Автономная некоммерческая образовательная организация
высшего образования
«КАЛИНИНГРАДСКИЙ ИНСТИТУТ УПРАВЛЕНИЯ»

Утверждено
Научно-методическим советом Института
протокол заседания
№ 10/23 от 29 мая 2024 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ РОССИИ (Б1.В.ОД.12)

Направление подготовки	**38.04.04. Государственное и муниципальное управление**
Направленность	**Национальная безопасность**
Квалификация (степень) выпускника (уровень направления подготовки)	**Магистр**
Форма обучения	**очная, очно-заочная, заочная**

Калининград

2024

Автономная некоммерческая образовательная организация высшего образования

«Калининградский институт управления»

Лист актуализации Б1.В.ОД.12 Информационная безопасность России
(наименование РПД с шифром)

Направление: 38.04.04 Государственное и муниципальное управление
Направленность: «Национальная безопасность»

В целях актуализации основной профессиональной образовательной программы обновлена основная и дополнительная литература

Разработчик: к.ю.н., доцент Минаев А.В. 29.05.24г
(ФИО, ученая степень, ученое звание) (дата)

Изменения (дополнения) в рабочую программу рассмотрены и утверждены на заседании научно-методического совета, протокол № 10/23 от 29 мая 2024 г.

СОГЛАСОВАНО:

Руководитель ОПОП Минаев А.В.

Начальник
отдела оценки качества образования Переляева А.М.

29 мая 2024 г.

М.П.

Лист согласования рабочей программы дисциплины

Рабочая программа дисциплины «Информационная безопасность России» разработана в соответствии с Федеральным законом от 29 декабря 2012 года №273-ФЗ «Об образовании в Российской Федерации»; Федеральным государственным образовательным стандартом по направлению подготовки 38.04.04 «Государственное и муниципальное управление» (уровень магистратура), утвержденный приказом Минобрнауки России от 13 августа 2020 г. № 1000

Составитель (автор) канд. юр. наук А.В. Минаев

Рабочая программа дисциплины рассмотрена и одобрена на заседании Научно-методического совета института, протокол № 10/23 от 29 мая 2024 г.

Регистрационный номер 20Гм/22

Содержание Стр.

1. Цели и задачи освоения дисциплины

Для направления 38.04.04 «Государственное и муниципальное управление» подготовки магистра дисциплина «Информационная безопасность России» является обязательной дисциплиной

Целями освоения дисциплины «Информационная безопасность России» является овладение знаниями в области базовых понятий и подходов теории безопасности, овладение умением сравнивать доктрины безопасности, владеть методикой составления прогнозов в соответствии с требованиями ФГОС ВО по направлению подготовки 38.04.04 «Государственное и муниципальное управление», направленность Национальная безопасность.

Изучение дисциплины «Информационная безопасность России» базируется на следующих дисциплинах:

Правовое обеспечение национальной безопасности

Экономическая и финансовая безопасность

Социально-политическая безопасность России

Основные положения дисциплины «Информационная безопасность России» используются в дальнейшем при изучении следующих дисциплин:

Экологическая и техногенная безопасность России

Стратегическое планирование и прогнозирование в области национальной безопасности

Программа составлена в соответствии с требованиями Федерального закона № 273-ФЗ «Об образовании в Российской Федерации», Приказа Министерства науки и высшего образования РФ от 06.04.2021 г. № 245 «Об утверждении Порядка организации и осуществления образовательной деятельности по образовательным программам высшего образования - программам бакалавриата, программам специалитета, программам магистратуры», ФГОС ВО и учебным планом по направлению подготовки38.04.04 «Государственное и муниципальное управление».

2. Место дисциплины в структуре ОПОП

2.1. Указание места дисциплины в структуре образовательной программы.

Дисциплина дисциплины «Информационная безопасность России» относится к блоку обязательных дисциплин вариативной части. Содержание дисциплины «Информационная безопасность России» соотносится с курсами «Правовое обеспечение национальной безопасности», «Экономическая и финансовая безопасность», «Социальная безопасность России».

Изучаются международные стандарты информационного обмена. Понятие угрозы, информационная безопасность в условиях функционирования в России глобальных сетей, виды противников или «нарушителей», понятие о видах вирусов, три вида возможных нарушений информационной системы. Защита, основные нормативные руководящие документы, касающиеся государственной тайны, нормативно-справочные документы, назначение и задачи в сфере обеспечения информационной безопасности на уровне государства, основные положения теории информационной безопасности. Модели безопасности и их применение, таксономия нарушений информационной безопасности вычислительной системы и причины, обуславливающие их существование, анализ способов нарушений информационной безопасности, использование защищенных компьютерных систем, методы криптографии, основные технологии построения защищенных систем, место информационной безопасности экономических систем в национальной безопасности страны.

Изучение данной дисциплины начинается с четвертого семестра второго курса.

Дисциплина «Информационная безопасность России» входит в блок обязательных дисциплин вариативной части Б1.В.ОД.12 учебного плана АНООВО «КИУ» по направлению подготовки 38.04.04 «Государственное и муниципальное управление».

Изучение дисциплины необходимо строить с учетом междисциплинарных связей с дисциплинами «Экологическая и техногенная безопасность России», «Стратегическое планирование и прогнозирование в области национальной безопасности».

Дисциплины, для которых изучение данной дисциплины необходимы как предшествующее «Правовое обеспечение национальной безопасности», «Экономическая и финансовая безопасность», «Социально-политическая безопасность России».

2.2. Календарный график формирования компетенции*

Таблица - 1 Календарный график формирования компетенции ПК-2

№ п/п	Наименование учебных дисциплин и практик, участвующих в формировании компетенции	1	2	3	4
1	Правовое обеспечение национальной безопасности			+	
2	Экономическая и финансовая безопасность России			+	
3	Социально-политическая безопасность России			+	
4	Информационная безопасность России				+
5	Стратегическое планирование и прогнозирование в области национальной безопасности				+
6	Экологическая и техногенная безопасность России				+
7	*Преддипломная практика*				+

* В соответствии с матрицей компетенций

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

Основное базовое понятие, используемое в дисциплине, это «безопасность». Под безопасностью понимается состояние общественных отношений, при котором личность, социальная группа, общность, народ, страна (государство) может самостоятельно, суверенно, без вмешательства и давления извне свободно выбирать и осуществлять свою стратегию международного поведения, духовного, социально-экономического и политического развития.

Для формирования профессиональной компетенции, подразумевающей способность использовать в профессиональной деятельности информационно-коммуникационные технологии, государственные и муниципальные информационные системы; применять технологии электронного правительства и предоставления государственных (муниципальных) услуг в содержание дисциплины были внесены следующие аспекты:

Международные стандарты информационного обмена. Понятие угрозы.

Информационная безопасность в условиях функционирования в России глобальных сетей

Виды противников или «нарушителей». Понятие о видах вирусов.

Три вида возможных нарушений информационной системы. Защита.

Основные нормативные руководящие документы, касающиеся государственной тайны, нормативно-справочные документы

Назначение и задачи в сфере обеспечения информационной безопасности на уровне государства

Основные положения теории информационной безопасности. Модели безопасности и их применение

Таксономия нарушений информационной безопасности вычислительной \системы и причины, обуславливающие их существование

Анализ способов нарушений информационной безопасности.

Использование защищенных компьютерных систем.

Методы криптографии

Основные технологии построения защищенных систем.

Место информационной безопасности экономических систем в национальной безопасности страны.

3.2. Планируемые результаты обучения

Планируемыми результатами обучения по дисциплине «Информационная безопасность России» являются знания, умения, владения (ПК-2), характеризующие уровень формирования компетенции ПК-2– способностью вырабатывать решения, учитывающие правовую и нормативную базу.

Таблица 2 – Перечень результатов обучения, формируемых в ходе изучения дисциплины

Перечень контролируемой компетенции (или её части)		Перечень планируемых результатов обучения по дисциплине
код	Содержание компетенций	
ПК-2	способность вырабатывать решения, учитывающие правовую и нормативную базу	***Знать:*** средства и методы предотвращения и обнаружения вторжений; технические каналы утечки информации; возможности технических средств перехвата информации; способы и средства защиты информации от утечки по техническим каналам и контроля эффективности защиты информации; организацию защиты информации от утечки по техническим каналам на объектах информатизации; ***Уметь:*** пользоваться нормативными документами по противодействию технической разведке; оценивать качество готового программного обеспечения; ***Владеть:*** методами и средствами технической защиты информации; методами расчета и инструментального контроля показателей технической защиты информации.

3.3. Матрица соотнесения разделов (тем) дисциплины с формируемыми в них компетенциями

Таблица 3 – соотнесения разделов (тем) дисциплины с формируемыми в них компетенциями

№ п/п	Наименование раздела/темы дисциплины	Кол-во часов	ПК-2
1	**Раздел 1.** Международные стандарты информационного обмена. Понятие угрозы.	4	+
2	**Раздел 2.** Информационная безопасность в условиях	6	+

	функционирования в России глобальных сетей		
3	**Раздел 3.** Виды противников или «нарушителей». Понятие о видах вирусов.	6	+
4	**Раздел 4.** Три вида возможных нарушений информационной системы. Защита.	6	+
5	**Раздел 5.** Основные нормативные руководящие документы, касающиеся государственной тайны, нормативно-справочные документы	6	+
6	**Раздел 6.** Назначение и задачи в сфере обеспечения информационной безопасности на уровне государства	6	+
7	**Раздел 7.** Основные положения теории информационной безопасности. Модели безопасности и их применение	6	+
8	**Раздел 8.** Таксономия нарушений информационной безопасности вычислительной \системы и причины, обуславливающие их существование	6	+
9	**Раздел 9.** Анализ способов нарушений информационной безопасности.	6	+
10	**Раздел 10.** Использование защищенных компьютерных систем.	6	+
11	**Раздел 11.** Методы криптографии	4	+
12	**Раздел 12.** Основные технологии построения защищенных систем.	4	+
13	**Раздел 13.** Место информационной безопасности экономических систем в национальной безопасности страны.	2	+
14	Зачет с оценкой	4	+

4. Объем, структура и содержание дисциплины в зачетных единицах с указанием количества академических/астрономических часов, выделенных на контактную работу обучающихся с преподавателем (по видам занятий) и на самостоятельную работу обучающихся.

