Аннотация к рабочей программе дисциплины «Основы управления информационной безопасностью»

Цель преподавания дисциплины

Целью преподавания дисциплины «Основы управления информационной безопасностью» является получение студентами знаний о основных подходов к разработке, реализации, эксплуатации, анализу, сопровождению и совершенствованию систем управления информационной безопасностью определенного объекта.

Задачи изучения дисциплины

−рассмотреть основы управления информационной безопасностью;

−рассмотреть угрозы информационной безопасности в информационных системах;

−рассмотреть оценочные стандарты в информационной безопасности;

−рассмотреть стандарты управления информационной безопасностью;

– рассмотреть создание системы управления информационной безопасности на предприятии;

– рассмотреть методики и технологии управления рисками;

– рассмотреть разработку корпоративной методики анализа рисков;

– рассмотреть современные методы и средства анализа и управление рисками информационных систем компаний;

– рассмотреть правовые меры обеспечения информационной безопасности;

– рассмотрение организационных меры обеспечения безопасности компьютерных информационных систем;

– рассмотреть программно-технические меры обеспечения информационной безопасности. Идентификация, аутентификация, управление доступом.

Компетенции, формируемые в результате освоения дисциплины

– ОПК-1: Способен оценивать роль информации, информационных технологий и информационной безопасности в современном обществе, их значение для обеспечения объективных потребностей личности, общества и государства.

– 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.

– ОПК-12: Способен проводить подготовку исходных данных для проектирования подсистем, средств обеспечения защиты информации и для технико-экономического обоснования соответствующих проектных решений.
– ОПК-4.1: Способен проводить организационные мероприятия по обеспечению безопасности информации в автоматизированных системах.

Разделы дисциплины

1	Основные понятия информационной безопасности.
2	Угрозы информационной безопасности в информационных системах.
3	Оценочные стандарты в информационной безопасности
4	Стандарты управления информационной безопасностью
5	Создание СУИБ на предприятии
6	Методики и технологии управления рисками
7	Разработка корпоративной методики анализа рисков
8	Современные методы и средства анализа и управление рисками информационных систем компаний
9	Правовые меры обеспечения информационной безопасности

МИНОБРНАУКИ РОССИИ

Юго-Западный государственный университет

УТВЕРЖДАЮ:
И.О. декана факультета
Фундаментальной и прикладной информатики
(наименование ф-та полностью)

_____М.О. Таныгин
(подпись, инициалы, фамилия)

«30» июня 2022 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Основы управления информационной безопасностью

(наименование дисциплины)

ОПОП ВО 10.03.01Информационная безопасность
(шифр согласно ФГОС и наименование направления подготовки (специальности))

направленность (профиль, специализация) «Безопасность автоматизированных систем в сфере информационных и коммуникационных технологий»
наименование направленности (профиля, специализации)

форма обучения очная
(очная, очно-заочная, заочная)

Курск – 2022

Рабочая программа дисциплины Основы управления информационной безопасностью в соответствии с ФГОС ВО – бакалавриат по направлению подготовки (специальности) 10.03.01Информационная безопасность на основании учебного плана ОПОП ВО 10.03.01Информационная безопасность, направленность «Безопасность автоматизированных систем в сфере информационных и коммуникационных технологий», одобренного Ученым советом университета (протокол №6 «26» февраля 2022 г.).

Рабочая программа дисциплины Основы управления информационной безопасностью обсуждена и рекомендована к реализации в образовательном процессе для обучения студентов по ОПОП ВО 10.03.01 Информационная безопасность, направленность «Безопасность автоматизированных систем в сфере информационных и коммуникационных технологий» на заседании кафедры информационной безопасности Протокол №11 «30» июня 2022 г.

Зав. кафедрой Таныгин М.О.

Разработчик программы Кулешова Е.А.

Директор научной библиотеки Макаровская В.Г.

Рабочая программа дисциплины Основы управления информационной безопасностью пересмотрена, обсуждена и рекомендована к реализации в образовательном процессе на основании учебного плана ОПОП ВО 10.03.01 Информационная безопасность, направленность «Безопасность автоматизированных систем в сфере информационных и коммуникационных технологий», одобренного Ученым советом университета Протокол № « » _____ 20 г., на заседании кафедры_____ .

(наименование кафедры, дата, номер протокола)

Зав. кафедрой _____

Рабочая программа дисциплины Основы управления информационной безопасностью пересмотрена, обсуждена и рекомендована к реализации в образовательном процессе на основании учебного плана ОПОП ВО 10.03.01 Информационная безопасность, направленность «Безопасность автоматизированных систем в сфере информационных и коммуникационных технологий», 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, соотнесённых с планируемыми результатами освоения образовательной программы

1.1. Цель преподавания дисциплины

Целью преподавания дисциплины «Основы управления информационной безопасностью» является получение студентами знаний о основных подходов к разработке, реализации, эксплуатации, анализу, сопровождению и совершенствованию систем управления информационной безопасностью определенного объекта.

1.2. Задачи изучения дисциплины

−рассмотреть основы управления информационной безопасностью;

−рассмотреть угрозы информационной безопасности в информационных системах;

−рассмотреть оценочные стандарты в информационной безопасности;

−рассмотреть стандарты управления информационной безопасностью;

– рассмотреть создание системы управления информационной безопасности на предприятии;

– рассмотреть методики и технологии управления рисками;

– рассмотреть разработку корпоративной методики анализа рисков;

– рассмотреть современные методы и средства анализа и управление рисками информационных систем компаний;

– рассмотреть правовые меры обеспечения информационной безопасности;

– рассмотрение организационных меры обеспечения безопасности компьютерных информационных систем;

– рассмотреть программно-технические меры обеспечения информационной безопасности. Идентификация, аутентификация, управление доступом.

