выполнению требований защиты информации ограниченного доступа в телекоммуникационных системах и сетях	ПК-8.1 Управляет работой специалистов по созданию и эксплуатации средств защиты информации в телекоммуникационных системах и сетях	<b>Знать:</b> порядок действий специалистов по созданию и эксплуатации средств защиты информации в телекоммуникационных системах и сетях <b>Уметь:</b> ставить задачи отдельным исполнителям при создании и

<i>Планируемые результаты освоения основной профессиональной образовательной программы (компетенции, закрепленные за практикой)</i>		<i>Код и наименование индикатора достижения компетенции, закрепленного за практикой</i>	<i>Планируемые результаты обучения по практике, соотнесенные с индикаторами достижения компетенций</i>
<i>код компетенции</i>	<i>наименование компетенции</i>		
			эксплуатации средств защиты информации в телекоммуникационных системах и сетях <b>Владеть (или Иметь опыт деятельности):</b> созданию и эксплуатации средств защиты информации в телекоммуникационных системах и сетях
		ПК-8.2 Формирует комплекс мер (принципов, правил, процедур, практических приемов, методов, средств) для защиты в телекоммуникационных системах и сетях информации ограниченного доступа	<b>Знать:</b> перечень угроз, на нейтрализацию которых направлена та или иная мера по защите информации <b>Уметь:</b> объединять отдельные мероприятия по обеспечению информационной безопасности в логически структурированные последовательности <b>Владеть (или Иметь опыт деятельности):</b> использования отдельных технологий обеспечения информационной безопасности в ТКС
		ПК-8.3 Управляет процессом разработки моделей угроз и моделей нарушителя безопасности компьютерных систем	<b>Знать:</b> административный регламент проведения работ по обеспечению информационной безопасности <b>Уметь:</b> принимать управленческие решения при проведении работ по обеспечению информационной безопасности <b>Владеть (или Иметь опыт деятельности):</b>

<i>Планируемые результаты освоения основной профессиональной образовательной программы (компетенции, закрепленные за практикой)</i>		<i>Код и наименование индикатора достижения компетенции, закрепленного за практикой</i>	<i>Планируемые результаты обучения по практике, соотнесенные с индикаторами достижения компетенций</i>
<i>код компетенции</i>	<i>наименование компетенции</i>		разработки моделей угроз и моделей нарушителя безопасности компьютерных систем
		ПК-8.4 Разрабатывает организационно-распорядительные документы, регламентирующие порядок эксплуатации телекоммуникационных систем и сетей	<b>Знать:</b> основные этапы жизненного цикла ТКС и регламентные мероприятия на каждом из них <b>Уметь:</b> выполнять отдельных действий по обеспечению информационной безопасности телекоммуникационных систем <b>Владеть (или Иметь опыт деятельности):</b> систематизации отдельных действий по обеспечению информационной безопасности телекоммуникационных систем
		ПК 8.5 Определяет действия сотрудников при проведении мероприятий по информационной безопасности	<b>Знать:</b> правовые нормы действующего законодательства, регулирующие отношения в различных сферах жизнедеятельности; <b>Уметь:</b> определять направления актуализации системы защиты информации в соответствии с текущими деловыми потребностями фирмы и выявленным уровнем уязвимости защищаемой информации; <b>Владеть (или Иметь опыт деятельности):</b>

<i>Планируемые результаты освоения основной профессиональной образовательной программы (компетенции, закрепленные за практикой)</i>		<i>Код и наименование индикатора достижения компетенции, закрепленного за практикой</i>	<i>Планируемые результаты обучения по практике, соотнесенные с индикаторами достижения компетенций</i>
<i>код компетенции</i>	<i>наименование компетенции</i>		
			применения нормативных правовых документов в своей деятельности; - навыками работы с информацией из различных источников;

## **2. Указание места дисциплины в структуре основной профессиональной образовательной программы**

Дисциплина «Организация и управление службой защиты информации» является элективной дисциплиной, входит в часть, формируемую участниками образовательных отношений, основной профессиональной образовательной программы – программы бакалавриата (специалитета, магистратуры) 10.03.01 Информационная безопасность направленность (профиль) «Безопасность автоматизированных систем (по отрасли или в сфере профессиональной деятельности)». Дисциплина изучается на 3 курсе в 6 семестре.

## **3 Объем дисциплины в зачетных единицах с указанием количества академических или астрономических часов, выделенных на контактную работу обучающихся с преподавателем (по видам учебных занятий) и на самостоятельную работу обучающихся**

Общая трудоемкость (объем) дисциплины составляет 3 зачетные единицы (з.е.), 108 академических часов.

Таблица 3.1 – Объем дисциплины

Виды учебной работы	Всего, часов
Общая трудоемкость дисциплины	108
Контактная работа обучающихся с преподавателем по видам учебных занятий (всего)	56,1
в том числе:	
лекции	28
лабораторные занятия	0



Виды учебной работы	Всего, часов
практические занятия	28, из них практическая подготовка – 4
Самостоятельная работа обучающихся (всего)	51,9
Контроль (подготовка к экзамену)	0
Контактная работа по промежуточной аттестации (всего АттКР)	0,1
в том числе:	
зачет	0,1
зачет с оценкой	не предусмотрен
курсовая работа (проект)	не предусмотрена
экзамен (включая консультацию перед экзаменом)	не предусмотрен

#### **4 Содержание дисциплины, структурированное по темам (разделам) с указанием отведенного на них количества академических часов и видов учебных занятий**