4.1 Объем дисциплины

Таблица 4 – Трудоемкость дисциплины

Объем дисциплины	Всего акад./ астр часов
Всего зачетных единиц	2
Всего академических/астрономических часов учебных занятий	72/54
В том числе:	
контактной работы обучающихся с преподавателем	
по видам учебных занятий:	
занятия лекционного типа	10
практические занятия	14
промежуточной аттестации	4

Самостоятельная работа обучающихся:	44
подготовка к контрольным работам	16
выполнение творческих заданий	16
курсовое проектирование	-
подготовка к зачету с оценкой	12

Промежуточная аттестация – зачет с оценкой

4.2. Структура дисциплины (обновляется по мере необходимости)

Таблица 5 – Структура дисциплины

Раздел дисциплины	Семестр	Неделя семестра	Всего	Виды учебной работы, включая самостоятельную работу обучающихся и трудоемкость (в часах ауд/астр)			Вид контроля*
				Лекции	Практ. зан.	СРС	
Раздел 1. Международные стандарты информационного обмена. Понятие угрозы.	**4**	**1**	**4**	**2**		**2**	Входной контроль Текущий контроль
Раздел 2. Информационная безопасность в условиях функционирования в России глобальных сетей	**4**	**2**	**4**	**2**		**2**	Текущий контроль
Раздел 3. Виды противников или «нарушителей». Понятие о видах вирусов.	**4**	**3**	**4**		**2**	**2**	Текущий контроль
Раздел 4. Три вида возможных нарушений информационной системы. Защита.	**4**	**4**	**4**		**2**	**2**	Текущий контроль
Раздел 5. Основные нормативные руководящие документы, касающиеся государственной тайны, нормативно-справочные документы	**4**	**5**	**4**	**2**		**2**	Рубежный контроль
Раздел 6. Назначение и задачи в сфере обеспечения информационной безопасности на уровне государства	**4**	**6**	**4**	**2**		**2**	Текущий контроль
Раздел 7. Основные положения теории информационной безопасности. Модели	**4**	**7**	**4**		**2**	**2**	Текущий контроль

безопасности и их применение							
Раздел 8. Таксономия нарушений информационной безопасности вычислительной системы и причины, обуславливающие их существование	**4**	**8**	**4**	**2**		**2**	Текущий контроль
Раздел 9. Анализ способов нарушений информационной безопасности.	**4**	**9**	**4**		**2**	**2**	Рубежный контроль
Раздел 10. Использование защищенных компьютерных систем.	**4**	**10**	**4**		**2**	**2**	Текущий контроль
Раздел 11. Методы криптографии	**4**	**11**	**6**		**2**	**4**	Текущий контроль
Раздел 12. Основные технологии построения защищенных систем.	**4**	**12**	**6**		**2**	**4**	Текущий контроль
Раздел 13. Место информационной безопасности экономических систем в национальной безопасности страны.	**4**	**13**	**4**			**4**	Текущий контроль
Зачет с оценкой			**16**			**12**	Итоговый контроль
Всего	**4**	**13**	**72**	**10**	**14**	**44**	

4.3. Содержание дисциплины, структурированное по темам (разделам)

4.3.1.Теоретические занятия - занятия лекционного типа

Таблица 6 – Содержание лекционного курса

№ п/п	Наименование раздела (модуля) дисциплины, темы	Содержание	Кол-во часов	Форма проведения занятия	Оценочное средство*	Формируемый результат**
1	**Раздел 1.** Международные стандарты информационного обмена. Понятие угрозы.	Международные стандарты информационного обмена. Понятие угрозы. Информационная безопасность в условиях функционирования в России глобальных сетей. Виды противников или «нарушителей». Понятие о видах вирусов. Понятие нарушителя информационной безопасности. Хакеры. Виды хакеров. Примеры хакерских атак. Вирусы как класс вредоносного программного обеспечения. Виды вирусов и их классификация. Три вида возможных нарушений информационной системы. Защита. Основные нормативные руководящие документы, касающиеся государственной тайны, нормативно-справочные документы. Понятие государственной, коммерческой, личной тайны. Основные нормативные документы в этой области. Рассекречивание документов. Уровень тайны. Основные нормативные руководящие документы, касающиеся государственной тайны, нормативно-справочные документы	2	Тематическая лекция	Текущий контроль	***3.1 – знать*** средства и методы предотвращения и обнаружения вторжений;
2	**Раздел 2.** Информационная безопасность в условиях функционирования в России	Основные положения теории информационной Назначение и задачи в сфере обеспечения информационной безопасности на уровне государства. Схема построения информационной безопасности на уровне государства. Назначение и задачи в сфере обеспечения безопасности. Специальные отделы и их функции в процессе обеспечения информационной	2	Лекция-визуализация	Аналитическое задание (презентация)	***3.2 – знать*** технические каналы утечки информации;

	глобальных сетей	безопасности государства. Военные подразделения в сфере информационной безопасности. Назначение и задачи в сфере обеспечения информационной безопасности на уровне государства Основные положения теории информационной безопасности. Модели безопасности и их применение. Основные положения теории информационной безопасности. Анализ различных моделей безопасности, как для крупного объекта, так и для относительно небольшой компании. Модели безопасности для домашней информационной системы. Применение методов информационной безопасности. Основные положения теории информационной безопасности. Модели безопасности и их применение .Таксономия нарушений информационной безопасности вычислительной системы и причины, обуславливающие их существование. Понятие таксономии нарушения безопасности. Причины нарушения информационной безопасности. Аудит событий в рамках информационной системы. Таксономия нарушений информационной безопасности вычислительной системы и причины, обуславливающие их существование Таксономия нарушений информационной безопасности вычислительной системы и причины, обуславливающие их существование способов нарушений информационной безопасности. (8 часов) Анализ различных способов нарушений информационной безопасности. Хакерские атаки, отказы оборудования в обслуживании, внешние факторы, влияющие прямо на информационную безопасность систем. Анализ способов нарушений информационной безопасности.				

3	**Раздел 5.** Основные нормативные руководящие документы, касающиеся государственной тайны, нормативно-справочные документы	Основные нормативные руководящие документы, касающиеся государственной тайны, нормативно-справочные документы. Понятие государственной, коммерческой, личной тайны. Основные нормативные документы в этой области. Рассекречивание документов. Уровень тайны.	2	Тематическая лекция	Текущий контроль	***3.3 – знать*** возможности технических средств перехвата информации;
4	**Раздел 6.** Назначение и задачи в сфере обеспечения информационной безопасности на уровне государства	Использование защищенных компьютерных систем. Защищенные компьютерные системы. Их виды и особенности. Примеры защищенных систем. Их использование и применение на практике. Использование защищенных компьютерных системМетоды криптографии Криптография, Криптоанализ. Основные понятия криптологии. История шифрования. Использование шифрования различными методами. Рассмотрение сокрытия информации таблицей Винжера. Программы для криптографии. Электронная цифровая подпись Основные технологии построения защищенных систем. Физические устройства. Их виды и использование. Программные пакеты. Виды программных пакетов для обеспечения защищенной системы. Правовые особенности использования средств информационной защиты Основные технологии построения защищенных систем	2	Тематическая лекция	Текущий контроль	***3.4– знать*** способы и средства защиты информации от утечки по техническим каналам и контроля эффективности защиты информации;

5.	**Раздел 8.** Таксономия нарушений информационной безопасности вычислительной системы и причины, обуславливающие их существование	Таксономия нарушений информационной безопасности вычислительной системы и причины, обуславливающие их существование Анализ способов нарушений информационной безопасности. Хакерские атаки, отказы оборудования в обслуживании, внешние факторы, влияющие прямо на информационную безопасность систем.	2	Лекция-визуализация	Аналитическое задание (презентация)	***З.5 – знать*** организацию защиты информации от утечки по техническим каналам на объектах информатизации;
Всего			**10**			З.1. З.2, З.3, З.4, З.5

4.3.2. Занятия семинарского типа

Таблица 7 – Содержание практического (семинарского) курса

№ п/п	Темы практических занятий.	Кол-во часов	Форма проведения занятия	Оценочное средство*	Формируемый результат**
1.	**Раздел 3.** Виды противников или «нарушителей». Понятие о видах вирусов. Понятие о видах вирусов. Понятие нарушителя информационной безопасности. Хакеры. Виды хакеров. Примеры хакерских атак. Вирусы как класс вредоносного программного обеспечения. Виды вирусов и их классификация. Понятие о видах вирусов Три вида возможных нарушений информационной системы. Защита.	2	Практическое занятие	Тест	***У.1 – уметь*** пользоваться нормативными документами по противодействию технической разведке;

№ п/п	Темы практических занятий.	Кол-во часов	Форма проведения занятия	Оценочное средство*	Формируемый результат**
2.	**Раздел 4.** Три вида возможных нарушений информационной системы. Защита. Три вида возможных нарушений информационной безопасности. 3 составляющих ИБ - целостность, доступность, конфиденциальность. Защита информационной системы от угроз.	2	Практическое занятие	Текущий контроль	***У.2 – уметь*** оценивать качество готового программного обеспечения;
3	**Раздел 7.** Основные положения теории информационной безопасности. Модели безопасности и их применение Назначение и задачи в сфере обеспечения информационной безопасности на уровне государства. Схема построения информационной безопасности на уровне государства. Назначение и задачи в сфере обеспечения безопасности. Специальные отделы и их функции в процессе обеспечения информационной безопасности государства. Военные подразделения в сфере информационной безопасности.	2	Практическое занятие	Текущий контроль	***В 1 – владеть*** методами и средствами технической защиты информации;
4	**Раздел 9.** Анализ способов нарушений информационной безопасности. Анализ различных способов нарушений информационной безопасности. Хакерские атаки, отказы оборудования в обслуживании, внешние факторы, влияющие прямо на информационную безопасность систем. Анализ способов нарушений информационной безопасности	2	Практическое занятие	Тест	***В 2 – владеть*** методами расчета и инструментального контроля показателей технической защиты информации
5	**Раздел 10.** Использование защищенных компьютерных	2	Практическ	Текущий	***У.1 – уметь*** пользоваться

№ п/п	Темы практических занятий.	Кол-во часов	Форма проведения занятия	Оценочное средство*	Формируемый результат**
	систем. Использование защищенных компьютерных систем. Защищенные компьютерные системы. Их виды и особенности. Примеры защищенных систем. Их использование и применение на практике		ое занятие	контроль	нормативными документами по противодействию технической разведке;
6	**Раздел 11.** Методы криптографии Криптография, Криптоанализ. Основные понятия криптологии. История шифрования. Использование шифрования различными методами. Рассмотрение сокрытия информации таблицей Винжера. Программы для криптографии. Электронная цифровая подпись.	2			***У.2 – уметь*** оценивать качество готового программного обеспечения;
7	**Раздел 12.** Основные технологии построения защищенных систем. Основные технологии построения защищенных систем. Физические устройства. Их виды и использование. Программные пакеты. Виды программных пакетов для обеспечения защищенной системы. Правовые особенности использования средств информационной защиты	2			***В 1 – владеть*** методами и средствами технической защиты информации;
9	Зачет с оценкой в письменной и устной формах	4	Тест и устный ответ	Зачет с оценкой в письменной и устной формах	У.1, У.2, В.1, В.2,ПК-2
10	**Всего**	**18**			