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

Таблица 1.3 – Результаты обучения по дисциплине

Планируемые результаты освоения основной профессиональной образовательной программы (компетенции, закрепленные за дисциплиной)		*Код и наименование индикатора достижения компетенции, закрепленного за дисциплиной*	*Планируемые результаты обучения по дисциплине, соотнесенные с индикаторами достижения компетенций*
код компетенции	*наименование компетенции*		

Планируемые результаты освоения основной профессиональной образовательной программы (компетенции, закрепленные за дисциплиной)		*Код и наименование индикатора достижения компетенции, закрепленного за дисциплиной*	*Планируемые результаты обучения по дисциплине, соотнесенные с индикаторами достижения компетенций*
код компетенции	*наименование компетенции*		
ОПК-1	Способен оценивать роль информации, информационных технологий и информационной безопасности в современном обществе, их значение для обеспечения объективных потребностей личности, общества и государства	ОПК-1.3 Определяет угрозы информационной безопасности для различных систем	***Знать:*** - основы работы в режиме пошаговой отладки передачи конфиденциальных данных в информационной системе; - особенности вывода промежуточных значений в ходе работы отдельных модулей информационных систем; - основы использования средств защиты информации. ***Уметь:*** - выполнять выявление контрафактной продукции; - организовать безопасную работу в Интернет; - выводить сообщения в случае возникновения нештатных ситуаций работы информационной системы; - интегрировать средства защиты на программном уровне. ***Владеть (****или* ***Иметь опыт деятельности):*** - навыками установки программных средств защиты; - технологией ведения протокола работы системы с выводом промежуточных результатов обработки данных. - навыками оценки защищенности информационной системы с учетом возможных угроз.
ОПК-5	Способен применять нормативные правовые акты, нормативные и методические документы, регламентирующие деятельность по защите информации в сфере профессиональной деятельности	ОПК-5.2 Формулирует основные требования по защите конфиденциальной информации, персональных данных и охране результатов интеллектуальной деятельности в	***Знать:*** Правовые нормы и стандарты по защите конфиденциальной информации, персональных данных и охране результатов интеллектуальной деятельности в организации; принципы формирования политики информационной безопасности в автоматизированных системах ***Уметь:*** применять действующую законодательную базу по защите конфиденциальной

Планируемые результаты освоения основной профессиональной образовательной программы (компетенции, закрепленные за дисциплиной)		*Код и наименование индикатора достижения компетенции, закрепленного за дисциплиной*	*Планируемые результаты обучения по дисциплине, соотнесенные с индикаторами достижения компетенций*
код компетенции	*наименование компетенции*		
		организации	информации, персональных данных и охране результатов интеллектуальной деятельности в организации; разрабатывать проекты локальных правовых актов, инструкций, регламентов и организационно-распорядительных документов, регламентирующих работу по обеспечению информационной безопасности в организации ***Владеть (****или* ***Иметь опыт деятельности):*** навыками работы с нормативными правовыми актами; навыками разработки проектов локальных правовых актов, инструкций, регламентов и организационно-распорядительных документов, регламентирующих работу по защите конфиденциальной информации, персональных данных и охране результатов интеллектуальной деятельности в организации.
		ОПК-5.3 Формулирует основные требования при лицензировании деятельности в области защиты информации, сертификации и аттестации по требованиям безопасности информации	***Знать:*** Правовые нормы и стандарты по лицензированию в области обеспечения защиты информации и сертификации средств защиты; основные отечественные и зарубежные стандарты в области информационной безопасности; терминологию, основные руководящие и регламентирующие документы в области ЭВМ, комплексов и систем. ***Уметь:*** применять действующую законодательную базу в области обеспечения информационной безопасности при лицензировании деятельности в области защиты информации, сертификации и аттестации по требованиям безопасности

Планируемые результаты освоения основной профессиональной образовательной программы (компетенции, закрепленные за дисциплиной)		*Код и наименование индикатора достижения компетенции, закрепленного за дисциплиной*	*Планируемые результаты обучения по дисциплине, соотнесенные с индикаторами достижения компетенций*
код компетенции	*наименование компетенции*		
			информации; разрабатывать проекты локальных правовых актов, инструкций, регламентов при лицензировании деятельности в области защиты информации, сертификации и аттестации по требованиям безопасности информации. ***Владеть (****или* ***Иметь опыт деятельности):*** навыками работы с нормативными правовыми актами; навыками работы с технической документацией на ЭВМ и вычислительные системы; навыками работы с технической документацией на компоненты автоматизированных систем на русском и иностранном языках.
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	ОПК-6.1 Разрабатывает модели угроз и модели нарушителя объекта информатизации	***Знать*** основные угрозы безопасности и модели нарушителя объекта информатизации ***Уметь:*** разрабатывать модели угроз и модели нарушителя объекта информатизации ***Владеть (или Иметь опыт деятельности):*** навыками оценки угроз для объекта информатизации
		ОПК-6.2 Определяет политику контроля доступа работников к информации ограниченного доступа	***Знать:*** - основные требования, предъявляемые к сотрудникам защиты информации ограниченного доступа; - угрозы безопасности; - модели нарушителя объекта информатизации. ***Уметь:*** - составлять перечень лиц, имеющих доступ к информации ограниченного доступа; - разрабатывать требования, предъявляемые к контролю доступа сотрудников к информации ограниченного доступа***;***

Планируемые результаты освоения основной профессиональной образовательной программы (компетенции, закрепленные за дисциплиной)		*Код и наименование индикатора достижения компетенции, закрепленного за дисциплиной*	*Планируемые результаты обучения по дисциплине, соотнесенные с индикаторами достижения компетенций*
код компетенции	*наименование компетенции*		
			Владеть (*или* ***Иметь опыт деятельности):*** - навыками формулирования основных требований, предъявляемых к организации защиты информации ограниченного доступа; - навыками создания локальных нормативных актов.***локальных нормативных актов.***
		ОПК-6.3 Формулирует требования, предъявляемые к физической защите объекта и пропускному режиму в организации	***Знать:*** - основные требования, предъявляемые к сотрудникам защиты информации ограниченного доступа; - угрозы безопасности; - модели нарушителя объекта информатизации. ***Уметь:*** - составлять перечень лиц, имеющих доступ к информации ограниченного доступа; - разрабатывать требования, предъявляемые к контролю доступа сотрудников к информации ограниченного доступа***;*** ***Владеть (****или* ***Иметь опыт деятельности):*** - навыками формулирования основных требований, предъявляемых к организации защиты информации ограниченного доступа; - навыками создания локальных нормативных актов.
		ОПК-6.4 Разрабатывает проекты инструкций, регламентов, положений и приказов, регламентирующих защиту информации ограниченного доступа в	***Знать*** правовые нормы и стандарты для разработки инструкций, регламентов, положений и приказов, регламентирующих защиту информации ***Уметь:*** составлять проекты инструкций, регламентов, положений и приказов, регламентирующих защиту информации ограниченного доступа в организации