##### **4.1 Содержание дисциплины**

Таблица 4.1 – Содержание дисциплины, структурированное по темам (разделам)

№ п/п	Раздел (тема) дисциплины	Содержание
1	2	3
1.	Структура службы информационной безопасности	Общая структурная схема службы защиты информации. Основные направления деятельности СУИБ
2.	Функции основных групп службы безопасности	Группа режима. Группа охраны и сопровождения. Техническая группа. Детективная группа. Должностные обязанности Минимальный штатный состав СБ и обязанности сотрудников
3.	Цели и задачи службы информационной безопасности	Цели обеспечения безопасности предприятия. Задачи службы Функции СИБ
4.	Организационные основы и принципы деятельности службы информационной безопасности	Организация деятельности службы безопасности Правовое обеспечение службы. Принципы организации службы. Гарантии безопасности объектов защиты Пакет документов для СИБ
5.	Лицензирование видов деятельности службы безопасности.	Лицензирование видов деятельности службы безопасности предприятия

6.	Управление службой защиты информации.	Методы управления СБП Функции процессов управления Функции процессов управления Методы управления Принципы управления СБП. Виды обеспечения деятельности СБП. Управление безопасностью предприятия в кризисных ситуациях
7.	Организация информационно-аналитической работы.	Цели и задачи информационно-аналитической работы. Направления и методы аналитической работы Этапы выполнения информационно-аналитических исследований производственных ситуаций. Методы выполнения аналитических исследований
8.	Организация работы с персоналом предприятия.	Подбор и подготовка кадров. Проверка персонала на благонадежность. Заключение контрактов и соглашений о секретности. Особенности увольнения сотрудников, владеющих конфиденциальной информацией

Таблица 4.1.2 – Содержание дисциплины и его методическое обеспечение

№ п/п	Раздел (тема) дисциплины	Виды деятельности			Учебно-методические материалы	Формы текущего контроля успеваемости (по неделям семестра)	Компетенции
		лек. , час	№ лаб .	№ пр.			
1	2	3	4	5	6	7	8
1.	Структура службы информационной безопасности	3			У-1 МУ-4	С	ОК-4, ОПК-5, ПК-10, ПК-15
2.	Функции основных групп службы безопасности	3			У-1,2, МУ-4	С	ПК-10, ПК-15
3.	Цели и задачи службы информационной безопасности	4	1		У-1,3 МУ-1,4	С,Т	ПК-8, ПК-10,
4.	Организационные основы и принципы деятельности службы информационной безопасности	4			У-1,4 МУ-4	С, Т	ОК-4, ОПК-5, ПК-8, ПК-15
5.	Лицензирование видов деятельности службы безопасности.	4	2		У-2,3 МУ-2,4	С	ОК-4, ОПК-5, ПК-8, ПК-10, ПК-15
6.	Управление службой защиты информации.	4	3		У-1,2,3 МУ-3,4	С	ОК-4, ОПК-5, ПК-8, ПК-10, ПК-15
7.	Организация информационно-аналитической	4			У-2-6, МУ-4	С	ОК-4, ОПК-5, ПК-15

	работы.					
8.	Организация работы персоналом предприятия.	с	4		У-1,3,4, МУ-4	С ОК-4, ОПК-5,

С – собеседование, Т- тестирование.

## 4.2 Лабораторные работы и (или) практические занятия

### 4.2.1 Практические работы

Таблица 4.2.1 – Практические работы

№	Наименование практической работы	Объем, час.
1.	Анализ заданного нормативно-правового акта Российской Федерации	9
2.	Работа с нормативно-правовыми документами	9, из них практическая подготовка – 2
3.	Система анализа рисков и проверки политики информационной безопасности предприятия	10, из них практическая подготовка – 2
Итого		32

## 4.3 Самостоятельная работа студентов (СРС)

Таблица 4.3 – Самостоятельная работа студентов

№	Наименование раздела учебной дисциплины	Срок выполнения	Время, затрачиваемое на выполнение СРС, час.
1.	Структура службы информационной безопасности	1-2 неделя	7
2.	Функции основных групп службы безопасности	3-4 неделя	7
3.	Цели и задачи службы информационной безопасности	5-6 неделя	7
4.	Организационные основы и принципы деятельности службы информационной безопасности	7-8 неделя	7
5.	Лицензирование видов деятельности службы безопасности.	9-10 неделя	7
6.	Управление службой защиты информации.	11 неделя	5,9
7.	Организация информационно-аналитической работы.	12-13 неделя	6
8.	Организация работы с персоналом предприятия.	14 неделя	5
Итого			51,9

## 5 Перечень учебно-методического обеспечения для самостоятельной работы обучающихся по дисциплине

Студенты могут при самостоятельном изучении отдельных тем и вопросов дисциплин пользоваться учебно-наглядными пособиями, учебным оборудованием и методическими разработками кафедры в рабочее время, установленное Правилами внутреннего распорядка работников.

Учебно-методическое обеспечение для самостоятельной работы обучающихся по данной дисциплине организуется:

библиотекой университета:

- библиотечный фонд укомплектован учебной, методической, научной, периодической, справочной и художественной литературой в соответствии с УП и данной РПД;

- имеется доступ к основным информационным образовательным ресурсам, информационной базе данных, в том числе библиографической, возможность выхода в Интернет.