4.3.3. Самостоятельная работа

Таблица 8 – Задания для самостоятельного изучения

№ п/п	Тема	Кол-во часов	Оценочное средство*	Формируемый результат**
1	**Раздел 1.** Международные стандарты информационного обмена. Понятие угрозы.	**2**	*Рецензирование научных статей*	***З.1 – знать*** средства и методы предотвращения и обнаружения вторжений;
2	**Раздел 2.** Информационная безопасность в условиях функционирования в России глобальных сетей	**2**	*Тест*	***З.2 – знать*** технические каналы утечки информации;
3	**Раздел 3.** Виды противников или «нарушителей». Понятие о видах вирусов.	**2**	*Реферат*	***У.1 – уметь*** пользоваться нормативными документами по противодействию технической разведке;
4	**Раздел 4.** Три вида возможных нарушений информационной системы. Защита.	**2**	*Презентация*	***У.2 – уметь*** оценивать качество готового программного обеспечения;
5	**Раздел 5.** Основные нормативные руководящие документы, касающиеся государственной тайны, нормативно-справочные документы	**2**	*Рецензирование научных статей*	***З.3 – знать*** возможности технических средств перехвата информации;
6	**Раздел 6.** Назначение и задачи в сфере обеспечения информационной безопасности на уровне государства	**2**	*Рецензирование научных статей*	***З.4– знать*** способы и средства защиты информации от утечки по техническим

				каналам и контроля эффективности защиты информации;
7	**Раздел 7.** Основные положения теории информационной безопасности. Модели безопасности и их применение	**2**	*Тест*	***В 1 – владеть*** методами и средствами технической защиты информации
8	**Раздел 8.** Таксономия нарушений информационной безопасности вычислительной системы и причины, обуславливающие их существование	**2**	*Реферат*	***З.5 – знать*** организацию защиты информации от утечки по техническим каналам на объектах информатизации;
9	**Раздел 9.** Анализ способов нарушений информационной безопасности.	**2**	*Презентация*	***В 2 – владеть*** методами расчета и инструментального контроля показателей технической защиты информации
10	**Раздел 10.** Использование защищенных компьютерных систем.	**2**	*Рецензирование научных статей*	***У.1 – уметь*** пользоваться нормативными документами по противодействию технической разведке;
11	**Раздел 11.** Методы криптографии	**4**	*Презентация*	***У.2 – уметь*** оценивать качество готового программного обеспечения;
12	**Раздел 12.** Основные технологии построения защищенных систем.	**4**	*Рецензирование научных статей*	***В 1 – владеть*** методами и средствами технической защиты информации;

13	**Раздел 13.** Место информационной безопасности экономических систем в национальной безопасности страны.	**4**	*Тест*	***В 2 – владеть*** методами расчета и инструментального контроля показателей технической защиты информации
14	***Подготовка к зачету с оценкой***	**12**	*Тест*	З.1, З.2,, З.3, З.4, З.5, У.1, У.2, В.1, В.2, ПК-2
12	**Всего**	**44**		

5. Перечень образовательных технологий, используемых при осуществлении образовательного процесса по дисциплине, включая перечень лицензионного программного обеспечения, современных профессиональных баз данных и информационных справочных систем

5.1. Перечень образовательных технологий

Формирование в компетентностном подходе у обучающегося профессиональной компетенции ПК-2 предусматривает использование в учебном процессе инновационных образовательных технологий, активных и интерактивных форм проведения занятий в сочетании с внеаудиторной работой.

Активные формы занятий побуждают обучаемых к мыслительной активности, к проявлению творческого, исследовательского подхода и поиску новых идей для решения разнообразных задач по специальности и способствуют разнообразному (индивидуальному, групповому, коллективному) изучению (усвоению) учебных вопросов (проблем), активному взаимодействию обучаемых и преподавателя, межличностной коммуникации в устной и письменной формах, живому обмену мнениями между ними, нацеленному на выработку правильного понимания содержания изучаемой темы и способов ее практического использования. В соответствии с этим при изучении дисциплины «Информационная безопасность России» предусматривается использование следующих образовательных технологий:

1. Входной контроль в виде решения тестовых заданий.
2. Теоретические занятия - занятия лекционного типа в виде:
– проблемная мультимедийная лекция с элементами беседы и визуализации;
– проблемная мультимедийная лекция с элементами дискуссии.
3. Занятия семинарского типа проводятся в виде практических занятий, семинаров-круглых столов, обсуждения творческих работ.

5.2. Лицензионное программное обеспечение

В образовательном процессе при изучении дисциплины используется следующее лицензионное программное обеспечение:

- ОС Windows 7 (подписка Azure Dev Tools for Teaching)
- MS Office 2007 (Microsoft Open License (Academic))
- Kaspersky Endpoint Security 10 (лицензия 1C1C1903270749246701337)
- Система тестирования INDIGO (лицензия №54736)

5.3. Информационные справочные системы

Изучение дисциплины сопровождается применением информационных справочных систем:

- Справочная информационно-правовая система «Гарант» (договор №118/12/11)
- Справочная информационно-правовая система «КонсультантПлюс» (договор №СВ16-182)

5.4. Современные профессиональные базы данных

Изучение дисциплины сопровождается применением современных профессиональных баз данных:

- Электронно-библиотечная система «Университетская Библиотека Онлайн» - https://biblioclub.ru/.
- Научная электронная библиотека - www.elibrary.ru.

Реферативная и справочная база данных рецензируемой литературы Scopus - https://www.scopus.com.

Политематическая реферативно-библиографическая и наукометрическая (библиометрическая) база данных Web of Science - https://apps.webofknowledge.com

Архив научных журналов НП Национальный Электронно-Информационный Консорциум (НЭИКОН) (arch.neicon.ru)

Научная библиотека открытого доступа - https://cyberleninka.ru

- Информационнаясистема Everyday English in Conversation - http://www.focusenglish.com.

- База данных OxfordJournals Оксфордская открытая инициатива включает полный и факультативный открытый доступ к более, чем 100 журналам, выбранным из каждой предметной области - https://academic.oup.com/journals/pages/social_sciences.

6. Оценочные средства для проведения входного, текущего, рубежного контроля и промежуточной аттестации обучающихся по дисциплине и методические материалы по ее освоению

Типовые задания, база тестов и иные материалы, необходимые для оценки результатов освоения дисциплины (в т.ч. в процессе её освоения), а также методические материалы, определяющие процедуры этой оценки приводятся в приложении 1 к рабочей программе дисциплины

Универсальная система оценивания результатов обучения выполняется в соответствии в положением о текущем контроле АНООВО «КИУ», утвержденном приказом ректора № 218 о/д от 19.09.2018 и включает в себя системы оценок:

1) «отлично», «хорошо», «удовлетворительно», «неудовлетворительно»;

2) «зачтено», «не зачтено».

7. Перечень основной и дополнительной учебной литературы, необходимой для освоения дисциплины (обновляется ежегодно)

7.1. Основная учебная литература

Аверченков, В. И. Аудит информационной безопасности : учебное пособие : [16+] / В. И. Аверченков. – 4-е изд., стер. – Москва : ФЛИНТА, 2021. – 269 с. : ил., схем., табл. – Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book&id=93245.

Основы национальной безопасности : учебное пособие / Н. Д. Эриашвили, Е. Н. Хазов, Л. Т. Чихладзе [и др.] ; под ред. Е. Н. Хазова, Н. Д. Эриашвили. – Москва : Юнити-Дана, 2018. – 335 с. – Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book&id=473285.

7.2. Дополнительная учебная литература

Национальная безопасность : учебник / Н. Д. Эриашвили, О. А. Миронова, Е. Н. Хазов [и др.] ; под ред. Н. Д. Эриашвили, О. А. Мироновой. – Москва : Юнити-Дана, 2017. – 288 с. : схем., табл., ил. – Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book&id=685365.

Основы теории национальной безопасности : учебное пособие / А. В. Блюм, А. А. Дик, Э. А. Мамонтова, А. М. Попов ; Тамбовский государственный технический университет. – Тамбов : Тамбовский государственный технический университет (ТГТУ), 2017. – 97 с. – Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book&id=499147.

Экономическая безопасность : учебник / В. Б. Мантусов, Н. Д. Эриашвили, Е. И. Кузнецова [и др.] ; под ред. В. Б. Мантусова, Н. Д. Эриашвили ; Российская таможенная академия. – 5-е изд., перераб. и доп. – Москва : Юнити, 2021. – 433 с. : схем., табл, ил. – Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book&id=682412.

8. Перечень ресурсов информационно-телекоммуникационной сети «Интернет» (далее – сеть «Интернет»), необходимых для освоения дисциплины (обновляется ежегодно)

1. http://biblioclub.ru/ - электронно-библиотечная система «Университетская библиотека ONLINE».
2. http://lib.usue.ru – Информационно библиотечный комплекс.
3. http://www.eLIBRARY.RU - научная электронная библиотека.
4. http://www.knigafund.ru -Электронная библиотека студента «КнигаФонд».

9. Требования к минимальному материально-техническому обеспечению, необходимого для осуществления образовательного процесса по дисциплине (обновляется ежегодно)

Для изучения дисциплины используется мультимедийная аудитория, вместимостью более 25 человек. Мультимедийная аудитория оснащена современными средствами воспроизведения и визуализации любой видео и аудио информации, получения и передачи электронных документов.

Типовая комплектация мультимедийной аудитории состоит из: мультимедийного проектора, проекционного экрана, акустической системы, персонального компьютера (с техническими характеристиками не ниже: процессор - 300 MHz, оперативная память -128 Мб), интерфейсы подключения: USB, audio, HDMI. Преподаватель имеет возможность легко управлять всей системой, что позволяет проводить лекции, практические занятия, презентации, вебинары, конференции и другие виды аудиторной нагрузки обучающихся в удобной и доступной для них форме с применением современных интерактивных средств обучения, в том числе с использованием в процессе обучения всех корпоративных ресурсов. Мультимедийная аудитория также оснащена широкополосным доступом в сеть интернет. Компьютерное оборудованием имеет соответствующее лицензионное программное обеспечение. Учебно-методическая литература для данной дисциплины имеется в наличии в электронно-библиотечной системе «Университетская библиотека ONLINE», доступ к которой предоставлен обучающимся. Электронно-библиотечная система «Университетская библиотека ONLINE» реализует легальное хранение, распространение и защиту цифрового контента учебно-методической литературы для вузов с условием обязательного соблюдения авторских и смежных прав. Электронно-библиотечная система «Университетская библиотека ONLINE» обеспечивает широкий законный доступ к необходимым для образовательного процесса изданиям с использованием инновационных технологий и соответствует всем требованиям ФГОС ВО по направлению 38.04.04 – «Государственное и муниципальное управление».

