Аннотация к рабочей программе дисциплины «Планирование и управление инфомационной безопасностью»

Цель преподавания дисциплины

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

Задачи изучения дисциплины

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

Компетенции, формируемые в результате освоения дисциплины

Способность осуществлять анализ научно-технической информации, нормативных и методических материалов по методам обеспечения информационной безопасности телекоммуникационных систем (ПК-1);

Способность участвовать в проведении аттестации телекоммуникационных систем по требованиям защиты информации (ПК-9);

Способность применять нормативные правовые акты в своей профессиональной деятельности (ОПК-7).

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. 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
Т.А. Ширабакина
(подпись, инициалы, фамилия)
«01» 02 2017 г

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Планирование и управление информационной безопасностью
(наименование дисциплины)

направление подготовки (специальность) 10.05.02
(шифр согласно ФГОС
Информационная безопасность телекоммуникационных систем
и наименование направление подготовки (специальности)

Защита информации в системах связи и управления
наименование профиля, специализации или магистерской программы)

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

Курск – 2017

Рабочая программа составлена в соответствии с Федеральным государственным образовательным стандартом высшего образования специальности подготовки 10.05.02 Информационная безопасность телекоммуникационных систем и на основании учебного плана специальности подготовки 10.05.02 Информационная безопасность телекоммуникационных систем (специализация Защита информации в системах связи и управления), одобренного Учёным советом университета, протокол № 5 «30» 01 2017 г.

Рабочая программа обсуждена и рекомендована к применению в учебном процессе для обучения студентов по специальности подготовки 10.05.02 Информационная безопасность телекоммуникационных систем на заседании кафедры информационной безопасности № «9» 01.02 2017г.

Зав. кафедрой ИБ Таныгин М.О.
Разработчик программы
доцент кафедры ИБ Спеваков А.Г.

Директор научной библиотеки Макаровская В.Г.

Рабочая программа пересмотрена, обсуждена и рекомендована к применению в образовательном процессе на основании учебного плана специальности подготовки 10.05.02 Информационная безопасность телекоммуникационных систем, одобренного Ученым советом университета протокол № 5 «30» 01 2017г. на заседании кафедры информационной безопасности 27.01.18
(наименование кафедры, дата, номер протокола)

Зав. кафедрой Таныгин М.О.

Рабочая программа пересмотрена, обсуждена и рекомендована к применению в образовательном процессе на основании учебного плана специальности подготовки 10.05.02 Информационная безопасность телекоммуникационных систем, одобренного Ученым советом университета протокол № 5 «30» 01 2017г. на заседании кафедры ИБ, протокол №12 от 29.06.18 г.
(наименование кафедры, дата, номер протокола)

Зав. кафедрой Таныгин М.О.

Рабочая программа пересмотрена, обсуждена и рекомендована к применению в образовательном процессе на основании учебного плана специальности подготовки 10.05.02 Информационная безопасность телекоммуникационных систем, одобренного Ученым советом университета протокол № « » 20 г. на заседании кафедры информационной безопасности 27.06.2019 №11
(наименование кафедры, дата, номер протокола)

Зав. кафедрой к.т.н доцент Таныгин М.О

Программа пересмотрена, обсуждена и рекомендована к применению в образовательном процессе на основании учебного плана направления подготовки *10.05.02 – «Информационная безопасность телекоммуникационных систем»*, одобренного Ученым советом университета протокол №_7_ «_25_» _02_ 20_20_ г. на заседании кафедры информационной безопасности. Протокол №_1_ от «_31_» _08_ 20_20_г.

Зав. кафедрой _____

Программа пересмотрена, обсуждена и рекомендована к применению в образовательном процессе на основании учебного плана направления подготовки *10.05.02 – «Информационная безопасность телекоммуникационных систем»*, одобренного Ученым советом университета протокол №_7_ «_25_» _02_ 20_20_ г. на заседании кафедры информационной безопасности. Протокол №_11_ от «_28_» _06_ 20_21_г.

Зав. кафедрой _____

Программа пересмотрена, обсуждена и рекомендована к применению в образовательном процессе на основании учебного плана направления подготовки *10.05.02 – «Информационная безопасность телекоммуникационных систем»*, одобренного Ученым советом университета протокол №_7_ «_25_» _02_ 20_20_ г. на заседании кафедры информационной безопасности. Протокол №_11_ от «_30_» _06_ 20_22_г.