кафедрой:

- путем обеспечения доступности всего необходимого учебно-методического и справочного материала;

- путем предоставления сведений о наличии учебно-методической литературы, современных программных средств;

- путем разработки:

- методических рекомендаций, пособий по организации самостоятельной работы студентов;

- тем рефератов;

- вопросов к зачету;

- методических указаний к выполнению лабораторных работ и т.д.

типографией университета:

- помощь авторам в подготовке и издании научной, учебной и методической литературы;

- удовлетворение потребности в тиражировании научной, учебной и методической литературы.

## **6 Образовательные технологии. Практическая подготовка обучающихся. Технологии использования воспитательного потенциала дисциплины**

### **Образовательные технологии**

Реализация компетентного подхода предусматривает широкое использование в образовательном процессе активных и интерактивных форм проведения занятий в сочетании с внеаудиторной работой с целью формирования универсальных, общепрофессиональных и профессиональных компетенций обучающихся. В рамках дисциплины предусмотрены встречи с экспертами и специалистами Комитета по труду и занятости населения Курской области.

Таблица 6.1 – Интерактивные образовательные технологии, используемые при проведении аудиторных занятий

№	Наименование раздела (темы лекции, практического или лабораторного занятия)	Используемые интерактивные образовательные технологии	Объем, час.
1.	Выполнение практической работы №1 «Анализ заданного нормативно-правового акта Российской Федерации».	Разбор конкретных ситуаций	4
2.	Выполнение практической работы №2 «Работа с нормативно-правовыми документами».	Разбор конкретных ситуаций	4
3.	Выполнение практической работы №3 «Система анализа рисков и проверки политики информационной безопасности предприятия»	Разбор конкретных ситуаций	4
	Итого		12

### **Практическая подготовка обучающихся**

Практическая подготовка обучающихся при реализации дисциплины осуществляется путем проведения практических занятий, предусматривающих участие обучающихся в выполнении отдельных элементов работ, связанных с будущей профессиональной деятельностью и направленных на формирование, закрепление, развитие практических навыков и компетенций по направленности (профилю) программы бакалавриата. Практическая подготовка включает в себя отдельные практические занятия, которые проводятся как в помещениях университета, так и в профильных организациях и предусматривают передачу учебной информации обучающимся, необходимой для последующего выполнения работ, связанных с будущей профессиональной деятельностью.

Практическая подготовка обучающихся при реализации дисциплины организуется в модельных условиях (оборудованных (полностью или частично) в подразделениях университета.

Практическая подготовка обучающихся проводится в соответствии с положением П 02.181.

### **Технологии использования воспитательного потенциала дисциплины**

Содержание дисциплины обладает значительным воспитательным потенциалом, поскольку в нем аккумулирован исторический и современный социокультурный опыт человечества. Реализация воспитательного потенциала дисциплины осуществляется в рамках единого образовательного и воспитательного процесса и способствует непрерывному развитию личности каждого обучающегося. Дисциплина вносит значимый вклад в формирование общей и профессиональной культуры обучающихся.

Содержание дисциплины способствует гражданскому, правовому, экономическому, профессионально-трудовому воспитанию обучающихся.

Реализация воспитательного потенциала дисциплины подразумевает:

– целенаправленный отбор преподавателем и включение в лекционный материал, материал для практических занятий содержания, демонстрирующего обучающимся образцы настоящего научного подвижничества создателей и представителей данной отрасли науки (производства, экономики, культуры), высокого профессионализма ученых (представителей производства, деятелей культуры), их ответственности за результаты и последствия деятельности для природы, человека и общества; примеры подлинной нравственности людей, причастных к развитию науки, культуры, экономики и производства;

– применение технологий, форм и методов преподавания дисциплины, имеющих высокий воспитательный эффект за счет создания условий для взаимодействия обучающихся с преподавателем, другими обучающимися, (командная работа, деловые игры, разбор конкретных ситуаций);

– личный пример преподавателя, демонстрацию им в образовательной деятельности и общении с обучающимися за рамками образовательного процесса высокой общей и профессиональной культуры.

Реализация воспитательного потенциала дисциплины на учебных занятиях направлена на поддержание в университете единой развивающей образовательной и воспитательной среды. Реализация воспитательного потенциала дисциплины в ходе самостоятельной работы обучающихся способствует развитию в них целеустремленности, инициативности, креативности, ответственности за результаты своей работы – качеств, необходимых для успешной социализации и профессионального становления.

## **7 Фонд оценочных средств для проведения промежуточной аттестации обучающихся по дисциплине**

### **7.1 Перечень компетенций с указанием этапов их формирования в процессе освоения основной профессиональной образовательной программы**

Таблица 7.1 – Этапы формирования компетенций

Код и наименование компетенции	Этапы* формирования компетенций и дисциплины (модули) и практики, при изучении/ прохождении которых формируется данная компетенция		
	начальный	основной	завершающий
1	2	3	4
ПК-8 Способен организовать работы по выполнению требований защиты информации ограниченного доступа в телекоммуникационных	Организация и управление службой защиты информации Система сертификации и	Порядок проведения аттестации объектов информатизации	Производственная преддипломная практика

системах и сетях	лицензирования деятельности по защите информации		
------------------	--	--	--

## 7.2 Описание показателей и критериев оценивания компетенций на различных этапах их формирования, описание шкал оценивания