Приложение 1
к рабочей программе дисциплины
Б1.В.ОД.12 Информационная безопасность России

ОЦЕНОЧНЫЕ СРЕДСТВА ДЛЯ ПРОВЕДЕНИЯ ВХОДНОГО, ТЕКУЩЕГО, РУБЕЖНОГО КОНТРОЛЯ И ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ОБУЧАЮЩИХСЯ ПО ДИСЦИПЛИНЕ И МЕТОДИЧЕСКИЕ МАТЕРИАЛЫ ПО ЕЕ ОСВОЕНИЮ

«ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ РОССИИ» (Б1.В.ОД.12)

Направление подготовки	**38.04.04. Государственное и муниципальное управление**
Направленность	**Национальная безопасность**
Квалификация (степень) выпускника (уровень направления подготовки)	**магистр**
Форма обучения	**очная, очно-заочная, заочная**

Калининград

2024

6.1. Оценочные средства для проведения входного, текущего, рубежного контроля и промежуточной аттестации обучающихся по дисциплине и методические материалы по ее освоению

6.1.1. Цель оценочных средств

Целью оценочных средств является установление соответствия уровня подготовленности обучающегося на данном этапе обучения требованиям рабочей программы по дисциплине «Информационная безопасность России».

Оценочные средства - это совокупность материалов, измерительных инструментов, описания оценочных форм и процедур, которые используются для измерения и оценки уровня сформированности компетенций (части компетенции) обучающихся, освоивших программу учебной дисциплины «Информационная безопасность России».

Контрольно-измерительные материалы (КИМ) – разновидность оценочных средств, направленных на два основных процесса: **контроль** и **измерение**.

Оценочные средства включают контрольно-измерительные материалы для проведения всех видов контроля и оценки в форме тестовых заданий, доклада-презентации по проблемным вопросами промежуточной аттестации в форме вопросов и заданий к экзамену /зачету.

6.1.2. Объекты оценивания – результаты освоения дисциплины

Объектами оценивания являются знания, умения и владения в соответствии с требованиями ФГОС ВО по освоению дисциплины «Информационная безопасность России».

Результатами освоения дисциплины являются освоение компетенции ПК-2 - способность вырабатывать решения, учитывающие правовую и нормативную базу.

Таблица 1 – Перечень компетенций, формируемых в процессе освоения дисциплины с указанием этапов их формирования

Контролируемые	Контролируемые компетенции (или её части)		Планируемые результаты освоения дисциплины*	Вид контроля и наименование оценочного средства*		
Разделы дисциплины Темы занятий	Код	Содержание компетенции		*входной*	*текущий*	*Промежуточная аттестация*
Раздел 1. Международные стандарты информационного обмена. Понятие угрозы.	*ПК-2*	способностью вырабатывать решения, учитывающие правовую и нормативную базу	***З.1 – знать*** средства и методы предотвращения и обнаружения вторжений;	Т1		
Раздел 2. Информационная безопасность в условиях функционирования в России глобальных сетей	*ПК-2*	способностью вырабатывать решения, учитывающие правовую и нормативную базу	***З.2 – знать*** технические каналы утечки информации;		П1	
Раздел 3. Виды противников или «нарушителей». Понятие о видах вирусов.	*ПК-2*	способностью вырабатывать решения, учитывающие правовую и нормативную базу	***У.1 – уметь*** пользоваться нормативными документами по противодействию технической разведке;	Т1		

Раздел 4. Три вида возможных нарушений информационной системы. Защита.	*ПК-2*	способностью вырабатывать решения, учитывающие правовую и нормативную базу	***У.2 – уметь*** оценивать качество готового программного обеспечения;		П1	
Раздел 5. Основные нормативные руководящие документы, касающиеся государственной тайны, нормативно-справочные документы	*ПК-2*	способностью вырабатывать решения, учитывающие правовую и нормативную базу	***З.3 – знать*** возможности технических средств перехвата информации;	Т1		
Раздел 6. Назначение и задачи в сфере обеспечения информационной безопасности на уровне государства	*ПК-2*	способностью вырабатывать решения, учитывающие правовую и нормативную базу	***З.4– знать*** способы и средства защиты информации от утечки по техническим каналам и контроля эффективности защиты информации;		П1	
Раздел 7. Основные положения теории информационной безопасности. Модели безопасности и их применение	*ПК-2*	способностью вырабатывать решения, учитывающие правовую и нормативную базу	***В 1 – владеть*** методами и средствами технической защиты информации	Т1		

Раздел 8. Таксономия нарушений информационной безопасности вычислительной системы и причины, обуславливающие их существование	*ПК-2*	способностью вырабатывать решения, учитывающие правовую и нормативную базу	***З.5 – знать*** организацию защиты информации от утечки по техническим каналам на объектах информатизации;		П1	
Раздел 9. Анализ способов нарушений информационной безопасности.	*ПК-2*	способностью вырабатывать решения, учитывающие правовую и нормативную базу	***В 2 – владеть*** методами расчета и инструментального контроля показателей технической защиты информации	Т1		
Раздел 10. Использование защищенных компьютерных систем.	*ПК-2*	способностью вырабатывать решения, учитывающие правовую и нормативную базу	***У.1 – уметь*** пользоваться нормативными документами по противодействию технической разведке;		П1	
Раздел 11. Методы криптографии	*ПК-2*	способностью вырабатывать решения, учитывающие правовую и нормативную базу	***У.2 – уметь*** оценивать качество готового программного обеспечения;	Т1		

Раздел 12. Основные технологии построения защищенных систем.	*ПК-2*	способностью вырабатывать решения, учитывающие правовую и нормативную базу	***В 1 – владеть*** методами и средствами технической защиты информации;		П1	
Раздел 13. Место информационной безопасности экономических систем в национальной безопасности страны.	*ПК-2*	способностью вырабатывать решения, учитывающие правовую и нормативную базу	***В 2 – владеть*** методами расчета и инструментального контроля показателей технической защиты информации	Т1		

**В соответствии с Перечнем планируемых результатов обучения по дисциплине (Таблица 2)*
Указывается вид контроля, предусмотренный рабочей программой

6.1.3. Примерные оценочные средства и иные материалы, необходимые для оценки знаний, умений, владений в процессе освоения дисциплины, характеризующих этапы формирования компетенций в процессе освоения дисциплины

Примерные оценочные средства для проведения входного контроля

1 Угрозы информационной безопасности предприятия (организации) и способы борьбы с ними
2 Современные средства защиты информации
3 Современные системы компьютерной безопасности
4 Современные средства противодействия экономическому шпионажу
5 Современные криптографические системы
6 Криптоанализ, современное состояние
7 Правовые основы защиты информации
8 Технические аспекты обеспечения защиты информации. Современное состояние
9 Атаки на систему безопасности и современные методы защиты
10 Современные пути решения проблемы информационной безопасности РФ

Примерные оценочные средства для проведения текущего и рубежного контроля
Текущий контроль осуществляется для оценки уровня сформированности компетенции «ПК-2».

Примерные задания для оценки компетенции «ПК-2»:

1. Что такое информационная безопасность?
2. Какие предпосылки и цели обеспечения информационной безопасности?
3. В чем заключаются национальные интересы РФ в информационной сфере?
4. Что включает в себя информационная борьба?
5. Какие пути решения проблем информационной безопасности РФ существуют?
6. Каковы общие принципы обеспечения защиты информации?
7. Какие имеются виды угроз информационной безопасности предприятия (организации)?
8. Какие источники наиболее распространенных угроз информационной безопасности существуют?
9. Какие виды сетевых атак имеются?
10. Какими способами снизить угрозу сниффинга пакетов?
11. Какие меры по устранению угрозы IP -спуфинга существуют?
12. Что включает борьба с атаками на уровне приложений?
13. Какие существуют проблемы обеспечения безопасности локальных вычислительных сетей? В чем заключается распределенное хранение файлов?
14. Что включают в себя требования по обеспечению комплексной системы информационной безопасности?
15. Какие уровни информационной защиты существуют, их основные составляющие?
16. В чем заключаются задачи криптографии?
17. Зачем нужны ключи?
18. Какая схема шифрования называется многоалфавитной подстановкой?
19. .Какие системы шифрования вы знаете?
20. Что включает в себя защита информации от несанкционированного доступа?
21. .В чем заключаются достоинства и недостатки программно-аппаратных средств защиты информации?

22. Какие виды механизмов защиты могут быть реализованы для обеспечения идентификации и аутентификации пользователей?

23. Какие задачи выполняет подсистема управления доступом?

24. Какие требования предъявляются к подсистеме протоколирования аудита?

25. Какие виды механизмов защиты могут быть реализованы для обеспечения конфиденциальности данных и сообщений?

26. В чем заключается контроль участников взаимодействия?

27. Какие функции выполняет служба регистрации и наблюдения?

28. Что такое информационно-опасные сигналы, их основные параметры?

29. .Какие требования необходимо выполнять при экранировании помещений, предназначенных для размещения вычислительной техники?

30. Какой процесс называется аутентификацией пользователя?

31. Какие схемы аутентификации вы знаете?

32. Что такое смарт-карты?

33. Какие требования предъявляются к современным криптографическим системам защиты информации?

34. Что такое симметричная криптосистема?

35. Какие виды симметричных криптосистем существуют?

36. Что такое асимметричная криптосистема?

37. Что понимается под односторонней функцией?

38. Как классифицируются криптографические алгоритмы по стойкости?

39. В чем заключается анализ надежности криптосистем?

40. Что такое дифференциальный криптоанализ?

41. В чем сущность криптоанализа со связанными ключами?

42. В чем сущность линейного криптоанализа?

43. Какие атаки изнутри вы знаете?

44. Какая программа называется логической бомбой?

45. Какими способами можно проверить систему безопасности?

46. Что является основными характеристиками технических средств защиты информации? Какие требования предъявляются к автоматизированным системам защиты третьей группы?

47. Какие требования предъявляются к автоматизированным системам защиты второй группы?

48. Какие требования предъявляются к автоматизированным системам защиты первой группы?

49. Какие классы защиты информации от несанкционированного доступа для средств вычислительной техники имеются? От чего зависит выбор класса защищенности?

50. Какие требования предъявляются к межсетевым экранам?

51. Какие имеются показатели защищенности межсетевых экранов?

52. Какие атаки системы снаружи вы знаете?

53. Какая программа называется вирусом?

54. Какая атака называется атакой отказа в обслуживании?

55. Какие виды вирусов вы знаете?

56. Какие вирусы называются паразитическими?

57. Как распространяются вирусы?