Зав. кафедрой _____

Программа пересмотрена, обсуждена и рекомендована к применению в образовательном процессе на основании учебного плана направления подготовки *10.05.02 – «Информационная безопасность телекоммуникационных систем»*, одобренного Ученым советом университета протокол №__ «___» _____ 20__ г. на заседании кафедры информационной безопасности. Протокол №__ от «__»_____20__г.

Зав. кафедрой _____

Программа пересмотрена, обсуждена и рекомендована к применению в образовательном процессе на основании учебного плана направления подготовки *10.05.02 – «Информационная безопасность телекоммуникационных систем»*, одобренного Ученым советом университета протокол №__ «___» _____ 20__ г. на заседании кафедры информационной безопасности. Протокол №__ от «__»_____20__г.

Зав. кафедрой _____

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

1.1. Цель дисциплины

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

1.2. Задачи дисциплины

– 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 службы защиты информации

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

Обучающиеся должны **знать:**

– организацию судебных, правоприменительных и правоохранительных органов;

– правовые нормы действующего законодательства, регулирующие отношения в различных сферах жизнедеятельности;

– основные положения и нормы конституционного, гражданского, семейного, трудового, административного и уголовного права;

– основные нормативные правовые документы;

– информационные технологии в системе информационно-аналитического обеспечения безопасности;

– систему мер противодействия промышленному шпионажу;

– активные и пассивные методы сбора информации;

– составные части информационно-вычислительной сети-аппаратное и программное обеспечение, подлежащее защите;

уметь:

– использовать нормативно-правовые знания в различных сферах жизнедеятельности;

– ориентироваться в системе законодательства и нормативных правовых актов, регламентирующих сферу профессиональной деятельности;

– определять направления актуализации системы защиты информации в соответствии с текущими деловыми потребностями фирмы и выявленным уровнем уязвимости защищаемой информации;

– разрабатывать и применять технологии обработки больших информационных потоков финансовой и экономической информации в режиме реального времени;

– структурировать информационные ресурсы в соответствии с их ценностью и полезностью, определять необходимость их защиты от несанкционированного доступа;

– работать с методической литературой и вырабатывать управленческие решения в области информационной безопасности;

владеть :

– поиска необходимых нормативных и законодательных документов и навыками работы с ними в профессиональной деятельности;

– применения нормативных правовых документов в своей деятельности; - навыками работы с информацией из различных источников;

– навыками изучения и обобщения опыта работы других учреждений, организаций и предприятий в области повышения эффективности защиты информации и сохранения государственной и других видов тайны;

У обучающихся формируются следующие компетенции:

– способность осуществлять анализ научно-технической информации, нормативных и методических материалов по методам обеспечения информационной безопасности телекоммуникационных систем (ПК-1);

– способность участвовать в проведении аттестации телекоммуникационных систем по требованиям защиты информации (ПК-9);

– способность применять нормативные правовые акты в своей профессиональной деятельности (ОПК-7).

2. Указание места дисциплины в структуре образовательной программы

«Планирование и управление информационной безопасностью» представляет дисциплину с индексом Б1.Б.41 базовой части учебного плана специальности 10.05.02 Информационная безопасность телекоммуникационных систем. Изучается на 5 курсе в 10 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 – Объём дисциплины

Виды учебной работы	Всего, часов
Общая трудоемкость дисциплины	108
Контактная работа обучающихся с преподавателем (по видам учебных занятий) (всего)	54
в том числе:	
лекции	18
лабораторные занятия	0
практические занятия	36
Самостоятельная работа обучающихся (всего)	53,9
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	Организация деятельности службы безопасности Правовое обеспечение службы. Принципы организации службы. Гарантии безопасности объектов защиты Пакет документов

	информационной безопасности	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 ее методическое обеспечение

№ п/п	Раздел (тема) дисциплины	Виды деятельности			Учебно-методические материалы	Формы текущего контроля успеваемости *(по неделям семестра)*	Компетенции
		лек., час	№ пр.	№ лб.			
1	2	3	4	5	6	7	8
1.	Структура службы информационной безопасности	2	1		У 1-5 МУ 1-2	УО, ЗПР, СЗ – 1-3	ПК-1, ПК-9
2.	Функции основных групп службы безопасности	2	2		У 1-5 МУ 1-2	УО, ЗПР – 4-6	ПК-1, ПК-9, ОПК-7
3.	Цели и задачи службы информационной безопасности	2			У 1-5 МУ 1-2	УО – 7-8	ПК-1, ПК-9, ОПК-7
4.	Организационные основы и принципы деятельности службы информационной безопасности	2			У 1-5 МУ 1-2	УО – 9-10	ПК-1, ПК-9, ОПК-7
5.	Лицензирование видов деятельности службы безопасности.	2	3		У 1-5 МУ 1-2	УО, ЗПР, СЗ – 11-12	ПК-1, ПК-9, ОПК-7
6.	Управление службой защиты информации.	4			У 1-5 МУ 1-2	УО – 13-14	ПК-1, ПК-9, ОПК-7
7.	Организация информационно-аналитической работы.	2			У 1-5 МУ 1-2	УО – 15-16	ПК-1, ПК-9, ОПК-7
8.	Организация работы с персоналом предприятия.	2	4		У 1-5 МУ 1-2	УО, ЗПР, СЗ – 17-18	ПК-1, ПК-9, ОПК-7