Таблица 7.2 – Показатели и критерии оценивания компетенций, шкала оценивания

Код компетенции/ этап (указывается название этапа из п.6.1)	Показатель и оценивания компетенций (индикаторы достижения компетенций, закрепленные за практикой)	Критерии и шкала оценивания компетенций		
		Пороговый уровень («удовлетворительно»)	Продвинутый уровень («хорошо»)	Высокий уровень («отлично»)
1	2	3	4	5
ПК-8/ завершающий	ПК-8.1 Управляет работой специалистов по созданию и эксплуатации средств защиты информации в телекоммуникационных системах и сетях	<b>Знать:</b> порядок действий специалистов по эксплуатации средств защиты информации в телекоммуникационных системах и сетях <b>Уметь:</b> ставить задачи отдельным исполнителям и эксплуатации средств защиты информации в телекоммуникационных системах и сетях <b>Владеть (или Иметь опыт деятельности):</b> эксплуатации средств защиты	<b>Знать:</b> порядок действий специалистов по созданию и эксплуатации средств защиты информации в телекоммуникационных системах и сетях <b>Уметь:</b> ставить задачи отдельным исполнителям при создании и эксплуатации средств защиты информации в телекоммуникационных системах и сетях <b>Владеть (или Иметь опыт деятельности):</b>	<b>Знать:</b> методику определения порядка действий специалистов по созданию и эксплуатации средств защиты информации в телекоммуникационных системах и сетях <b>Уметь:</b> ставить задачи всем исполнителям при создании и эксплуатации средств защиты информации в телекоммуникационных системах и сетях <b>Владеть (или Иметь опыт</b>

1	2	3	4	5
		информации в телекоммуникационных системах и сетях	созданию и эксплуатации средств защиты информации в телекоммуникационных системах и сетях	<b>деятельности):</b> создания и эксплуатации сложных средств защиты информации в телекоммуникационных системах и сетях
	ПК-8.2 Формирует комплекс мер (принципов, правил, процедур, практических приемов, методов, средств) для защиты в телекоммуникационных системах и сетях информации и ограниченного доступа	<b>Знать:</b> перечень угроз, на нейтрализацию которых направлены отдельные меры по защите информации <b>Уметь:</b> проводить отдельные мероприятия по обеспечению информационной безопасности в логически структурированные последовательности и <b>Владеть (или Иметь опыт деятельности):</b> использования отдельных технологий обеспечения информационной безопасности в ТКС	<b>Знать:</b> перечень угроз, на нейтрализацию которых направлена та или иная мера по защите информации <b>Уметь:</b> последовательно проводить отдельные мероприятия по обеспечению информационной безопасности в логически структурированные последовательности и <b>Владеть (или Иметь опыт деятельности):</b> использования типовых технологий обеспечения информационной безопасности в ТКС	<b>Знать:</b> методики определения угроз, на нейтрализацию которых направлена та или иная мера по защите информации <b>Уметь:</b> объединять отдельные мероприятия по обеспечению информационной безопасности в логически структурированные последовательности и <b>Владеть (или Иметь опыт деятельности):</b> использования разнообразных технологий обеспечения информационной безопасности в ТКС
	ПК-8.3 Управляет процессом разработки моделей угроз и моделей нарушителя безопасности и компьютерных систем	<b>Знать:</b> административный регламент проведения работ по обеспечению информационной безопасности <b>Уметь:</b> при поддержке принимать управленческие решения при проведении работ	<b>Знать:</b> административный регламент проведения работ по обеспечению информационной безопасности <b>Уметь:</b> принимать управленческие решения при проведении работ по обеспечению информационной	<b>Знать:</b> правила и административный регламент проведения работ по обеспечению информационной безопасности <b>Уметь:</b> принимать и обосновывать управленческие решения при проведении работ по обеспечению



1	2	3	4	5
		по обеспечению информационной безопасности <b>Владеть</b> (или <b>Иметь опыт деятельности</b> ): разработки элементов моделей угроз и моделей нарушителя безопасности компьютерных систем	безопасности <b>Владеть</b> (или <b>Иметь опыт деятельности</b> ): разработки моделей угроз и моделей нарушителя безопасности для типовых компьютерных систем	информационной безопасности <b>Владеть</b> (или <b>Иметь опыт деятельности</b> ): разработки оригинальных моделей угроз и моделей нарушителя безопасности компьютерных систем
	ПК-8.4 Разрабатывает организационно-распорядительные документы, регламентирующие порядок эксплуатации и телекоммуникационных систем и сетей	<b>Знать:</b> номенклатуру этапов жизненного цикла ТКС и регламентные мероприятия на каждом из них <b>Уметь:</b> выполнять отдельные действия по обеспечению информационной безопасности телекоммуникационных систем <b>Владеть</b> (или <b>Иметь опыт деятельности</b> ): систематизации отдельных действий по обеспечению информационной безопасности телекоммуникационных систем	<b>Знать:</b> основные этапы жизненного цикла ТКС и регламентные мероприятия на каждом из них <b>Уметь:</b> выполнять небольшие последовательность и отдельных действий по обеспечению информационной безопасности телекоммуникационных систем <b>Владеть</b> (или <b>Иметь опыт деятельности</b> ): систематизации последовательность и действий по обеспечению информационной безопасности телекоммуникационных систем	<b>Знать:</b> все возможные этапы жизненного цикла ТКС и регламентные мероприятия на каждом из них <b>Уметь:</b> выполнять связанные последовательность и действий по обеспечению информационной безопасности телекоммуникационных систем <b>Владеть</b> (или <b>Иметь опыт деятельности</b> ): систематизации сложных последовательностей действий по обеспечению информационной безопасности телекоммуникационных систем
	ПК 8.5 Определяет действия сотрудников в при проведении мероприятий по информационной безопасности	<b>Знать:</b> Организацию судебных, правоприменительных и правоохранительных органов <b>Уметь:</b> определять перечень действий для проведения анализа ИБ	<b>Знать:</b> правовые нормы действующего законодательства, регулирующие отношения в различных сферах жизнедеятельности. <b>Уметь:</b> работать с нормативными документами	<b>Знать:</b> основные положения и нормы конституционного, гражданского, семейного, трудового, административного и уголовного права. <b>Уметь:</b> определять актуальные