Планируемые результаты освоения основной профессиональной образовательной программы (компетенции, закрепленные за дисциплиной)		*Код и наименование индикатора достижения компетенции, закрепленного за дисциплиной*	*Планируемые результаты обучения по дисциплине, соотнесенные с индикаторами достижения компетенций*
код компетенции	*наименование компетенции*		
		организации	***Владеть (****или* ***Иметь опыт деятельности):*** навыками организации документооборота в области защиты информации.
ОПК-12	Способен проводить подготовку исходных данных для проектирования подсистем, средств обеспечения защиты информации и для технико-экономического обоснования соответствующих проектных решений	ОПК-12.3 Оценивает информационные риски в автоматизированных системах	***Знать:*** классификацию, виды и типы угроз безопасности автоматизированных систем, принципы построения средств защиты информации и возможные риски нарушения безопасности функционирования объекта информатизации; основные компоненты автоматизированных систем объекта информатизации, состав, структуры и принципы функционирования современных автоматизированных систем, требования основных законов и нормативных документов в области безопасности автоматизированных систем; методы, способы и методики анализа рисков безопасности автоматизированных систем; ***Уметь:*** определять угрозы безопасности автоматизированных систем, определять возможные риски нарушения безопасности функционирования объекта информатизации; определять состав, структуру и принципы функционирования современных автоматизированных систем, анализировать требования основных законов и нормативных документов в области безопасности автоматизированных систем; применять методики анализа рисков безопасности автоматизированных систем; определять основные источники угроз, принимать технические меры, направленные на повышение защищенности и снижения рисков нарушения безопасности автоматизированных

Планируемые результаты освоения основной профессиональной образовательной программы (компетенции, закрепленные за дисциплиной)		*Код и наименование индикатора достижения компетенции, закрепленного за дисциплиной*	*Планируемые результаты обучения по дисциплине, соотнесенные с индикаторами достижения компетенций*
код компетенции	*наименование компетенции*		
			систем. ***Владеть (****или* ***Иметь опыт деятельности):*** навыками анализа защищенности автоматизированных систем; навыками защиты информации в компьютерных системах; навыками определения угроз безопасности автоматизированных систем, выбора средств защиты информации; требованиями основных законов и нормативных документов в области безопасности автоматизированных систем; методиками анализа рисков безопасности автоматизированных систем и выявления источников угроз; навыками проведения и организации комплекса мероприятий по повышению защищенности и снижению рисков нарушения безопасности автоматизированных систем; навыками построения комплексной системы защиты автоматизированных систем объекта информатизации.
ОПК-4.1	Способен проводить организационные мероприятия по обеспечению безопасности информации в автоматизированных системах	ОПК-4.1.1 Определяет подлежащие защите информационные ресурсы автоматизированных систем	***Знать*** основные требования по защите информационной системы. ***Уметь:*** определять правила и процедуры, реализуемые оператором, для обеспечения защиты информации в информационной системе в ходе ее эксплуатации. ***Владеть (****или* ***Иметь опыт деятельности):*** навыками разработки организационно-распорядительной документации по защите информации.
		ОПК-4.1.2 Составляет комплексы правил, процедур, практических приемов, принципов	***Знать*** организационные основы информационной безопасности ***Уметь:*** анализировать и оценивать угрозы информационной безопасности объекта

Планируемые результаты освоения основной профессиональной образовательной программы (компетенции, закрепленные за дисциплиной)		*Код и наименование индикатора достижения компетенции, закрепленного за дисциплиной*	*Планируемые результаты обучения по дисциплине, соотнесенные с индикаторами достижения компетенций*
код компетенции	*наименование компетенции*		
		и методов, средств обеспечения защиты информации в автоматизированной системе	***Владеть (****или* ***Иметь опыт деятельности):*** навыками оценки состояния организационной защиты информации на объекте и разработки рациональных мер по обеспечению организационной защиты
		ОПК-4.1.3 Организует работу персонала автоматизированной системы с учетом требований по защите информации	***Знать*** основные нормативно-правовые акты в области информационной безопасности и защиты информации. ***Уметь:*** формулировать задачи для организации работы персонала автоматизированной системы; оценивать итоги исполнения поставленных задач перед персоналом. ***Владеть (****или* ***Иметь опыт деятельности):*** организационно-управленческой работы.

2. Указание места дисциплины в структуре основной профессиональной образовательной программы

Дисциплина «Основы управления информационной безопасностью», входит в обязательную часть блока 1 «Дисциплины (модули)») основной профессиональной образовательной программы – программы бакалавриата 10.03.01 Информационная безопасность, направленность «Безопасность автоматизированных систем в сфере информационных и коммуникационных технологий». Дисциплина изучается на 4 курсе в 7 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 4 зачетных единицы (з.е.), 144 академических часа.

Таблица 3 - Объём дисциплины

Виды учебной работы	Всего, часов
Общая трудоемкость дисциплины	144
Контактная работа обучающихся с преподавателем по видам учебных занятий (всего)	72
в том числе:	
лекции	36
лабораторные занятия	0
практические занятия	36
Самостоятельная работа обучающихся (всего)	43,85
Контроль (подготовка к экзамену)	27
Контактная работа по промежуточной аттестации (всего АттКР)	1,15
в том числе:	
зачет	не предусмотрен
зачет с оценкой	не предусмотрен
курсовая работа (проект)	не предусмотрена
экзамен (включая консультацию перед экзаменом)	1,15

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	Организация деятельности службы безопасности Правовое обеспечение службы. Принципы организации службы.

	деятельности службы информационной безопасности	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 4.2 –Содержание дисциплины и её методическое обеспечение

№ п/п	Раздел (тема) дисциплины	Виды деятельности			Учебно-методические материалы	Формы текущего контроля успеваемости *(по неделям семестра)*	Компетенции
		лек., час	№ лб.	№ пр.			
1	2	3	4	5	6	7	8
1.	Структура службы информационной безопасности	4		1	У- 1-5 МУ-1,2	УО, ЗПР 1-2	ОПК-1, ОПК-5, ОПК-6, ОПК-12, ОПК-4.1
2.	Функции основных групп службы безопасности	4			У- 1-5 МУ-2	УО 3-4	ОПК-1, ОПК-5, ОПК-6, ОПК-12, ОПК-4.1
3.	Цели и задачи службы информационной безопасности	4		2	У- 1-5 МУ-1,2	УО, ЗПР 5-6	ОПК-1, ОПК-5, ОПК-6, ОПК-12, ОПК-4.1
4.	Организационные основы и принципы деятельности службы информационной безопасности	4		3	У- 1-5 МУ-1,2	УО, ЗПР 7-8	ОПК-1, ОПК-5, ОПК-6, ОПК-12, ОПК-4.1
5.	Лицензирование видов деятельности службы безопасности.	4			У- 1-5 МУ-2	УО 9-10	ОПК-1, ОПК-5, ОПК-6, ОПК-12, ОПК-4.1
6.	Управление службой защиты информации.	4			У- 1-5 МУ-2	УО 11-12	ОПК-1, ОПК-5, ОПК-6, ОПК-12, ОПК-4.1