УО – устный опрос, ЗПР – защита практической работы, СЗ – ситуационная задача

4.2 Лабораторные работы и (или) практические занятия

4.2.1 Практические работы

Таблица 4.3 – Практические занятия

№	Наименование практической работы	Объем, час.
1.	Определение класса государственной информационной системы (ГИС)	6
2.	Разработка структуры государственных и международных стандартов в Российской Федерации в области информационной безопасности и защиты информации	6
3.	Техническое задание на создание информационной системы и системы защиты информации	12
4.	Основные методы управления информационной безопасностью в ГИС	12
Итого		36

4.3. Самостоятельная работа студентов (СРС)

Таблица 4.4 – Самостоятельная работа студентов

№	Наименование раздела учебной дисциплины	Срок выполнения	Время, затрачиваемое на выполнение СРС, час.
1.	Структура службы информационной безопасности	1-2 неделя	9
2.	Функции основных групп службы безопасности	3-4 неделя	9
3.	Цели и задачи службы информационной безопасности	5-6 неделя	9
4.	Организационные основы и принципы деятельности службы информационной безопасности	7-8 неделя	9
5.	Лицензирование видов деятельности службы безопасности.	9-10 неделя	9
6.	Управление службой защиты информации.	11-14 неделя	9
7.	Организация информационно-аналитической работы.	15-16 неделя	9
8.	Организация работы с персоналом предприятия.	17-18неделя	8,9
Итого			53,9

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;

– вопросов к зачету;

–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

В соответствии с требованиями ФГОС и Приказа Министерства образования и науки РФ от 19 декабря 2013 г. № 1367 реализация компетентностного подхода предусматривает широкое использование в образовательном процессе активных и интерактивных форм проведения занятий в сочетании с внеаудиторной работой с целью формирования и развития профессиональных навыков студентов. Удельный вес занятий, проводимых в интерактивных формах, 33,3 процента от аудиторных занятий согласно УП. Средствами промежуточного контроля успеваемости студентов являются опросы на практических занятиях по темам лекций.

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

№	Наименование раздела (темы лекции, практического или лабораторного занятия)	Используемые интерактивные образовательные технологии	Объём, час.
1.	Выполнение практической работы №1	Разбор конкретных ситуаций	6
2.	Выполнение практической работы №3	Разбор конкретных ситуаций	6
3.	Выполнение практической работы №4	Разбор конкретных ситуаций	6
	Итого		18

7. Фонд оценочных средств для проведения промежуточной аттестации обучающихся по дисциплине

7.1 Перечень компетенций с указанием этапов их формирования в процессе освоения образовательной программы

Таблица 7.1 – Этапы формирования компетенций

Код и содержание компетенции	Этапы* формирования компетенций и дисциплины (модули), при изучении которых формируется данная компетенция		
	начальный	основной	завершающий
1	2	3	4
Способность использовать нормативные правовые акты в профессиональной деятельности (ОПК-7)	Инженерная графика		Организационное и правовое обеспечение информационной безопасности Преддипломная практика
Способность осуществлять анализ научно-технической информации, нормативных и методических материалов по методам обеспечения информационной безопасности телекоммуникационных систем (ПК-1)	Русский язык и культура речи Практика по получению первичных профессиональных умений, в том числе первичных умений и навыков научно-исследовательской деятельности Учебно-лабораторный практикум	Информационная безопасность телекоммуникационных систем Основы информационной безопасности Основы криптографии Основы теории чисел Научно-исследовательская работа	Информационная безопасность телекоммуникационных систем Планирование и управление информационной безопасностью Основы многоканальных систем передачи Системы и сети радиосвязи Системы и сети мобильной связи Практика по получению профессиональных умений и опыта профессиональной деятельности Преддипломная Практика
Способность участвовать в проведении аттестации телекоммуникационных систем по требованиям защиты информации (ПК-9)	Измерения в телекоммуникационных системах		Планирование и управление информационной безопасностью Основы мониторинга безопасности инфокоммуникационных систем и сетей Система сертификации и аттестации телекоммуникационных систем Порядок проведения аттестации объектов