58. Какие методы обнаружения вирусов вы знаете?
59. Какая программа называется монитором обращения?
60. Что представляет собой домен?
61. Как осуществляется защита при помощи ACL -списков?
62. Какой список называется перечнем возможностей?
63. Какие способы защиты перечней возможностей вы знаете?
64. Из чего состоит высоконадежная вычислительная база (ТСВ)?
65. Какие модели многоуровневой защиты вы знаете?
66. В чем заключается организация работ по защите от несанкционированного доступа интегрированной информационной системы управления предприятием?
67. Какие характеристики положены в основу системы классификации информационных систем управления предприятием?
68. Какие задачи решает система компьютерной безопасности?
69. Какие пути защиты информации в локальной сети существуют?
70. Какие задачи решают технические средства противодействия экономическому шпионажу?
71. Какой порядок организации системы видеонаблюдения?
72. Что включает в себя защита информационных систем с помощью планирования? Какие условия работы оцениваются при планировании?
73. Из каких этапов состоят работы по обеспечению информационной безопасности предприятия?
74. Что такое мобильные программы?
75. Что такое концепция потоков?
76. Что представляет собой метод «песочниц»?
77. Что такое интерпретация?
78. Что такое программы с подписями?
79. Что представляет собой безопасность в системе Java ?
80. Назовите несколько примеров политик безопасности пакета JDK 1.2?
81. Какие международные документы регламентируют деятельность по обеспечению защиты информации?
82. Что понимают под политикой информационной безопасности?
83. Что включает в себя политика информационной безопасности РФ?
84. Какие нормативные документы РФ определяют концепцию защиты информации?

Примерные вопросы для тестирования

Правильный вариант ответа отмечен знаком +

1) К правовым методам, обеспечивающим информационную безопасность, относятся:

- Разработка аппаратных средств обеспечения правовых данных
- Разработка и установка во всех компьютерных правовых сетях журналов учета действий
+ Разработка и конкретизация правовых нормативных актов обеспечения безопасности

2) Основными источниками угроз информационной безопасности являются все указанное в списке:

- Хищение жестких дисков, подключение к сети, инсайдерство
+ Перехват данных, хищение данных, изменение архитектуры системы
- Хищение данных, подкуп системных администраторов, нарушение регламента работы

3) Виды информационной безопасности:

+ Персональная, корпоративная, государственная
- Клиентская, серверная, сетевая
- Локальная, глобальная, смешанная
4) Цели информационной безопасности – своевременное обнаружение, предупреждение:
+ несанкционированного доступа, воздействия в сети
- инсайдерства в организации
- чрезвычайных ситуаций
5) Основные объекты информационной безопасности:
+ Компьютерные сети, базы данных
- Информационные системы, психологическое состояние пользователей
- Бизнес-ориентированные, коммерческие системы
6) Основными рисками информационной безопасности являются:
- Искажение, уменьшение объема, перекодировка информации
- Техническое вмешательство, выведение из строя оборудования сети
+ Потеря, искажение, утечка информации
7) К основным принципам обеспечения информационной безопасности относится:
+ Экономической эффективности системы безопасности
- Многоплатформенной реализации системы
- Усиления защищенности всех звеньев системы
8) Основными субъектами информационной безопасности являются:
- руководители, менеджеры, администраторы компаний
+ органы права, государства, бизнеса
- сетевые базы данных, фаерволлы
9) К основным функциям системы безопасности можно отнести все перечисленное:
+ Установление регламента, аудит системы, выявление рисков
- Установка новых офисных приложений, смена хостинг -компании
- Внедрение аутентификации, проверки контактных данных пользователей
10) Принципом информационной безопасности является принцип недопущения:
+ Неоправданных ограничений при работе в сети (системе)
- Рисков безопасности сети, системы
- Презумпции секретности
11) Принципом политики информационной безопасности является принцип:
+ Невозможности миновать защитные средства сети (системы)
- Усиления основного звена сети, системы
- Полного блокирования доступа при риск-ситуациях
12) Принципом политики информационной безопасности является принцип:
+ Усиления защищенности самого незащищенного звена сети (системы)
- Перехода в безопасное состояние работы сети, системы
- Полного доступа пользователей ко всем ресурсам сети, системы
13) Принципом политики информационной безопасности является принцип:
+ Разделения доступа (обязанностей, привилегий) клиентам сети (системы)
- Одноуровневой защиты сети, системы
- Совместимых, однотипных программно-технических средств сети, системы
14) К основным типам средств воздействия на компьютерную сеть относится:
- Компьютерный сбой

+ Логические закладки («мины»)
- Аварийное отключение питания
15) Когда получен спам по e-mail с приложенным файлом, следует:
- Прочитать приложение, если оно не содержит ничего ценного – удалить
- Сохранить приложение в парке «Спам», выяснить затем IP-адрес генератора спама
+ Удалить письмо с приложением, не раскрывая (не читая) его
16) Принцип Кирхгофа:
- Секретность ключа определена секретностью открытого сообщения
- Секретность информации определена скоростью передачи данных
+ Секретность закрытого сообщения определяется секретностью ключа
17) ЭЦП – это:
- Электронно-цифровой преобразователь
+ Электронно-цифровая подпись
- Электронно-цифровой процессор
18) Наиболее распространены угрозы информационной безопасности корпоративной системы:
- Покупка нелицензионного ПО
+ Ошибки эксплуатации и неумышленного изменения режима работы системы
- Сознательного внедрения сетевых вирусов
19) Наиболее распространены угрозы информационной безопасности сети:
- Распределенный доступ клиент, отказ оборудования
- Моральный износ сети, инсайдерство
+ Сбой (отказ) оборудования, нелегальное копирование данных
20) Наиболее распространены средства воздействия на сеть офиса:
- Слабый трафик, информационный обман, вирусы в интернет
+ Вирусы в сети, логические мины (закладки), информационный перехват
- Компьютерные сбои, изменение администрирования, топологии
21) Утечкой информации в системе называется ситуация, характеризуемая:
+ Потерей данных в системе
- Изменением формы информации
- Изменением содержания информации
22) Свойствами информации, наиболее актуальными при обеспечении информационной безопасности являются:
+ Целостность
- Доступность
- Актуальность
23) Угроза информационной системе (компьютерной сети) – это:
+ Вероятное событие
- Детерминированное (всегда определенное) событие
- Событие, происходящее периодически
24) Информация, которую следует защищать (по нормативам, правилам сети, системы) называется:
- Регламентированной
- Правовой
+ Защищаемой

25) Разновидностями угроз безопасности (сети, системы) являются все перечисленное в списке:
+ Программные, технические, организационные, технологические
- Серверные, клиентские, спутниковые, наземные
- Личные, корпоративные, социальные, национальные
26) Окончательно, ответственность за защищенность данных в компьютерной сети несет:
+ Владелец сети
- Администратор сети
- Пользователь сети
27) Политика безопасности в системе (сети) – это комплекс:
+ Руководств, требований обеспечения необходимого уровня безопасности
- Инструкций, алгоритмов поведения пользователя в сети
- Нормы информационного права, соблюдаемые в сети
28) Наиболее важным при реализации защитных мер политики безопасности является:
- Аудит, анализ затрат на проведение защитных мер
- Аудит, анализ безопасности
+ Аудит, анализ уязвимостей, риск-ситуаций
Темы докладов:
1. Информация - фактор существования и развития общества. Основные формы проявления информации, её свойства как объекта безопасности.
2. Понятие безопасности и её составляющие. Безопасность информации.
3. Обеспечение информационной безопасности: содержание и структура понятия.
4. Национальные интересы в информационной сфере.
5. Источники и содержание угроз в информационной сфере.
6. Соотношение понятий «информационная безопасность» и «национальная безопасность»
7. Понятие национальной безопасности. Интересы и угрозы в области национальной безопасности.
8. Влияние процессов информатизации общества на составляющие национальной безопасности и их содержание.
9. Система обеспечения информационной безопасности.
10. Обеспечение информационной безопасности Российской Федерации.
11. Понятие информационной войны. Проблемы информационной войны.
12. Информационное оружие и его классификация.
13. Цели информационной войны, её составные части и средства её ведения. Объекты воздействия в информационной войне.
14. Уровни ведения информационной войны. Информационные операции.
Психологические операции.
15. Уровни ведения информационной войны. Оперативная маскировка.
Радиоэлектронная борьба. Воздействие на сети.
16. Основные положения государственной информационной политики Российской Федерации.
17. Первоочередные мероприятия по реализации государственной политики обеспечения информационной безопасности.
18. Виды защищаемой информации в сфере государственного и муниципального управления.

19. Обеспечение информационной безопасности организации.
20. Характеристика эффективных стандартов по безопасности.
21. Требования к полноте эффективных стандартов по безопасности.
22. Риск работы на персональном компьютере. Планирование безопасной работы на персональном компьютере.
23. Информация - фактор существования и развития общества.
24. Обеспечение информационной безопасности: содержание и структура понятия.
25. Система обеспечения информационной безопасности. Обеспечение информационной безопасности организации.
26. Обеспечение информационной безопасности Российской Федерации.
27. Международная нормативная база обеспечения безопасности. Федеральная нормативная база обеспечения безопасности
28. Организационные структуры государственной системы обеспечения информационной безопасности федеральных органов исполнительной власти.
29. Административный уровень обеспечения информационной безопасности.
30. Организационные структуры системы обеспечения информационной безопасности предприятия (организации).
31. Корпоративная нормативная база по защите информации.
32. Основные организационные мероприятия по обеспечению информационной безопасности организации (предприятия).
33. Основные организационные мероприятия по обеспечению информационной безопасности организации (предприятия).
34. Нормативно-методические документы по обеспечению безопасности информации.
35. Управление персоналом на предприятиях и в организациях.
36. Подбор и расстановка кадров.
37. Мотивация добросовестной деятельности сотрудников.
38. Порядок проведения служебных расследований.
39. Организация подготовки кадров и повышения квалификации в области обеспечения информационной безопасности.
40. Категорирование объектов информатизации.
41. Общие положения по категорированию объектов информатизации. Порядок проведения категорирования объектов на предприятий.
42. Классификация автоматизированных систем в составе объектов вычислительной техники.
43. Правовые основы лицензирования. Основные понятия и принципы лицензирования. Общие положения по организации лицензирования.
44. Государственная система лицензирования. Система лицензирования деятельности в области защиты государственной тайны.
45. Правовые основы сертификации и аттестации средств защиты информации.
46. Основные понятия и принципы сертификации.
47. Организация и проведение сертификации.
48. Организация и проведение лицензирования, сертификации и аттестации.
49. Требования к объектам информатизации и необходимость проведения их аттестации. Порядок проведения аттестации объектов информатизации.
50. Права и обязанности органов системы аттестации объектов информатизации.