1	2	3	4	5	6	7	8
7.	Организация информационно-аналитической работы.	6			У- 1-5 МУ-2	УО 13-15	ОПК-1, ОПК-5, ОПК-6, ОПК-12, ОПК-4.1
8.	Организация работы с персоналом предприятия.	6		4	У- 1-5 МУ-2	УО 16-18	ОПК-1, ОПК-5, ОПК-6, ОПК-12, ОПК-4.1
	Всего	36					

УО – устный опрос, ЗПР – защита практической работы

4.2 Лабораторные работы и (или) практические занятия

4.2.1 Практические занятия

Таблица 4.4 – Практические занятия

№	Наименование практической работы	Объем, час.
1.	Определение класса государственной информационной системы (ГИС)	8
2.	Разработка структуры государственных и международных стандартов в Российской Федерации в области информационной безопасности и защиты информации	8
3.	Составление обзорного документа по сертифицированным продуктам в заданной области информационной безопасности	10
4.	Анализ заданного нормативно-правового акта Российской Федерации	10
Итого		36

4.3 Самостоятельная работа студентов (СРС)

Таблица 4.5 – Самостоятельная работа студентов

№	Наименование раздела учебной дисциплины	Срок выполнения	Время, затрачиваемое на выполнение СРС, час.
1.	Структура службы информационной безопасности	1-2 недели	4
2.	Функции основных групп службы безопасности	3-4 недели	4
3.	Цели и задачи службы информационной безопасности	5-6 недели	4
4.	Организационные основы и принципы деятельности службы информационной безопасности	7-8 недели	6
5.	Лицензирование видов деятельности службы безопасности.	9-10 недели	6
6.	Управление службой защиты информации.	11-12 недели	6
7.	Организация информационно-аналитической работы.	13-15 недели	6
8.	Организация работы с персоналом предприятия.	16-18 недели	7,85
Итого			43,85

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 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 за счёт выкладывания на сайт кафедры ИБ в интернете (адрес http://www.swsu.ru/structura/up/fivt/k_tele/index.php);

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

путем разработки:

- методических рекомендаций, пособий по организации самостоятельной работы студентов;

– заданий для самостоятельной работы;

– вопросов и задач к экзамену;

–методических указаний к выполнению практических 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. Технологии использования воспитательного потенциала дисциплины

Реализация компетентностного подхода предусматривает широкое использование в образовательном процессе активных и интерактивных форм проведения занятий в сочетании с внеаудиторной работой с целью формирования общепрофессиональных компетенций обучающихся. В рамках дисциплины предусмотрены встречи с экспертами и специалистами Комитета цифрового развития и связи Курской области.

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

№	Наименование раздела	Используемые интерактивные образовательные технологии	Объём, час.
1.	Практическая работа №1 «Определение класса государственной информационной системы (ГИС)»	Разбор конкретных ситуаций	2
2.	Практическая работа №2 «Разработка структуры государственных и международных стандартов в РФ в области информационной безопасности и защиты информации»	Разбор конкретных ситуаций	2
3.	Практическая работа №3 «Составление обзорного документа по сертифицированным продуктам в заданной области информационной безопасности»	Разбор конкретных ситуаций	2
4.	Практическая работа №4 «Анализ заданного нормативно-правового акта РФ»	Разбор конкретных ситуаций	4
	Итого		10

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, специализации) программы бакалавриата.

Содержание дисциплины обладает значительным воспитательным потенциалом, поскольку в нем аккумулирован научный 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 профессиональной культуры обучающихся. Содержание дисциплины способствует правовому, 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, высокого профессионализма ученых (представителей производства, деятелей культуры), их ответственности за результаты и последствия деятельности для природы, человека и общества;

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

– 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
ОПК-1 Способен оценивать роль информации, информационных технологий и информационной безопасности в современном обществе, их значение для обеспечения объективных потребностей личности, общества и государства	Основы информационной безопасности	Производственная эксплуатационная практика	Основы управления информационной безопасностью
ОПК-5 Способен применять нормативные правовые акты, нормативные и методические документы, регламентирующие деятельность по защите информации в сфере профессиональной деятельности	Организационное и правовое обеспечение информационной безопасности	Производственная эксплуатационная практика	Основы управления информационной безопасностью
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;	Организационное и правовое обеспечение информационной безопасности	Производственная эксплуатационная практика	Основы управления информационной безопасностью
ОПК-12 Способен проводить подготовку исходных данных для проектирования подсистем, средств обеспечения защиты информации и для технико-экономического обоснования соответствующих проектных решений;	Защита информации от утечки по техническим каналам		Основы управления информационной безопасностью
ОПК-4.1 Способен проводить организационные мероприятия по обеспечению безопасности	Организационное и правовое обеспечение информационной безопасности		Программно-аппаратные средства защиты информации Основы

информации в автоматизированных системах		управления информационной безопасностью

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

Таблица 7.2 Показатели, критерии и шкала оценивания компетенций

Код компетенции/ этап (указывается название этапа изп.7.1)	Показатели оценивания компетенций *(индикаторы достижения компетенций, закрепленные за дисциплиной)*	Критерии и шкала оценивания компетенций		
		Пороговый (удовлетворительно)	Продвинутый (хорошо)	Высокий (отлично)
1	2	3	4	5
ОПК-1/ завершающий	ОПК-1.3 Определяет угрозы информационной безопасности для различных систем	***Знать:*** - основы работы в режиме пошаговой отладки передачи конфиденциальных данных в информационной системе; ***Уметь:*** - выполнять выявление контрафактной продукции; - выводить сообщения в случае возникновения нештатных ситуаций работы информационной системы; ***Владеть (****или* ***Иметь опыт деятельности):*** - навыками установки программных средств защиты; - навыками оценки защищенности информационной системы с учетом возможных угроз.	***Знать:*** - особенности вывода промежуточных значений в ходе работы отдельных модулей информационных систем; - основы использования средств защиты информации. ***Уметь:*** - организовать безопасную работу в Интернет; - выводить сообщения в случае возникновения нештатных ситуаций работы информационной системы; - интегрировать средства защиты на программном уровне. ***Владеть (****или* ***Иметь опыт деятельности):*** - навыками установки программных средств защиты; - навыками оценки защищенности информационной системы с учетом	***Знать:*** - основы работы в режиме пошаговой отладки передачи конфиденциальных данных в информационной системе; - особенности вывода промежуточных значений в ходе работы отдельных модулей информационных систем; - основы использования средств защиты информации. ***Уметь:*** - выполнять выявление контрафактной продукции; - организовать безопасную работу в Интернет; - выводить сообщения в случае возникновения нештатных ситуаций работы информационной системы; - интегрировать средства защиты на программном уровне. ***Владеть (****или* ***Иметь опыт деятельности):*** - навыками установки программных средств защиты; - технологией ведения