		информатизации Технологическая практика

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

Таблица 7.2 – Показатели и критерии оценивания компетенций, шкала оценивания

Код компетенции/ этап *(указывается название этапа из п.7.1)*	Показатели оценивания компетенций	Критерии и шкала оценивания компетенций		
		Пороговый уровень («удовлетворительно)	Продвинутый уровень (хорошо»)	Высокий уровень («отлично»)
1	2	3	4	5
ОПК-7/ завершающий	*1.Доля освоенных обучающимся знаний, умений, навыков от общего объема ЗУН, установленных в п.1.3РПД* *2.Качество освоенных обучающимся знаний, умений, навыков* *3.Умение применять знания, умения, навыки в типовых и нестандартных ситуациях*	Знать: -методологию исследовательской деятельности, основные проблемы в области информационной безопасности; Уметь: - определять программу проведения исследований, Владеть: - планированием исследовательской деятельности и определением целесообразных методов для решения поставленных в исследовании задач	Знать: - основы культуры научного исследования в информационной безопасности, Уметь: - использовать и применять их в современных информационно-коммуникационных технологиях Владеть: - способностью к критическому анализу результатов научного творчества	Знать: - основные положения и методы социальных, гуманитарных и экономических наук при решении педагогических задач Уметь: - использовать теоретический материал в педагогической, научно-исследовательской, творческой, управленческой деятельностях Владеть: -организационными формами и методами проведения научных исследований;
ПК-1/ завершающий	*1.Доля освоенных обучающимся знаний, умений, навыков от общего объема*	Знать: порядок формирования службы защиты информации на предприятии Уметь: работать с нормативными	Знать: требования к обеспечению функционирования службы защиты информации. Уметь: проектировать	Знать: полный перечень действий по созданию службы защиты информации. Уметь: проектировать и

Код компетенции/ этап *(указывается название этапа из п.7.1)*	Показатели оценивания компетенций	Критерии и шкала оценивания компетенций		
		Пороговый уровень («удовлетворительно)	Продвинутый уровень (хорошо»)	Высокий уровень («отлично»)
1	2	3	4	5
	ЗУН, установленных в п.1.3РПД *2.Качество освоенных обучающимся знаний, умений, навыков* *3.Умение применять знания, умения, навыки в типовых и нестандартных ситуациях.*	документами регуляторов в области информационной безопасности Владеть навыками: анализа нормативных требований регуляторов	технологический процесс обеспечения информационной безопасности. Владеть навыками: составления проектов организации службы защиты информации;	реализовывать технологический процесс обеспечения информационной безопасности на предприятии; Владеть навыками: организации службы защиты информации
ПК-9/ завершающий	*1.Доля освоенных обучающимся знаний, умений, навыков от общего объема ЗУН, установленных в п.1.3РПД* *2.Качество освоенных обучающимся знаний, умений, навыков* *3.Умение применять знания, умения, навыки в типовых и нестандартных ситуациях.*	Знать: общие принципы лицензирования и сертификации в области ИБ Уметь: определять перечень действий для проведения анализа ИБ Владеть навыками: Участия в анализе требований регуляторов в области ИБ;	Знать: порядок проведения лицензирования и аттестации Уметь: определять несоответсвия между текущим состоянием объекта информатизации и требованиями регуляторов в области ИБ; Владеть навыками: Анализа информационных систем на предмет соответствия нормативно-правовым документам	Знать: требования к лицензиатам и сертифицированным объектам Уметь: сопоставлять текущую структуру предприятия требованиям регуляторов в области ИБ; Владеть навыками: Формирования программ лицензирования и сертификации;