51. Проведение аттестационных испытаний.
52. Основы организации и обеспечения работ по технической защите информации.
53. Цели и задачи защиты информации.
54. Организация защиты конфиденциальной информации.
55. Концепция безопасности предприятия и ее содержание.
56. Организация работы подразделений (служб) обеспечения информационной безопасности.
57. Организация защиты информации на предприятии.
58. Выявление и классификация угроз.
59. Принципы обеспечения информационной безопасности.
60. Управление информационной безопасностью.
61. Политика безопасности.
62. Разработка и внедрение системы управления информационной безопасности.
Обеспечение информационной безопасности организации.
63. Характеристика эффективных стандартов по безопасности.
64. Требования к полноте эффективных стандартов по безопасности.
65. Риск работы на персональном компьютере. Планирование безопасной работы на персональном компьютере.
66. Информация - фактор существования и развития общества.
67. Обеспечение информационной безопасности: содержание и структура понятия.
68. Система обеспечения информационной безопасности. Обеспечение информационной безопасности организации.
69. Обеспечение информационной безопасности Российской Федерации.
70. Международная нормативная база обеспечения безопасности. Федеральная нормативная база обеспечения безопасности
71. Организационные структуры государственной системы обеспечения информационной безопасности федеральных органов исполнительной власти.
72. Административный уровень обеспечения информационной безопасности.
73. Общие положения по категорированию объектов информатизации. Порядок проведения категорирования объектов на предприятий.
74. Классификация автоматизированных систем в составе объектов вычислительной техники.
75. Правовые основы лицензирования. Основные понятия и принципы лицензирования. Общие положения по организации лицензирования.
76. Государственная система лицензирования. Система лицензирования деятельности в области защиты государственной тайны.
77. Правовые основы сертификации и аттестации средств защиты информации.
78. Основные понятия и принципы сертификации.
79. Организация и проведение сертификации.
80. Организация и проведение лицензирования, сертификации и аттестации.
81. Уровни ведения информационной войны. Оперативная маскировка.
Радиоэлектронная борьба. Воздействие на сети.
82. Основные положения государственной информационной политики Российской Федерации.

83. Первоочередные мероприятия по реализации государственной политики обеспечения информационной безопасности.

84. Виды защищаемой информации в сфере государственного и муниципального управления.

85. Международная нормативная база обеспечения безопасности. Федеральная нормативная база обеспечения безопасности

86. Организационные структуры государственной системы обеспечения информационной безопасности федеральных органов исполнительной власти.

87. Административный уровень обеспечения информационной безопасности.

Примерные оценочные средства для проведения промежуточной аттестации (зачета с оценкой).

1. Что такое информационная безопасность?
2. Какие предпосылки и цели обеспечения информационной безопасности?
3. В чем заключаются национальные интересы РФ в информационной сфере?
4. Что включает в себя информационная борьба?
5. Какие пути решения проблем информационной безопасности РФ существуют?
6. Каковы общие принципы обеспечения защиты информации?
7. Какие имеются виды угроз информационной безопасности предприятия (организации)?
8. Какие источники наиболее распространенных угроз информационной безопасности существуют?
9. Какие виды сетевых атак имеются?
10. Какими способами снизить угрозу сниффинга пакетов?
11. Какие меры по устранению угрозы IP -спуфинга существуют?
12. Что включает борьба с атаками на уровне приложений?
13. Какие существуют проблемы обеспечения безопасности локальных вычислительных сетей?
14. В чем заключается распределенное хранение файлов?
15. Что включают в себя требования по обеспечению комплексной системы информационной безопасности?
16. Какие уровни информационной защиты существуют, их основные составляющие?
17. В чем заключаются задачи криптографии?
18. Зачем нужны ключи?
19. Какая схема шифрования называется многоалфавитной подстановкой?
20. Какие системы шифрования вы знаете?
21. Что включает в себя защита информации от несанкционированного доступа?
22. В чем заключаются достоинства и недостатки программно-аппаратных средств защиты информации?
23. Какие виды механизмов защиты могут быть реализованы для обеспечения идентификации и аутентификации пользователей?
24. Какие задачи выполняет подсистема управления доступом?
25. Какие требования предъявляются к подсистеме протоколирования аудита?
26. Какие виды механизмов защиты могут быть реализованы для обеспечения конфиденциальности данных и сообщений?
27. В чем заключается контроль участников взаимодействия?
28. Какие функции выполняет служба регистрации и наблюдения?
29. Что такое информационно-опасные сигналы, их основные параметры?

30.Какие требования необходимо выполнять при экранировании помещений, предназначенных для размещения вычислительной техники?

31.Какой процесс называется аутентификацией пользователя?

32.Какие схемы аутентификации вы знаете?

33.Что такое смарт-карты?

34.Какие требования предъявляются к современным криптографическим системам защиты информации?

35.Что такое симметричная криптосистема?

36.Какие виды симметричных криптосистем существуют?

37.Что такое асимметричная криптосистема?

38.Что понимается под односторонней функцией?

39.Как классифицируются криптографические алгоритмы по стойкости?

40.В чем заключается анализ надежности криптосистем?

41.Что такое дифференциальный криптоанализ?

42.В чем сущность криптоанализа со связанными ключами?

43.В чем сущность линейного криптоанализа?

44.Какие атаки изнутри вы знаете?

45.Какая программа называется логической бомбой?

46.Какими способами можно проверить систему безопасности?

47.Что является основными характеристиками технических средств защиты информации?

48.Какие требования предъявляются к автоматизированным системам защиты третьей группы?

49.Какие требования предъявляются к автоматизированным системам защиты второй группы?

50.Какие требования предъявляются к автоматизированным системам защиты первой группы?

51.Какие классы защиты информации от несанкционированного доступа для средств вычислительной техники имеются? От чего зависит выбор класса защищенности?

52.Какие требования предъявляются к межсетевым экранам?

53.Какие имеются показатели защищенности межсетевых экранов?

54.Какие атаки системы снаружи вы знаете?

55.Какая программа называется вирусом?

56.Какая атака называется атакой отказа в обслуживании?

57.Какие виды вирусов вы знаете?

58.Какие вирусы называются паразитическими?

59.Как распространяются вирусы?

60.Какие методы обнаружения вирусов вы знаете?

61.Какая программа называется монитором обращения?

62.Что представляет собой домен?

63.Как осуществляется защита при помощи ACL -списков?

64.Какой список называется перечнем возможностей?

65.Какие способы защиты перечней возможностей вы знаете?

66.Из чего состоит высоконадежная вычислительная база (ТСВ)?

67.Какие модели многоуровневой защиты вы знаете?

68.В чем заключается организация работ по защите от несанкционированного доступа интегрированной информационной системы управления предприятием?

69.Какие характеристики положены в основу системы классификации информационных систем управления предприятием?

70.Какие задачи решает система компьютерной безопасности?

71.Какие пути защиты информации в локальной сети существуют?

72.Какие задачи решают технические средства противодействия экономическому шпионажу?

73.Какой порядок организации системы видеонаблюдения?

74.Что включает в себя защита информационных систем с помощью планирования?

75.Какие условия работы оцениваются при планировании?

76.Из каких этапов состоят работы по обеспечению информационной безопасности предприятия?

77.Что такое мобильные программы?

78.Что такое концепция потоков?

79.Что представляет собой метод «песочниц»?

80.Что такое интерпретация?

81.Что такое программы с подписями?

82.Что представляет собой безопасность в системе Java ?

83.Назовите несколько примеров политик безопасности пакета JDK 1.2?

84.Какие международные документы регламентируют деятельность по обеспечению защиты информации?

85.Что понимают под политикой информационной безопасности?

86.Что включает в себя политика информационной безопасности РФ?

87.Какие нормативные документы РФ определяют концепцию защиты информации?

6.1.4. Комплект оценочных материалов для проведения диагностической работы по дисциплине «Информационная безопасность России»

Вариант №1 для диагностирования сформированности компетенции ПК-2

А. Задания закрытого типа:

Задание с выбором одного верного ответа из трех предложенных.

Задание 1.

Прочитайте текст, выберите один правильный вариант ответа и запишите соответствующую ему букву (цифру) в поле «Ответ».

Вопрос. Дайте определение «Информационная безопасность»:

а) состояние защищенности национальных интересов страны (жизненно важных интересов личности, общества и государства на сбалансированной основе) в информационной сфере от внутренних и внешних угроз;

6) бескомпромиссная приверженность идеологии насилия, характеризующаяся стремлением к решительному и кардинальному изменению основ конституционного строя Российской Федерации, нарушению единства и территориальной целостности Российской Федерации;

в) совокупность взглядов и идей, представляющих насильственные и иные противоправные действия как основное средство разрешения политических, расовых, национальных, религиозных и социальных конфликтов.

Ответ:

Задание с выбором нескольких вариантов ответа из четырёх предложенных.

Задание 2.

Прочитайте текст, выберите все правильные варианты ответов и запишите соответствующие им буквы (цифры) в поле «Ответ» без пробелов и знаков препинания.

Назовите три базовых принципа, которые должна обеспечивать информационная безопасность:
А) целостность данных — защита от сбоев, ведущих к потере информации, а также зашита от неавторизованного создания или уничтожения данных;
Б) конфиденциальность информации;
В) доступность информации для всех авторизованных пользователей.
Г) на установлении и соблюдении правовых механизмов управления.

Ответ:

Задание на установление соответствия.

Задание 3.

Прочитайте текст и установите соответствие.

…

К каждой позиции, данной в левом столбце подберите соответствующую позицию из правого столбца:

А	Судебная власть	1	Военная прокуратура
Б	Исполнительная власть	2	Президент РФ
В	Законодательная власть	3	Федеральное собрание РФ
Г	Генеральная прокуратура	4	Правительство РФ
		5	Конституционный суд

Запишите выбранные цифры под соответствующими буквами в поле «Ответ».

Ответ:

А	Б	В	Г

Задание на установление последовательности.

Задание 4.

Прочитайте текст и установите последовательность.

Определите иерархию Законов РФ:

А.ФКЗ РФ

Б. ФЗ РФ.

В. Конституция РФ.

Г. Указы Президента РФ.

Д. Постановления Правительства РФ.

Запишите соответствующую последовательность букв (цифр) слева направо без пробелов и знаков препинания в поле «Ответ»:

Ответ:

Б. Задания комбинированного типа

Задание с выбором одного верного ответа из четырёх предложенных и обоснованием выбора.

Задание 5.

Прочитайте текст, выберите один правильный вариант ответа и запишите соответствующую ему букву (цифру) в поле «Ответ». Запишите аргументы, обосновывающие выбор ответа в поле «Обоснование»

Вставьте в текст одно правильное слово (А. Риск, Б. Опасность, В. Непристойность или Г. Трудность):
Угроза информационной безопасности Российской Федерации - совокупность действий и факторов, создающих ……. нанесения ущерба национальным интересам в информационной сфере.

Ответ:

Обоснование:

Задание с выбором нескольких вариантов ответа из четырёх предложенных и развёрнутым обоснованием выбора.