			возможных угроз.	протокола работы системы с выводом промежуточных результатов обработки данных. - навыками оценки защищенности информационной системы с учетом возможных угроз.
ОПК-5/ завершающий	ОПК-5.2 Формулирует основные требования по защите конфиденциальной информации, персональных данных и охране результатов интеллектуальной деятельности в организации	Знать: - основные нормативные правовые документы. Уметь: - ориентироваться в системе законодательства и нормативных правовых актов в области защиты информации. Владеть: - навыками поиска необходимых нормативных и законодательных документов и навыками работы с ними в профессиональной деятельности	Знать: - нормативно правовые документы. Уметь: - использовать нормативно правовые акты в задачах защиты информации Владеть: - навыками поиска необходимых нормативных и законодательных документов и навыками анализа результатов их применения.	Знать: - Российские и международные нормативно правовые документы в области защиты информации. Уметь: - разрабатывать рекомендации по применению нормативно правовых документов в области защиты информации. Владеть: - навыками разработки организационно-распорядительной документации на объекте информатизации
	ОПК-5.3 Формулирует основные требования при лицензировании деятельности в области защиты информации, сертификации и аттестации по требованиям безопасности информации	Знать: - основные нормативные правовые документы. Уметь: - ориентироваться в системе законодательства и нормативных правовых актов в области защиты информации. Владеть: - навыками поиска необходимых нормативных и законодательных документов и навыками работы с ними в профессиональной деятельности	Знать: - нормативно правовые документы. Уметь: - использовать нормативно правовые акты в задачах защиты информации Владеть: - навыками поиска необходимых нормативных и законодательных документов и навыками анализа результатов их применения.	Знать: - Российские и международные нормативно правовые документы в области защиты информации. Уметь: - разрабатывать рекомендации по применению нормативно правовых документов в области защиты информации. Владеть: - навыками разработки организационно-распорядительной документации на объекте информатизации
ОПК-6/ завершающий	ОПК-6.1 Разрабатывает модели угроз и модели нарушителя объекта информатизации	Знать: - основные нормативные правовые документы по разработке модели нарушителя и угроз. Уметь: - ориентироваться в системе законодательства и нормативных правовых	Знать: - нормативно правовые документы. Уметь: - использовать нормативно правовые акты при разработке моделей угроз и	Знать: - Российские и международные нормативно правовые документы в области защиты информации. Уметь: - разрабатывать модели угроз и модели нарушителя объекта

		актов в области защиты информации. Владеть: - навыками поиска необходимых нормативных и законодательных документов для разработки модели угроз и нарушителя	нарушителей. Владеть: - навыками поиска необходимых нормативных и законодательных документов и навыками анализа результатов их применения.	информатизации. Владеть: - навыками анализа защищенности модели угроз и нарушителей.
	ОПК-6.2 Определяет политику контроля доступа работников к информации ограниченного доступа	*Знать* основные требования, предъявляемые к организации защиты информации ограниченного доступа *Уметь:* формулировать требования, предъявляемые к организации защиты информации ограниченного доступа *Владеть (или Иметь опыт деятельности):* навыками формулирования основных требований, предъявляемых к организации защиты информации ограниченного доступа	*Знать* требования, предъявляемые к организации защиты информации ограниченного доступа объекта информатизации *Уметь:* разрабатывать требования, предъявляемые к организации защиты информации ограниченного доступа *Владеть (или Иметь опыт деятельности):* навыками формулирования основных требований, предъявляемых к организации защиты информации ограниченного доступа	*Знать* требования, предъявляемые к организации защиты информации ограниченного доступа угрозы безопасности и модели нарушителя объекта информатизации *Уметь:* разрабатывать требования, предъявляемые к организации защиты информации ограниченного доступа *Владеть (или Иметь опыт деятельности):* навыками формулирования требований, предъявляемых к организации защиты информации ограниченного доступа
	ОПК-6.3 Формулирует требования, предъявляемые к физической защите объекта и пропускному режиму в организации	*Знать* основные требования, предъявляемые к организации защиты информации ограниченного доступа *Уметь:* формулировать требования, предъявляемые к организации защиты информации ограниченного доступа *Владеть (или Иметь опыт деятельности):* навыками формулирования основных требований, предъявляемых к организации защиты информации ограниченного доступа	*Знать* требования, предъявляемые к организации защиты информации ограниченного доступа объекта информатизации *Уметь:* разрабатывать требования, предъявляемые к организации защиты информации ограниченного доступа *Владеть (или Иметь опыт деятельности):* навыками	*Знать* требования, предъявляемые к организации защиты информации ограниченного доступа угрозы безопасности и модели нарушителя объекта информатизации *Уметь:* разрабатывать требования, предъявляемые к организации защиты информации ограниченного доступа *Владеть (или Иметь опыт деятельности):* навыками формулирования требований, предъявляемых к

			формулирования основных требований, предъявляемых к организации защиты информации ограниченного доступа	организации защиты информации ограниченного доступа
	ОПК-6.4 Разрабатывает проекты инструкций, регламентов, положений и приказов, регламентирующих защиту информации ограниченного доступа в организации	Знать: - основные нормативные правовые документы по разработке инструкций, регламентов, положений и приказов, регламентирующих защиту информации ограниченного доступа в организации. Уметь: - ориентироваться в системе законодательства и нормативных правовых актов в области защиты информации. Владеть: - навыками поиска необходимых нормативных и законодательных документов для разработки инструкций, регламентов, положений и приказов.	Знать: - нормативно правовые документы по разработке инструкций, регламентов, положений и приказов, регламентирующих защиту информации ограниченного доступа в организации. Уметь: - использовать нормативно правовые акты при разработке инструкций, регламентов, положений и приказов. Владеть: - навыками поиска необходимых нормативных и законодательных документов и навыками анализа результатов их применения.	Знать: - Российские и международные нормативно правовые документы в области защиты информации. Уметь: - разрабатывать инструкции, регламенты, положения и приказы, регламентирующие защиту информации ограниченного доступа в организации. Владеть: - навыками анализа уязвимостей инструкций, регламентов, положений и приказов, регламентирующих защиту информации ограниченного доступа в организации.
ОПК-12/ завершающий	ОПК-12.3 Оценивает информационные риски в автоматизированных системах.	Знать: классификацию, виды и типы угроз безопасности автоматизированных систем, принципы построения средств защиты информации и возможные риски нарушения безопасности функционирования объекта информатизации. Уметь: определять угрозы безопасности автоматизированных систем, определять возможные риски нарушения безопасности функционирования объекта информатизации. Владеть: навыками анализа	Знать: основные компоненты автоматизированных систем объекта информатизации, состав, структуры и принципы функционирования современных автоматизированных систем, требования основных законов и нормативных документов в области безопасности автоматизированных систем. Уметь: определять состав, структуру и принципы	Знать: методы, способы и методики анализа рисков безопасности автоматизированных систем; классификацию основных источников угроз, комплекс мероприятий, технических мер и методов, направленных на повышение защищенности и снижения рисков нарушения безопасности автоматизированных систем; основные принципы построения комплексной системы защиты автоматизированных систем.