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 образовательной программы

Таблица 7.3 – Паспорт комплекта оценочных средств для текущего контроля

№ п/п	Раздел (тема) дисциплины	Код контролируемой компетенции (или её части)	Технология форматирования	Оценочные средства		Описание шкал оценивания
				наимено-вание	№ заданий	
1	2	3	4	5	6	7
1	Структура службы информационной безопасности	ПК-1, ПК-9	Лекция, СРС, практическая работа	Вопросы для УО КВЗПР РСЗ	1-10 1-10 1-15	Согласно табл. 7.2
2	Функции основных групп службы безопасности	ПК-1, ПК-9, ОПК-7	Лекция, СРС, практическая работа	Вопросы для УО КВЗПР	1-10 1-10	Согласно табл. 7.2
3	Цели и задачи службы информационной безопасности	ПК-1, ПК-9, ОПК-7	Лекция, СРС,	Вопросы для УО	1-10	Согласно табл. 7.2
4	Организационные основы и принципы деятельности службы информационной безопасности	ПК-1, ПК-9, ОПК-7	Лекция, СРС	Вопросы для УО	1-10	Согласно табл. 7.2
5	Лицензирование видов деятельности службы безопасности	ПК-1, ПК-9, ОПК-7	Лекция, СРС, практическая работа	Вопросы для УО КВЗПР РСЗ	1-10 1-10 1-15	Согласно табл. 7.2
6	Управление службой защиты информации.	ПК-1, ПК-9, ОПК-7	Лекция, СРС	Вопросы для УО	1-10	Согласно табл. 7.2
7	Организация информационно-аналитической работы.	ПК-1, ПК-9, ОПК-7	Лекция, СРС	Вопросы для УО	1-10	Согласно табл. 7.2
8	Организация работы с персоналом предприятия.	ПК-1, ПК-9, ОПК-7	Лекция, СРС, практическая работа	Вопросы для УО КВЗПР РСЗ	1-10 1-10 1-15	Согласно табл. 7.2

КВЗПР – контрольные вопросы для защиты практических работ, РСЗ – решение ситуационной задачи

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?

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 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.

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 (по вариантам).

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 также 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 «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	2	Выполнил, доля правильных ответов от 50% до 90%	4	Выполнил, доля правильных ответов более 90%
Выполнение практической работы №2	2	Выполнил, доля правильных ответов от 50% до 90%	4	Выполнил, доля правильных ответов более 90%
Выполнение практической работы №3	2	Выполнил, доля правильных ответов от 50% до 90%	4	Выполнил, доля правильных ответов более 90%
Выполнение практической работы №4	2	Выполнил, доля правильных ответов от 50% до 90%	4	Выполнил, доля правильных ответов более 90%
Устный опрос по теме 1	1	Доля правильных ответов от 50% до 90%	2	Доля правильных ответов более 90%

Устный опрос по теме 2	1	Доля правильных ответов от 50% до 90%	2	Доля правильных ответов более 90%
Устный опрос по теме 3	1	Доля правильных ответов от 50% до 90%	2	Доля правильных ответов более 90%
Устный опрос по теме 4	1	Доля правильных ответов от 50% до 90%	2	Доля правильных ответов более 90%
Устный опрос по теме 5	1	Доля правильных ответов от 50% до 90%	2	Доля правильных ответов более 90%
Устный опрос по теме 6	1	Доля правильных ответов от 50% до 90%	2	Доля правильных ответов более 90%
Устный опрос по теме 7	1	Доля правильных ответов от 50% до 90%	2	Доля правильных ответов более 90%
Устный опрос по теме 8	1	Доля правильных ответов от 50% до 90%	2	Доля правильных ответов более 90%
Решение ситуационных задач	8	Выполнил, доля правильных ответов от 50% до 90%	16	Выполнил, доля правильных ответов более 90%
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 –2балла,
- 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.

8.2 Дополнительная литература

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.

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.

8.2 Перечень методических указаний

1. Планирование и управление 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. Планирование и управление информационной безопасностью: методические указания для самостоятельной работы / Юго-Зап. гос. ун-т; сост.: Е.А. Кулешова. – Курск, 2023. – 57 с.: Библиогр.: с. 57.

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 ВИНИТИ РАН [официальный сайт]. Режим доступа: http://www.consultant.ru/
6) База данных "Патенты России"
7) Аналитический раздел комании «Код Безопасности» https://www.securitycode.ru/documents/analytics/

10. Методические указания для обучающихся по освоению дисциплины

Основными видами аудиторной работы студента при изучении дисциплины «Планирование и управление информационной безопасностью» 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.

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 «Планирование и управление информационной безопасностью»: 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 лекции, 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 закрепление 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 «Планирование и управление информационной безопасностью» с целью усвоения и закрепления компетенций.

Основная цель самостоятельной работы студента при изучении дисциплины «Планирование и управление информационной безопасностью» - 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

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/l 7 TFT E700 (6 шт).

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
	измененных	заменённых	аннулированных	новых			