1	2	3	4	5
	и	<b>Владеть (или Иметь опыт деятельности):</b> Навыками работы с нормативно-правовыми документами	регуляторов в области информационной безопасности <b>Владеть (или Иметь опыт деятельности):</b> работой с методической литературой и выработать управленческие решения в области информационной безопасности;	вопросы защиты информации в соответствии с уровнем уязвимости <b>Владеть (или Иметь опыт деятельности):</b> Навыками применения нормативных правовых документов в конкретных практических ситуациях

**7.3 Типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций в процессе освоения основной профессиональной образовательной программы**

Таблица 7.3 – Паспорт комплекта оценочных средств для текущего контроля успеваемости

№ п/п	Раздел (тема) дисциплины	Код контролируемой компетенции (или её части)	Технология форматирования	Оценочные средства		Описание шкал оценивания
				наименование	№ заданий	
1	2	3	4	5	6	7
1	Структура службы информационной безопасности	ПК-8	Лекция, СРС	Собеседование	1-4	Согласно табл. 7.2
2	Функции основных групп службы безопасности	ПК-8	Лекция, СРС,	Собеседование	1-8	Согласно табл. 7.2
3	Цели и задачи службы информационной безопасности	ПК-8	Лекция, СРС, практическая работа	Собеседование, тест	1-3	Согласно табл. 7.2
				Контрольные вопросы к ПР №1		
				Производственные задачи к занятию 1		

4	Организационные основы и принципы деятельности службы информационной безопасности	ПК-8	Лекция, СРС, практическая работа	Собеседование	1-7	Согласно табл. 7.2
				Тест	1-7	
5	Лицензирование видов деятельности службы безопасности	ПК-8	Лекция, СРС	Собеседование		Согласно табл. 7.2
				Контрольные вопросы к ПР №2		
				Производственные задачи к занятию 2		
6	Управление службой защиты информации.	ПК-8	Лекция, СРС, практическая работа	Собеседование	1-9	Согласно табл. 7.2
				Контрольные вопросы к практической №3		
7	Организация информационно-аналитической работы.	ПК-8	Лекция, СРС	Собеседование	1-7	Согласно табл. 7.2
8	Организация работы с персоналом предприятия.	ПК-8	Лекция, СРС	Собеседование	1-8	Согласно табл. 7.2

### Примеры типовых контрольных заданий для проведения текущего контроля успеваемости

#### Вопросы для собеседования

Тема 7. Организация информационно-аналитической работы.

1. Цели и задачи информационно-аналитической работы
2. Задачи, возникающие при выполнении информационно-аналитической работы
3. Направления и методы аналитической работы
4. Что включает в себя такое направление, как обнаружение каналов несанкционированного доступа к информации?

#### Тесты для текущего контроля знаний

Тема 4. Организационные основы и принципы деятельности службы информационной безопасности.

1. Следующее структурное подразделение службы защиты информации отвечает за контакты с правоохранительными органами по всем вопросам обеспечения безопасности деятельности объекта

- Группа режима
- Группа охраны и сопровождения
- Техническая группа
- Детективная группа

2. В обязанности какого сотрудника входит разработка и поддержка эффективных мер защиты по обработке информации для обеспечения сохранности данных
  - Сотрудник группы безопасности
  - Администратор безопасности системы
  - Администратор безопасности данных
  - Руководитель группы
3. В обязанности какого сотрудника входит контроль за выполнением плана восстановления после инцидента информационной безопасности
  - Сотрудник группы безопасности
  - Администратор безопасности системы
  - Администратор безопасности данных
  - Руководитель группы

Производственная задача для контроля результатов практической подготовки обучающихся на практическом занятии №1

Разработайте инструкцию по работе с персональными данными в административном подразделении образовательной организации.

Производственная задача для контроля результатов практической подготовки обучающихся на практическом занятии № 2

Разработайте план работ по проведению мероприятий по организационной защите информации в переговорной комнате предприятия.

#### Типовые задания для проведения промежуточной аттестации обучающихся

Промежуточная аттестация по дисциплине проводится в форме зачета. Зачет проводится в виде компьютерного тестирования.

Для тестирования используются контрольно-измерительные материалы (КИМ) – вопросы и задания в тестовой форме, составляющие банк тестовых заданий (БТЗ) по дисциплине, утвержденный в установленном в университете порядке.

Проверяемыми на промежуточной аттестации элементами содержания являются темы дисциплины, указанные в разделе 4 настоящей программы. Все темы дисциплины отражены в КИМ в равных долях (%). БТЗ включает в себя не менее 100 заданий и постоянно пополняется. БТЗ хранится на бумажном носителе в составе УММ и электронном виде в ЭИОС университета.