Задание 6.
Прочитайте текст, выберите все правильные варианты ответов и запишите соответствующие им буквы (цифры) в поле «Ответ» без пробелов и знаков препинания. Запишите аргументы, обосновывающие выбор ответа в поле «Обоснование»

Вставьте в текст одно правильное слово (А. разные, Б. равнозначны, В. законные или Г. значимые):
Статья 1 Конституции РФ гласит:
1. Российская Федерация - Россия есть демократическое федеративное правовое государство с республиканской формой правления.
2. Наименования Российская Федерация и Россия _____.

Ответ:

Обоснование:

В. Задания открытого типа
Задание с развёрнутым ответом.
Задание 7.
Прочитайте текст и запишите в поле «Ответ» свои аргументы, обосновывающие выбор ответа. Используйте чёткие, компактные формулировки.

Под *«национальной безопасностью»* в новой Стратегии 2021 года понимается …
Ответ:

Задание с развёрнутым ответом.
Задание 8.
Прочитайте текст и запишите в поле «Ответ» свои аргументы, обосновывающие выбор ответа. Используйте чёткие, компактные формулировки.

Какой нормативно-правовой документ определяет Стратегию национальной безопасности Российской Федерации до 2025 года?

Ответ:

Вариант № 2 для диагностирования сформированности компетенции ПК-2

А. Задания закрытого типа:
Задание с выбором одного верного ответа из трех предложенных.
Задание 1.
Прочитайте текст, выберите один правильный вариант ответа и запишите соответствующую ему букву (цифру) в поле «Ответ».

Вопрос. Что понимается «Под предметом информационной безопасности»:

а) совокупность взглядов и идей, оправдывающих применение насилия для достижения политических, идеологических, религиозных и иных целей;

6) область защиты информации на конфиденциальность, целостность и доступность;

в) совокупность взглядов и идей, представляющих насильственные и иные противоправные действия как основное средство разрешения политических, расовых, национальных, религиозных и социальных конфликтов.

Ответ:

Задание с выбором нескольких вариантов ответа из четырёх предложенных.
Задание 2.
Прочитайте текст, выберите все правильные варианты ответов и запишите соответствующие им буквы (цифры) в поле «Ответ» без пробелов и знаков препинания.

Правовой основой формирования федеративных отношений служит:

а) Федеративный договор между РФ и субъектами РФ;

б) Конституция РФ;

в) Указы Президента РФ;

г) Постановления Правительства РФ.

Ответ:

Задание на установление соответствия.
Задание 3.

Прочитайте текст и установите соответствие.
К каждой позиции, данной в левом столбце подберите соответствующую позицию из правого столбца:

А	Указ, Закон, Конституция РФ	1	Муниципальные образования
Б	Постановление, Распоряжение	2	Министерства (ведомства, федеральные службы и агентства) РФ
В	Устав региона, Конституция республики	3	Губернатор
Г	Приказ, распоряжение	4	Председатель Правительства РФ
		5	Президент РФ

Запишите выбранные цифры под соответствующими буквами в поле «Ответ».
Ответ:

А	Б	В	Г

Задание на установление последовательности.
Задание 4.
Прочитайте текст и установите последовательность.

Прочитайте текст и установите последовательность.
Стадии законодательного процесса в РФ:
А. Рассмотрение законопроекта
Б. Законодательная инициатива.
В. Одобрение закона.
Г.. Принятие закона
Д. Подписание и обнародование.

Запишите соответствующую последовательность букв (цифр) слева направо без пробелов и знаков препинания в поле «Ответ»:
Ответ:

Б. Задания комбинированного типа
Задание с выбором одного верного ответа из четырёх предложенных и обоснованием выбора.

Задание 5.
Прочитайте текст, выберите один правильный вариант ответа и запишите соответствующую ему букву (цифру) в поле «Ответ». Запишите аргументы, обосновывающие выбор ответа в поле «Обоснование»

Вопрос: Вставьте в текст одно правильное слово (А. Способы, Б. Средства, В. Методы или Г. Продукты):
Средства обеспечения информационной безопасности - правовые, организационные, технические и другие ……., используемые силами обеспечения информационной безопасности.

Ответ:

Обоснование:

Задание с выбором нескольких вариантов ответа из четырёх предложенных и развёрнутым обоснованием выбора.

Задание 6.
Прочитайте текст, выберите все правильные варианты ответов и запишите соответствующие им буквы (цифры) в поле «Ответ» без пробелов и знаков препинания. Запишите аргументы, обосновывающие выбор ответа в поле «Обоснование»

Вставьте в текст одно правильное слово (А. судьба, Б. обязанность, В. желание, Г. жизнь):
Статья 2 Конституции РФ гласит:
Человек, его права и свободы являются высшей ценностью. Признание, соблюдение и защита прав и свобод человека и гражданина - _____ государства.

Ответ:

Обоснование:

В. Задания открытого типа
Задание с развёрнутым ответом.
Задание 7.
Прочитайте текст и запишите в поле «Ответ» свои аргументы, обосновывающие выбор ответа. Используйте чёткие, компактные формулировки.

Национальные интересы России – это …

Ответ:

Задание с развёрнутым ответом.
Задание 8.
Прочитайте текст и запишите в поле «Ответ» свои аргументы, обосновывающие выбор ответа. Используйте чёткие, компактные формулировки.

Какой нормативно-правовой документ определяет Стратегию противодействия экстремизму в Российской Федерации до 2025 года?

Ответ:

Распределение заданий по типам и уровням сложности по дисциплине «Информационная безопасность РФ», компетенция ПК-2, вариант № 1; 2.

Код компетенции	Индикатор сформированности компетенции	Номер задания	Тип задания	Уровень сложности задания	Время выполнения (мин.)
ПК-2. способность вырабатывать решения, учитывающие правовую и нормативную базу	***Знать:*** – З.1 – средства и методы предотвращения и обнаружения вторжений; технические каналы утечки информации; возможности технических средств перехвата информации; способы и средства защиты информации от утечки по техническим каналам и контроля эффективности защиты информации; организацию защиты информации от утечки по техническим каналам на объектах	1	Задание с выбором одного верного ответа из четырёх предложенных.	Базовый	1-3

	информатизации;. ***Уметь:*** – У.1 – пользоваться нормативными документами по противодействию технической разведке; оценивать качество готового программного обеспечения; ***Владеть:*** - В.1 – методами и средствами технической защиты информации;методами расчета и инструментального контроля показателей технической защиты информации..				
	Знать: – З.1 – средства и методы предотвращения и обнаружения вторжений; технические каналы утечки информации; возможности технических средств перехвата информации; способы и средства защиты информации от утечки по техническим каналам и контроля	2	Задание с выбором нескольких вариантов ответа из четырёх предложенных.	Базовый	1-3

	эффективности защиты информации; организацию защиты информации от утечки по техническим каналам на объектах информатизации;. ***Уметь:*** – У.1 – пользоваться нормативными документами по противодействию технической разведке; оценивать качество готового программного обеспечения; ***Владеть:*** - В.1 – методами и средствами технической защиты информации;методами расчета и инструментального контроля показателей технической защиты информации..				
	Знать: – З.1 – средства и методы предотвращения и обнаружения вторжений; технические каналы утечки информации; возможности технических средств	3	Задание на установление соответствия.	Повышенный	3-5

	перехвата информации; способы и средства защиты информации от утечки по техническим каналам и контроля эффективност и защиты информации; организацию защиты информации от утечки по техническим каналам на объектах информатизац ии;. ***Уметь:*** – У.1 – пользоваться нормативным и документами по противодейст вию технической разведке; оценивать качество готового программного обеспечения; ***Владеть:*** - В.1 – методами и средствами технической защиты информации;методам и расчета и инструментального контроля показателей технической защиты информации..				
	Знать: – З.1 – средства и методы предотвращен	4	Задание на установление последовательности.	Повышенный	3-5

	ия и обнаружения вторжений; технические каналы утечки информации; возможности технических средств перехвата информации; способы и средства защиты информации от утечки по техническим каналам и контроля эффективности защиты информации; организацию защиты информации от утечки по техническим каналам на объектах информатизации;. ***Уметь:*** – У.1 – пользоваться нормативными документами по противодействию технической разведке; оценивать качество готового программного обеспечения; ***Владеть:*** - В.1 – методами и средствами технической защиты				

	информации;методами расчета и инструментального контроля показателей технической защиты информации..				
	Знать: – З.1 – средства и методы предотвращения и обнаружения вторжений; технические каналы утечки информации; возможности технических средств перехвата информации; способы и средства защиты информации от утечки по техническим каналам и контроля эффективности защиты информации; организацию защиты информации от утечки по техническим каналам на объектах информатизации;. ***Уметь:*** – У.1 – пользоваться нормативными документами по противодействию технической	5	Задание с выбором одного верного ответа из четырёх предложенных и обоснованием выбора.	Повышенный	3-5

	разведке; оценивать качество готового программного обеспечения; ***Владеть:*** - В.1 – методами и средствами технической защиты информации;методами и расчета и инструментального контроля показателей технической защиты информации..				
	Знать: – З.1 – средства и методы предотвращения и обнаружения вторжений; технические каналы утечки информации; возможности технических средств перехвата информации; способы и средства защиты информации от утечки по техническим каналам и контроля эффективности защиты информации; организацию защиты информации от утечки по техническим каналам на объектах информатизации;.	6	Задание с выбором нескольких вариантов ответа из четырёх предложенных и развёрнутым обоснованием выбора.	Повышенный	3-5

	Уметь: – У.1 – пользоваться нормативными документами по противодействию технической разведке; оценивать качество готового программного обеспечения; ***Владеть:*** - В.1 – методами и средствами технической защиты информации;методами расчета и инструментального контроля показателей технической защиты информации..				
	Знать: – З.1 – средства и методы предотвращения и обнаружения вторжений; технические каналы утечки информации; возможности технических средств перехвата информации; способы и средства защиты информации от утечки по техническим каналам и контроля эффективности защиты	7	Задание с развёрнутым ответом.	Высокий	5-10

	информации; организацию защиты информации от утечки по техническим каналам на объектах информатизации;. ***Уметь:*** – У.1 – пользоваться нормативными документами по противодействию технической разведке; оценивать качество готового программного обеспечения; ***Владеть:*** - В.1 – методами и средствами технической защиты информации;методами и расчета и инструментального контроля показателей технической защиты информации..				
	Знать: – З.1 – средства и методы предотвращения и обнаружения вторжений; технические каналы утечки информации; возможности технических средств перехвата информации;	8	Задание с развёрнутым ответом.	Высокий	5-10

	способы и средства защиты информации от утечки по техническим каналам и контроля эффективности защиты информации; организацию защиты информации от утечки по техническим каналам на объектах информатизации;. ***Уметь:*** – У.1 – пользоваться нормативными документами по противодействию технической разведке; оценивать качество готового программного обеспечения; ***Владеть:*** - В.1 – методами и средствами технической защиты информации;методами расчета и инструментального контроля показателей технической защиты информации..				