		защищенности автоматизированных систем; навыками защиты информации в компьютерных системах; навыками определения угроз безопасности автоматизированных систем.	функционирования современных автоматизированных систем, анализировать требования основных законов и нормативных документов в области безопасности автоматизированных систем Владеть: навыками выбора средств защиты информации; требованиями основных законов и нормативных документов в области безопасности автоматизированны х систем.	Уметь: применять методики анализа рисков безопасности автоматизированных систем; определять основные источники угроз, принимать технические меры, направленные на повышение защищенности и снижения рисков нарушения безопасности автоматизированных систем. Владеть: методиками анализа рисков безопасности автоматизированных систем и выявления источников угроз; навыками проведения и организации комплекса мероприятий по повышению защищенности и снижению рисков нарушения безопасности автоматизированных систем; навыками построения комплексной системы защиты автоматизированных систем объекта информатизации.
ОПК-4.1/ завершающий	ОПК-4.1.1 Определяет подлежащие защите информационные ресурсы автоматизированных систем	*Знать* основные требования по защите информационных ресурсов и систем. *Уметь:* определять правила и процедуры, реализуемые оператором, для обеспечения защиты информации в информационной системе в ходе ее эксплуатации. *Владеть (или Иметь опыт деятельности):* навыками разработки организационно-распорядительной документации по защите информации.	*Знать* основные требования по защите информационных ресурсов и систем. Методы контроля исполнения правил и процедур для обеспечения защиты информации. *Уметь:* определять правила и процедуры, реализуемые оператором, для обеспечения защиты информации в информационной системе в ходе ее эксплуатации. *Владеть (или Иметь опыт деятельности):*	*Знать* основные требования по защите информационных ресурсов и систем. Методы контроля исполнения правил и процедур для обеспечения защиты информации. *Уметь:* определять правила и процедуры, реализуемые оператором, для обеспечения защиты информации в информационной системе в ходе ее эксплуатации. *Владеть (или Иметь опыт деятельности):* навыками разработки организационно-распорядительной документации по защите информации;

			навыками разработки организационно-распорядительной документации по защите информации.	навыками экспертизы документации, определяющие правила и процедуры, реализуемые оператором для обеспечения защиты информации в информационной системе в ходе ее эксплуатации.
	ОПК-4.1.2 Составляет комплексы правил, процедур, практических приемов, принципов и методов, средств обеспечения защиты информации в автоматизированной системе	*Знать* организационные основы информационной безопасности; основы составления комплексов правил, процедур, практических приемов, принципов и методов обеспечения защиты информации в автоматизированной системе составления *Уметь:* формулировать основные требования для составления правил, процедур, практических приемов, принципов и методов, средств обеспечения защиты информации в автоматизированной системе *Владеть:* навыками конфиденциального документооборота, разработки организационно-распорядительной документации	*Знать* организационные мероприятия информационной безопасности; методы составления комплексов правил, процедур, практических приемов, принципов и методов обеспечения защиты информации в автоматизированной системе составления *Уметь:* формулировать основные требования для составления правил, процедур, практических приемов, принципов и методов, средств обеспечения защиты информации в автоматизированной системе *Владеть:* навыками конфиденциального документооборота, разработки организационно-распорядительной документации	*Знать* организационные мероприятия информационной безопасности; методы составления комплексов правил, процедур, практических приемов, принципов и методов обеспечения защиты информации в автоматизированной системе составления *Уметь:* формулировать требования для составления правил, процедур, практических приемов, принципов и методов, средств обеспечения защиты информации в автоматизированной системе *Владеть:* навыками конфиденциального документооборота, разработки организационно-распорядительной документации, навыками анализа правильности разработанной документации
	ОПК-4.1.3 Организует работу персонала автоматизированной системы с учетом требований по защите информации	*Знать* основные принципы организации работы персонала автоматизированной системы с учетом требований по защите информации. *Уметь:* формулировать задачи для организации работы персонала автоматизированной системы; *Владеть (или Иметь опыт*	*Знать* нормативно-правовые акты в области информационной безопасности и защиты информации. принципы организации работы персонала автоматизированной системы с учетом требований по защите	*Знать* нормативно-правовые акты в области информационной безопасности и защиты информации РФ и др. стран. принципы организации работы персонала автоматизированной системы с учетом требований по защите информации. *Уметь:*

		деятельности): организационно-управленческой работы.	информации. *Уметь:* формулировать задачи для организации работы персонала автоматизированной системы; *Владеть (или Иметь опыт деятельности):* организационно-управленческой работы.	формулировать задачи для организации работы персонала автоматизированной системы; оценивать итоги исполнения поставленных задач перед персоналом. *Владеть (или Иметь опыт деятельности):* организационно-управленческой работы.