Для проверки знаний используются вопросы и задания в различных формах:

- закрытой (с выбором одного или нескольких правильных ответов),
- открытой (необходимо вписать правильный ответ),
- на установление правильной последовательности,
- на установление соответствия.

Результаты практической подготовки (умения, навыки (или опыт деятельности) и компетенции) проверяются с помощью компетентностно-

ориентированных задач (ситуационных, производственных или кейсового характера) и различного вида конструкторов.

Все задачи являются многоходовыми. Некоторые задачи, проверяющие уровень сформированности компетенций, являются многовариантными. Часть умений, навыков и компетенций прямо не отражена в формулировках задач, но они могут быть проявлены обучающимися при их решении.

В каждый вариант КИМ включаются задания по каждому проверяемому элементу содержания во всех перечисленных выше формах и разного уровня сложности. Такой формат КИМ позволяет объективно определить качество освоения обучающимися основных элементов содержания дисциплины и уровень сформированности компетенций.

#### Примеры типовых заданий для проведения промежуточной аттестации обучающихся

Задание в закрытой форме:

Распределение засекречиваемых данных, согласно уровню секретности, регламентацию и разделение допуска к защищаемым данным \_\_\_\_\_

Задание в открытой форме:

Структурное подразделение службы защиты информации, которое отвечает за контакты с правоохранительными органами по всем вопросам обеспечения безопасности деятельности объекта:

- а) группа режима;
- б) группа охраны и сопровождения;
- в) техническая группа;
- г) детективная группа.

Задание на установление правильной последовательности:

Обследование состояния объекта и уровня организации защиты информации, разработка и обоснование задач по защите информации, выявление потенциально возможных угроз информации, внедрение системы защиты информации, анализ безопасности используемых для передачи конфиденциальной информации линий связи.

Задание на установление соответствия:

1. режимно-секретное подразделение;
2. бюро пропусков;
3. контрольно-пропускной пункт (КПП).

А) отвечает за выполнение комплекса мероприятий по пропускному режиму и осуществляют постоянный контроль над их выполнением

Б) служат для непрерывного осуществления пропускного режима на территорию и объекты предприятия, контролируют вход и выход лиц с территории предприятия

В) решает непосредственно задачи по учету, хранению, уничтожению и выдаче пропусков сотрудникам предприятия, а также другим лицам, имеющим на это право.

Компетентностно-ориентированная задача:

Провести анализ потенциальных каналов утечки в аудитории проведения занятий. Составить перечень каналов утечки информации на защищаемом объекте с указанием места расположения и предлагаемые технические и организационные меры противодействия.

Полностью оценочные материалы и оценочные средства для проведения промежуточной аттестации обучающихся представлены в УММ по дисциплине.

#### **7.4 Методические материалы, определяющие процедуры оценивания знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций**

Процедуры оценивания знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций, регулируются следующими нормативными актами университета:

– положение П 02.016 «О балльно-рейтинговой системе оценивания результатов обучения по дисциплинам (модулям) и практикам при освоении обучающимися образовательных программ»;

– методические указания, используемые в образовательном процессе, указанные в списке литературы.

Для текущего контроля успеваемости по дисциплине в рамках действующей в университете балльно-рейтинговой системы применяется следующий порядок начисления баллов:

Таблица 7.4 – Порядок начисления баллов в рамках БРС

Форма контроля	Минимальный балл		Максимальный балл	
	балл	примечание	балл	примечание
Выполнение практической работы №1 «Анализ заданного нормативно-правового акта Российской Федерации».	6	Выполнил, но «не защитил»	8	Выполнил и «защитил»
Производственные задачи к занятию 4	0		4	
Выполнение практической работы №2 «Работа с нормативно-правовыми документами».	6	Выполнил, но «не защитил»	8	Выполнил и «защитил»
Производственные задачи к занятию 2	0		4	

Выполнение практической работы №3 «Система анализа рисков и проверки политики информационной безопасности предприятия»	6	Выполнил, но «не защитил»	8	Выполнил и «защитил»
СРС	6		16	
Итого	24		48	
Посещаемость	0		16	
Зачет	0		36	
Итого	24		100	

Для промежуточной аттестации обучающихся, проводимой в виде тестирования, используется следующая методика оценивания знаний, умений, навыков и (или) опыта деятельности. В каждом варианте КИМ –16 заданий (15 вопросов и одна задача).

Каждый верный ответ оценивается следующим образом:

- задание в закрытой форме –2 балла,
- задание в открытой форме – 2 балла,
- задание на установление правильной последовательности – 2 балла,
- задание на установление соответствия – 2 балла,
- решение компетентностно-ориентированной задачи – 6 баллов.

Максимальное количество баллов за тестирование –36 баллов.

## **8 Перечень основной и дополнительной учебной литературы, необходимой для освоения дисциплины**

### **8.1 Основная учебная литература**

1. Аверченков, В. И. Служба защиты информации: организация и управление : учебное пособие для вузов / В. И. Аверченков, М. Ю. Рытов. - 3-е изд., стереотип. - М.: Флинта, 2016. - 186 с. - URL: <https://biblioclub.ru/index.php?page=book&id=93356> (дата обращения: 26.08.2021). - Режим доступа: по подписке. – Текст : электронный.

2. Литвак, Б. Г. Разработка управленческого решения [Текст] : учебник для студ. вуз. / Б. Г. Литвак. - М. : Дело, 2000. - 392 с.

3. Степанова, Е. Е. Информационное обеспечение управленческой деятельности [Текст] : учебное пособие / Е. Е. Степанова, Н. В. Хмелевская. - М. : Форум, 2004. - 154 с.

### **8.2 Дополнительная учебная литература**

1. Аверченков, В. И. Аудит информационной безопасности : учебное пособие для вузов / В. И. Аверченков. - 3-е изд., стереотип. - М. : Флинта, 2016. - 269 с. – URL: <https://biblioclub.ru/index.php?page=book&id=93245> (дата обращения: 26.08.2021). – Режим доступа: по подписке. – Текст : электронный.

2. Загинайлов, Ю. Н. Теория информационной безопасности и методология защиты информации : учебное пособие / Ю. Н. Загинайлов. - М. ; Берлин : Директ-Медиа, 2015. - 253 с. – URL: <https://biblioclub.ru/index.php?page=book&id=276557> (дата обращения: 26.08.2021). – Режим доступа: по подписке. – Текст : электронный.

3. Лопин, В. Н. Защита информации в компьютерных системах [Текст] : учебное пособие / В. Н. Лопин, И. С. Захаров, А. В. Николаев ; Министерство образования и науки Российской Федерации, Курский государственный технический университет. - Курск : КГТУ, 2006. - 159 с.

4. Мельников, В. В. Защита информации в компьютерных системах [Текст] / В. В. Мельников. - М. : Финансы и статистика, 1997. - 368 с.

5. Петренко, В. И. Теоретические основы защиты информации : учебное пособие / В. И. Петренко ; Министерство образования и науки Российской Федерации, Федеральное государственное автономное образовательное учреждение высшего профессионального образования «Северо-Кавказский федеральный университет». - Ставрополь :СКФУ, 2015. - 222 с. – URL: <https://biblioclub.ru/index.php?page=book&id=458204> (дата обращения: 26.08.2021). – Режим доступа: по подписке. – Текст : электронный.

6. Ярочкин, В. И. Безопасность информационных систем [Текст] / В. И. Ярочкин. - М. : Ось-89, 1996. - 320 с.

## 8.2 Перечень методических указаний

1) Анализ заданного нормативно-правового акта Российской Федерации : методические указания по выполнению лабораторной работы : [для студентов укрупненной группы специальностей 10.00.00 дневной формы обучения] / Юго-Зап. гос. ун-т ; сост.: В. В. Карасовский, О. А. Демченко. - Курск : ЮЗГУ, 2017. - 6 с. - Библиогр.: с. 6. - Текст : электронный.

2) Система анализа рисков и проверки политики информационной безопасности предприятия : методические указания по выполнению лабораторной работы : [для студентов укрупненной группы специальностей 10.00.00 дневной формы обучения] / Юго-Зап. гос. ун-т ; сост.: В. В. Карасовский, О. А. Демченко. - Курск : ЮЗГУ, 2017. - 9 с. : ил., табл. - Библиогр.: с. 8. - Текст : электронный.

3) Работа с нормативно-правовыми документами : методические указания по выполнению лабораторной работы : [для студентов укрупненной группы специальностей 10.00.00 дневной формы обучения] / Юго-Зап. гос. ун-т ; сост.: В. В. Карасовский, О. А. Демченко. - Курск : ЮЗГУ, 2017. - 11 с. : табл. - Библиогр.: с. 11. - Текст : электронный.

## 9 Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины



- 1) Федеральная служба безопасности [официальный сайт]. Режим доступа: <http://www.fsb.ru/>
- 2) Федеральная служба по техническому и экспортному контролю [официальный сайт]. Режим доступа: <http://fstec.ru/>
- 3) Электронно-библиотечная система «Университетская библиотека онлайн» Режим доступа: <http://biblioclub.ru>
- 4) Компания «Консультант Плюс» [официальный сайт]. Режим доступа: <http://www.consultant.ru>
- 5) Научно-информационный портал ВИНТИ РАН [официальный сайт]. Режим доступа: <http://www.consultant.ru/>
- 6) База данных "Патенты России"
- 7) Аналитический раздел компании «Код Безопасности» <https://www.securitycode.ru/documents/analytics/>

## **10 Методические указания для обучающихся по освоению дисциплины**

Основными видами аудиторной работы студента при изучении дисциплины «Организация и управление службой защиты информации» являются лекции и практические работы. Студент не имеет права пропускать занятия без уважительных причин.

На лекциях излагаются и разъясняются основные понятия темы, связанные с ней теоретические и практические проблемы, даются рекомендации для самостоятельной работы. В ходе лекции студент должен внимательно слушать и конспектировать материал.

Изучение наиболее важных тем или разделов дисциплины завершают практические работы, которые обеспечивают: контроль подготовленности студента; закрепление учебного материала; приобретение опыта устных публичных выступлений, ведения дискуссии, в том числе аргументации и защиты выдвигаемых положений и тезисов.

Практической работе предшествует самостоятельная работа студента, связанная с освоением материала, полученного на лекциях, и материалов, изложенных в учебниках и учебных пособиях, а также литературе, рекомендованной преподавателем.

По согласованию с преподавателем или по его заданию студенты готовят рефераты по отдельным темам дисциплины, выступают на занятиях с докладами. Основу докладов составляет, как правило, содержание подготовленных студентами рефератов.

Качество учебной работы студентов преподаватель оценивает по результатам тестирования, собеседования, защиты отчетов по практическим работам, а также по результатам докладов.