7.3Типовые 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 формирования	Оценочные средства		Описание шкал оценивания
				наименование	№№ заданий	
1	2	3	4	5	6	7
1	Структура службы информационной безопасности	ОПК-1, ОПК-5, ОПК-6, ОПК-12, ОПК-4.1	Лекция, СРС, практическое занятие	Вопросы для УО КВЗПР №1	1-4 1-7	Согласно таблице 7.2
2	Функции основных групп службы безопасности	ОПК-1, ОПК-5, ОПК-6, ОПК-12, ОПК-4.1	Лекция, СРС	Вопросы для УО	1-8	Согласно таблице 7.2
3	Цели и задачи службы информационной безопасности	ОПК-1, ОПК-5, ОПК-6, ОПК-12, ОПК-4.1	Лекция, СРС, практическое занятие	Вопросы для УО КВЗПР №2	1-3 1-3	Согласно таблице 7.2
4	Организационные основы и принципы деятельности службы информационной безопасности	ОПК-1, ОПК-5, ОПК-6, ОПК-12, ОПК-4.1	Лекция, СРС, практическое занятие	Вопросы для УО КВЗПР №3	1-7 1-4	Согласно таблице 7.2
5	Лицензировани	ОПК-1,		Вопросы для УО	1-4	Согласно

	е видов деятельности службы безопасности.	ОПК-5, ОПК-6, ОПК-12, ОПК-4.1	Лекция, СРС			таблице 7.2
6	Управление службой защиты информации.	ОПК-1, ОПК-5, ОПК-6, ОПК-12, ОПК-4.1	Лекция, СРС	Вопросы для УО	1-9	Согласно таблице 7.2
7	Организация информационно-аналитической работы.	ОПК-1, ОПК-5, ОПК-6, ОПК-12, ОПК-4.1	Лекция, СРС	Вопросы для УО	17	Согласно таблице 7.2
8	Организация работы с персоналом предприятия.	ОПК-1, ОПК-5, ОПК-6, ОПК-12, ОПК-4.1	Лекция, СРС, практическое занятие	Вопросы для УО КВЗПР №4	1-8 1-3	Согласно таблице 7.2

СРС – самостоятельная работа студента,
КВЗПР – контрольные вопросы для защиты практических работ,

Примеры типовых контрольных заданий для проведения текущего контроля успеваемости

Ситуационные задачи

1. Ваша компания рассматривает возможность перехода на облачные технологии. Ваша задача - провести анализ рисков и предложить конкретные меры для обеспечения безопасности данных и приложений в облачной среде. Какие действия вы будете предпринимать, чтобы выполнить это задание и продемонстрировать свою компетентность в области облачных технологий и безопасности информационных систем?

2. Ваша компания недавно была атакована злоумышленниками, которые украли данные и вымогали выкуп. Ваша задача - разработать стратегию обеспечения безопасности информационных систем компании, чтобы избежать подобных инцидентов в будущем. Какие действия вы будете предпринимать, чтобы выполнить это задание и продемонстрировать свою компетентность в области безопасности информационных систем и управления рисками?

3. Вы работаете в отделе информационной безопасности крупной компании. Ваша задача - разработать и реализовать программу обучения по безопасности информационных систем для всех сотрудников компании. Какие методы обучения и материалы вы будете использовать, чтобы

обеспечить эффективность программы обучения и продемонстрировать свою компетентность в области обучения и безопасности информационных систем?

Вопросы для устного опроса по разделу (теме) 1. «Основные понятия информационной безопасности»:

1. Понятие информационной безопасности.
2. Основные составляющие информационной безопасности.
3. Управление информационной безопасностью.
4. Важность и сложность проблемы информационной безопасности

Контрольные вопросы к практической работе №1 «Определение класса государственной информационной системы (ГИС)»:

1. Какие функции выполняет СЗИ предприятия для решения задач защиты информации?
2. Как строится структура полномасштабной системы обеспечения безопасности и защиты информации предприятия?
3. Какова специфика организации и выполнения охранных функций?
4. Каковы суть и содержание нормативной основы организации ЗСИ?
5. Какие факторы влияют на формирование организационно-правового обеспечения защиты информации?
6. Какова структура организационно-правовой основы защиты информации?

Полностью оценочные материалы и оценочные средства для проведения текущего контроля успеваемости представлены в УММ по дисциплине.

Типовые задания для проведения промежуточной аттестации обучающихся

Промежуточная аттестация по дисциплине проводится в форме экзамена. Экзамен проводится в виде бланкового 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.

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:

Что включают в себя системы управления ИБ?

A. Политика, планирование, должностные обязанности, процедуры, процессы и ресурсы.

B. Организационную структуру, политики, планирование, должностные обязанности, практики,

C. Организационную структуру, политики, планирование, должностные обязанности, практики.

D. Организационную структуру, политики, планирование, должностные обязанности, практики, процедуры, процессы и ресурсы.

E. Организационную структуру, политики, должностные обязанности, практики, процессы и ресурсы.

Задание в открытой форме:

1. Основными принципами политики безопасности являются…

2. Политика безопасности верхнего уровня включает…

3. Удаленный доступ к сервису организован…

4.Системный подход к защите информации базируется на принципах…

Задание на установление правильной последовательности.

Установить действия этапа анализа рисков:

1. Оценка вероятности того, что угроза будет реализована на практике

2. Оценка рисков технологических и информационных активов

3. Идентификация и оценка стоимости технологических и информационных активов

4. Анализ угроз, для которых технологические и информационные активы являются целевым объектом

Задание на установление соответствия:
между средствами и функциями

1	Человек, информация, технические средства	А	Информационное оружие
2	Целенаправленное производство и распространение специальной информации, оказывающей непосредственное влияние на функционирование и развитие психологической среды общества, психику и поведение населения, руководства страны, военнослужащих	Б	Информационное воздействие
3	Комплекс технических средств и технологий, предназначенных для получения контроля над информационными ресурсами потенциального противника в целях выведения их из строя, получения или модификации содержащихся в них данных, целенаправленного продвижения выгодной информации (или дезинформации)	В	Элементы информационного пространства
4	Применение средств, позволяющих производить с передаваемой, обрабатываемой, создаваемой, уничтожаемой и воспринимаемой информацией задуманные действия	Г	Психологическое воздействие

Компетентностно-ориентированная задача:

В Курской области создается Комитет Курской области по контролю успеваемости учащихся образовательных организациях Курской области (выделяется часть функций из комитета образования и науки).

В рамках комитета создается автоматизированная система внутренней работы. Все сотрудники должны иметь автоматизированные рабочие места.

Структура комитета:

Руководитель – 1

Заместитель руководителя по внутренней работе – 1

Заместитель руководителя по контролю успеваемости – 1

Отдел кадров – 1

Бухгалтерия – 2

Отдел контроля успеваемости – 5

Отдел автоматизации деятельности – 1

Комитет занимает 8 помещений на 1 этаже (схема составляется самостоятельно), возможен прием посетителей.

Примерный бюджет на всю информатизацию и защиту информации 2,5 млн. руб.

Должен быть создан банк данных успеваемости, при этом имеется разработчик специального ПО, который реализует интерфейсную часть по необходимым требованиям с учетом выбранной аттестуемым СУБД. СУБД

интегрируется с порталом госуслуг. Ввод данных осуществляется путем выгрузки данных из действующей системы Аверс по каналу связи.