Преподаватель уже на первых занятиях объясняет студентам, какие формы обучения следует использовать при самостоятельном изучении дисциплины «Организация и управление службой защиты информации»: конспектирование учебной литературы и лекции, составление словарей понятий и терминов и т. п.

В процессе обучения преподаватели используют активные формы работы со студентами: чтение лекций, привлечение студентов к творческому процессу на лекциях, отработку студентами пропущенных лекций, участие в групповых и индивидуальных консультациях (собеседовании). Эти формы способствуют выработке у студентов умения работать с учебником и литературой. Изучение литературы составляет значительную часть самостоятельной работы студента. Это большой труд, требующий усилий и желания студента. В самом начале работы над книгой важно определить цель и направление этой работы. Прочитанное следует закрепить в памяти. Одним из приемов закрепления освоенного материала является конспектирование, без которого немислима серьезная работа над литературой. Систематическое конспектирование помогает научиться правильно, кратко и четко излагать своими словами прочитанный материал.

Самостоятельную работу следует начинать с первых занятий. От занятия к занятию нужно регулярно прочитывать конспект лекций, знакомиться с соответствующими разделами учебника, читать и конспектировать литературу по каждой теме дисциплины. Самостоятельная работа дает студентам возможность равномерно распределить нагрузку, способствует более глубокому и качественному освоению учебного материала. В случае необходимости студенты обращаются за консультацией к преподавателю по вопросам дисциплины «Организация и управление службой защиты информации» с целью освоения и закрепления компетенций.

Основная цель самостоятельной работы студента при изучении дисциплины «Организация и управление службой защиты информации» - закрепить теоретические знания, полученные в процессе лекционных занятий, а также сформировать практические навыки самостоятельного анализа особенностей дисциплины.

#### **11 Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине, включая перечень программного обеспечения и информационных справочных систем (при необходимости)**

Microsoft Office 2016.Лицензионный договор №S0000000722 от 21.12.2015 г. с ООО «АйТи46», лицензионный договор №K0000000117 от 21.12.2015 г. с ООО «СМСКанал»,

Kaspersky Endpoint Security Russian Edition, лицензия 156A-140624-192234,

Windows 7, договор IT000012385

#### **12 Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине**

Для осуществления практической подготовки обучающихся при реализации дисциплины используются оборудование и технические средства обучения кафедры информационной безопасности:

- учебная аудитория для проведения занятий лекционного и практического типа или лаборатории кафедры информационная безопасность, оснащенные мебелью: столы, стулья для обучающихся; стол, стул для преподавателя; доска, проектор для демонстрации презентаций;

- помещение для самостоятельной работы;

- компьютер PDC2160/iC33/2\*512Mb/HDD 160Gb/DVD-ROM/FDD/ATX350W/K/m/OFF/17"TFTE700(6шт).

Для осуществления практической подготовки обучающихся при реализации дисциплины используются оборудование и технические средства обучения кафедры информационной безопасности:

- проектор для демонстрации презентаций;

- аттестованное помещение для обработки конфиденциальной информации

- Сейф;

### **13 Особенности реализации дисциплины для инвалидов и лиц с ограниченными возможностями здоровья**

При обучении лиц с ограниченными возможностями здоровья учитываются их индивидуальные психофизические особенности. Обучение инвалидов осуществляется также в соответствии с индивидуальной программой реабилитации инвалида (при наличии).

Для лиц с нарушением слуха возможно предоставление учебной информации в визуальной форме (краткий конспект лекций; тексты заданий, напечатанные увеличенным шрифтом), на аудиторных занятиях допускается присутствие ассистента, а также сурдопереводчиков и тифлосурдопереводчиков. Текущий контроль успеваемости осуществляется в письменной форме: обучающийся письменно отвечает на вопросы, письменно выполняет практические задания. Доклад (реферат) также может быть представлен в письменной форме, при этом требования к содержанию остаются теми же, а требования к качеству изложения материала (понятность, качество речи, взаимодействие с аудиторией и т. д.) заменяются на соответствующие требования, предъявляемые к письменным работам (качество оформления текста и списка литературы, грамотность, наличие иллюстрационных материалов и т.д.). Промежуточная аттестация для лиц с нарушениями слуха проводится в письменной форме, при этом используются общие критерии оценивания. При необходимости время подготовки к ответу может быть увеличено.

Для лиц с нарушением зрения допускается аудиальное предоставление информации, а также использование на аудиторных занятиях звукозаписывающих устройств (диктофонов и т.д.). Допускается присутствие на занятиях ассистента (помощника), оказывающего обучающимся

необходимую техническую помощь. Текущий контроль успеваемости осуществляется в устной форме. При проведении промежуточной аттестации для лиц с нарушением зрения тестирование может быть заменено на устное собеседование по вопросам.

Для лиц с ограниченными возможностями здоровья, имеющих нарушения опорно-двигательного аппарата, на аудиторных занятиях, а также при проведении процедур текущего контроля успеваемости и промежуточной аттестации могут быть предоставлены необходимые технические средства (персональный компьютер, ноутбук или другой гаджет); допускается присутствие ассистента (ассистентов), оказывающего обучающимся необходимую техническую помощь (занять рабочее место, передвигаться по аудитории, прочесть задание, оформить ответ, общаться с преподавателем).

**14 Лист дополнений и изменений, внесенных в рабочую программу дисциплины**

Номер изменения	Номера страниц			Всего страниц	Дата	Основание для изменения и подпись лица, проводившего изменения
	измененных	замененных	аннулированных новых			