Руководитель и заместители должны иметь доступ ко всей информации и Интернет, отдел контроля – только к ИС контроля, бухгалтерия и отдел кадров – только к ресурсу кадров и бухгалтерии, а так же к АС бюджетная система и закупки.

Деятельность бухгалтерии – стандартная, база данных 1С совмещена с отделом кадров.

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 02.016–2018 Обалльно-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
1	2	3	4	5
Практическая работа №1	3	Выполнил, доля правильных ответов от 50% до 90%	6	Выполнил, доля правильных ответов более 90%
Практическая работа №2	3	Выполнил, доля правильных ответов от 50% до 90%	6	Выполнил, доля правильных ответов более 90%

Практическая работа №3	3	Выполнил, доля правильных ответов от 50% до 90%	6	Выполнил, доля правильных ответов более 90%
Практическая работа №4	3	Выполнил, доля правильных ответов от 50% до 90%	6	Выполнил, доля правильных ответов более 90%
Устный опрос по темам 1-9	6	Доля правильных ответов от 50% до 90%	12	Доля правильных ответов более 90%
Решение ситуационных задач	6	Выполнил, доля правильных ответов от 50% до 90%	12	Выполнил, доля правильных ответов более 90%
Итого	24		48	
Посещаемость	0		16	
Зачёт	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. Технологии обеспечения безопасности информационных систем : учебное пособие / А. Л. Марухленко, Л. О. Марухленко, М. А. Ефремов и др. – Москва ; Берлин : Директ-Медиа, 2021. – 210 с. – URL: https://biblioclub.ru/index.php?page=book&id=598988 (дата обращения: 02.09.2022). – Режим доступа: по подписке. – Текст : электронный.

2. Корнилова, А. А. Защита персональных данных : учебное пособие / А. А. Корнилова, Д. С. Юнусова, А. С. Исмагилова ; Башкирский государственный университет. – Уфа : Башкирский государственный университет, 2020. – 119 с. –

URL: https://biblioclub.ru/index.php?page=book&id=611314 (дата обращения: 02.09.2022). – Режим доступа: по подписке. – Текст : электронный.

3. Арзуманян, А. Б. Международные стандарты правовой защиты информации и информационных технологий : учебное пособие / А. Б. Арзуманян ; Южный федеральный университет. – Ростов-на-Дону ; Таганрог : Южный федеральный университет, 2020. – 140 с. – URL: https://biblioclub.ru/index.php?page=book&id=612162 (дата обращения: 02.09.2022). - Режим доступа: по подписке. – Текст : электронный.

8.2 Дополнительная учебная литература

4. Информационная безопасность в цифровом обществе : учебное пособие / А. С. Исмагилова, И. В. Салов, И. А. Шагапов, А. А. Корнилова ; Башкирский государственный университет. – Уфа : Башкирский государственный университет, 2019. – 128 с. – URL: https://biblioclub.ru/index.php?page=book&id=611084 (дата обращения: 02.09.2022). - Режим доступа: по подписке. Текст : электронный.

5. Мицук, С. В. Защита и обработка конфиденциальных документов: виды тайн : учебное пособие / С. В. Мицук ; Липецкий государственный педагогический университет им. П. П. Семенова-Тян-Шанского. – Липецк : Липецкий государственный педагогический университет имени П.П. Семенова-Тян-Шанского, 2017. – 62 с. – URL: https://biblioclub.ru/index.php?page=book&id=577437 (дата обращения: 02.09.2022). - Режим доступа: по подписке. – Текст : электронный.

8.3 Перечень методических указаний

1. Основы управления информационной безопасностью: методические указания по выполнению практических работ / Юго-Зап. гос. ун-т; сост.: Е.А. Кулешова. – Курск, 2023. – 26 с.: Библиогр.: с. 26.

2. Основы управления информационной безопасностью: методические указания для самостоятельной работы / Юго-Зап. гос. ун-т; сост.: Е.А. Кулешова. – Курск, 2023. – 56 с.: Библиогр.: с. 57.

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

1. http://e.lanbook.com - Электронно-библиотечная система «Лань».
2. http://www.iqlib.ru - Электронно-библиотечная система IQLib.
3. http://window.edu.ru -Электронная библиотека «Единое окно доступа к образовательным ресурсам».

4. http://biblioclub.ru – Электронно-библиотечная система «Университетская библиотека онлайн».

5. http://www.fsb.ru - Федеральная служба безопасности [официальный сайт].

6. http://fstec.ru - Федеральная служба по техническому и экспортному контролю [официальный сайт].

7. http://microsoft.com - Корпорация Microsoft[официальный сайт].

8. http://www.consultant.ruКомпания«Консультант Плюс» [официальный сайт].

10. Методические указания для обучающихся по освоению дисциплины

Основными видами аудиторной работы студента при изучении дисциплины «Основы управления информационной безопасностью» являются лекции и практические занятия. 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 занятия, 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.

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

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

Преподаватель уже на первых занятиях объясняет студентам, какие формы обучения следует использовать при самостоятельном изучении дисциплины: 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, промежуточный контроль путем отработки студентами пропущенных лекций, участие в групповых и индивидуальных консультациях (собеседованиях). Эти формы способствуют выработке у студентов умения работать с учебником и литературой. Изучение литературы и справочной документации 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 немыслима 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 усвоению учебного материала. В случае необходимости студенты обращаются за консультацией к преподавателю по вопросам дисциплины с целью усвоения и закрепления компетенций.

Основная цель самостоятельной работы студента при изучении дисциплины - 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)

MicrosoftOffice 2016.Лицензионный договор №S0000000722 от 21.12.2015 г. с ООО «АйТи46», лицензионный договор №К0000000117 от 21.12.2015 г. с ООО «СМСКанал»,

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

Windows 7, договор IT000012385

Антивирусная программа Kaspersky Internet Security.

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

Учебная аудитория для проведения занятий лекционного типа и лаборатории кафедры информационной безопасности, оснащенные учебной мебелью: столы, стулья для обучающихся; стол, стул для преподавателя; доска. Компьютеры (10шт) CPU AMD-Phenom, ОЗУ 16 GB, HDD 2 Tb, монитор Aok 21”. Проекционный экран на штативе; Мультимедиацентр: ноут-букASUSX50VLPMD-T2330/14"/1024Mb/160Gb/сумка/проекторinFocusIN24+

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. 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, прочитать 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
	Изме-нённых	Заменённых	Аннулированных	новых			