6.2. Методические материалы

6.2.1. Методические указания для обучающихся по освоению дисциплины

Успешное усвоение курса предполагает активное, творческое участие обучающегося на всех этапах ее освоения путем планомерной, повседневной работы.

Общие рекомендации: изучение дисциплины следует начинать с проработки настоящей рабочей программы, методических указаний и разработок, указанных в программе, особое внимание уделяется целям, задачам, структуре и содержанию курса.

Методические материалы обеспечивают подготовку обучающегося к текущим аудиторным занятиям и контрольным мероприятиям для всех дисциплин учебного плана, включая конкретную учебную дисциплину: «Информационная безопасность России».

Результаты подготовки к занятиям проявляются в активности обучающегося на занятиях и в качестве выполненных контрольных работ, тестовых заданий, сделанных докладов, компьютерных презентаций и других форм текущего контроля.

Методические материалы по самостоятельной работе обучающегося включает следующие виды деятельности:

- работа со справочным материалом, предусматривающая проработку справочной и учебной литературы;
- поиск (подбор) и обзор литературы, электронных источников информации по индивидуально заданной проблеме курса, подготовка компьютерной презентации и публичного выступления по заданной проблеме;
- выполнение домашнего задания к занятию;
- выполнение домашней контрольной работы (решение заданий, подготовка творческих заданий);
- изучение материала, вынесенного на самостоятельную проработку (отдельные темы);
- подготовка к практическим занятиям;
- подготовка к контрольной работе;
- подготовка к аттестации.

Для успешного усвоения дисциплины «Информационная безопасность России» обучающийся должен систематически готовиться к практическим занятиям. Для этого необходимо:

- выполнить все задания, рассматриваемые на практических занятиях;
- выполнить все домашние задания, получаемые от преподавателя;
- систематически выполнять задания преподавателя, предлагаемые для выполнения во внеаудиторное время.

Продолжительность подготовки к практическому занятию должна составлять не менее того объема, что определено тематическим планированием в рабочей программе, то есть примерно 2 часа в неделю. Практические занятия по дисциплине «Информационная безопасность России» могут проводиться в различных формах:

- устные ответы на вопросы преподавателя;
- письменные ответы на вопросы преподавателя;
- групповое обсуждение той или иной проблемы под руководством и контролем преподавателя;
- заслушивания и обсуждение докладов;
- выполнение контрольных работ;
- подготовка компьютерных презентаций.

Подготовка к практическим занятиям должна носить систематический характер. Это позволит обучающемуся в полном объеме выполнить все требования преподавателя. Для получения более глубоких знаний обучающимся рекомендуется изучать дополнительную литературу (список приведен в рабочей программе по дисциплине).

6.2.2. Методические рекомендации (учебно-методическое обеспечение) по организации самостоятельной работы обучающихся

Внеаудиторная самостоятельная работа обучающийся (далее самостоятельная работа обучающийся) – планируемая учебная, учебно-исследовательская, научно-исследовательская работа обучающийся, выполняемая во внеаудиторное время по заданию и при методическом руководстве преподавателя, но без его непосредственного участия.

Цель самостоятельной работы обучающихся – научить осмысленно и самостоятельно работать сначала с учебным материалом, затем с научной информацией, заложить основы самоорганизации и самовоспитания с тем, чтобы привить умение в дальнейшем непрерывно повышать свою квалификацию.

Самостоятельная работа обучающихся способствует развитию самостоятельности, ответственности и организованности, творческого подхода к решению различных проблем.

Объем самостоятельной работы обучающихся определяется ФГОС и обозначен в данной рабочей программе.

Самостоятельная работа обучающихся является обязательной для каждого обучающегося и определяется учебным планом по направлению. Для успешной организации самостоятельной работы необходимы следующие условия:

- готовность обучающихся к самостоятельной работе по данной дисциплине и высокая мотивация к получению знаний;
- наличие и доступность необходимого учебно-методического и справочного материала;
- регулярный контроль качества выполненной самостоятельной работы (проверяет преподаватель во время практических занятий и консультаций, а также с помощью применения электронной почты или образовательной электронной среды);
- консультационная помощь преподавателя (проводится по расписанию, составленному на кафедре и утвержденному заведующим кафедрой).

При изучении каждой дисциплины организация СРС должна представлять единство трех взаимосвязанных форм:

1. внеаудиторная самостоятельная работа;
2. аудиторная самостоятельная работа, которая осуществляется под непосредственным руководством преподавателя;
3. творческая, в том числе научно-исследовательская работа.

Виды внеаудиторной самостоятельной работы обучающихся:

- подготовка и написание рефератов, докладов;
- подбор и изучение литературных источников;
- поиск и анализ информации по заданной теме;
- подготовка к участию в научно-практических конференциях с докладами по темам изучаемой дисциплины, смотрах, олимпиадах и др.

Виды аудиторной самостоятельной работы:

- на практических занятиях обучающиеся самостоятельно выполняют, читают и переводят тексты, выполняют тестовые задания и т.д.

Вид творческой самостоятельной работы:

- обучающийся может выбрать тему, связанную с вопросами по дисциплине и подготовить выступление, презентацию на заданную тему;
- обучающийся может выбрать заинтересовавшую его тему и развивать ее в виде доклада или статьи на студенческую конференцию. Все виды активности преподаватель фиксирует в течение семестра и обязательно учитывает при оценке знаний обучающегося по данной дисциплине.

6.2.3. Методические рекомендации освоению лекционного материала по дисциплине для обучающихся

Для качественного освоения лекционного материала учащимся рекомендуется во время лекционного занятия вести конспект лекции. Задавать все возникающие у него вопросы. Дома рекомендуется еще раз перечитать записанную лекцию, осмыслить ее и подготовить список вопросов, касающихся тех аспектов, которые не совсем были ясны.

6.2.4. Методические указания по подготовке к сдаче зачета с оценкой:

Для успешной подготовки к сдаче зачета с оценкой рекомендуется еще раз перечитать конспект лекций, просмотреть записи, сделанные на практических занятиях, просмотреть весь материал основных пособий и проделать те задания, которые были пропущены. Помимо этого рекомендуется проработать дополнительные учебные пособия, рекомендуемые к освоение данной программы.

Критерии оценки уровня и степени овладения обучающимся, заявленных в РПД, образовательных результатов

Критерии оценивания тестов

% правильных ответов	Оценка по традиционной системе
90-100	Отлично
75-89	Хорошо
60-74	Удовлетворительно
0-59	Неудовлетворительно

Критерии оценивания по устному опросу

Оценка	*Критерии оценки*
«отлично»	Выставляется, если обучающийся раскрыл содержание материала в объеме, предусмотренном программой, изложил материал грамотным языком в определенной логической последовательности, точно используя терминологию данного предмета как учебной дисциплины; отвечал самостоятельно без наводящих вопросов преподавателя; успешно ответил на тестовые задания. Возможны одна-две неточности при освещении второстепенных вопросов или в выкладках, которые обучающийся легко исправил по замечанию преподавателя.
«хорошо»	Выставляется, если ответ обучающегося удовлетворяет в основном требованиям на отметку «отлично», но при этом имеет место один из недостатков: допущены одна-две неточности при освещении основного содержания ответа, исправленные по замечанию преподавателя; допущены ошибка или более двух неточностей при освещении второстепенных вопросов или в выкладках, легко исправленные по замечанию преподавателя.
«удовлетворительно»	Выставляется если неполно или непоследовательно раскрыто содержание материала, имеются ошибки при ответах на тесты, но показано общее понимание вопроса и продемонстрированы умения, достаточные для дальнейшего усвоения материала, определенного учебной программой дисциплины.
«неудовлетворительно»	Выставляется в случаях, если не раскрыто основное содержание

	учебного материала; обнаружено незнание или неполное понимание обучающимся большей или наиболее важной части учебного материала; допущены грубые ошибки при ответах на вопросы собеседования, допущены ошибки в ответах на тесты.

Критерии оценки докладов-сообщений (по желанию дополнительно)

Оценка	*Критерии оценки*
«отлично»	Наличие четкого плана доклада. Раскрытие в докладе сути проблемы. Самостоятельность в подборе фактического материала и аналитического отношения к нему. Свободное изложение материала и четкие ответы на поставленные вопросы.
«хорошо»	Умение изложить сжато основные положения доклада. Раскрытие в докладе сути проблемы. Самостоятельность в подборе фактического материала и аналитического отношения к нему. Свободное изложение материала и ответы на поставленные вопросы с несущественными, но быстро исправляемыми докладчиком ошибками.
«удовлетворительно»	Содержательное выступление, но докладчик затрудняется сжато изложить основные положения доклада. Демонстрация обучающимся недостаточно полных знаний по теме доклада, отсутствие аргументации. Не структурированное изложение материала доклада, при ответе на вопросы допускает ошибки.

Критерии оценивания презентации

Создание слайдов	*Максимальное количество баллов*
Использование дополнительных эффектов Power Point (смена слайдов, звук, графики)	**10**
Достаточное количество слайдов (не менее 10)	**10**
Титульный лист с информационным заголовком	**5**
Заключительный слайд	**5**
Содержание	
Текст хорошо написан и сформулирован, структурирован, изложение доступное и ясное	**10**
Информация представлена с научной точки зрения, основана на объективных данных	**15**
Выводы, обоснованы, базируются на доказательной базе	**15**
Организация	
Наличие иллюстраций (графики, табл.. и т.д.)	**10**
Слайды представлены в логической последовательности	**10**
Оформление презентации, дизайн	**10**
Общие баллы	**100**
Итоговая оценка	

Форма оценивания:
«отлично»- 80 -100

«хорошо» - 45 -75
«удовлетворительно» - 30 -40
«неудовлетворительно» - менее 30

Критерии оценки по промежуточной аттестации

Критерии оценки по ПРАКТИЧЕСКИМ НАВЫКАМ И УМЕНИЯМ

Оценка	Критерии оценки
«отлично»	***Знает:*** средства и методы предотвращения и обнаружения вторжений; технические каналы утечки информации; возможности технических средств перехвата информации; способы и средства защиты информации от утечки по техническим каналам и контроля эффективности защиты информации; организацию защиты информации от утечки по техническим каналам на объектах информатизации; ***Умеет:*** пользоваться нормативными документами по противодействию технической разведке; оценивать качество готового программного обеспечения; ***Владеет:*** методами и средствами технической защиты информации; методами расчета и инструментального контроля показателей технической защиты информации.
«хорошо»	обучающийся обладает теоретическими знаниями, самостоятельно демонстрирует выполнение практических умений, допуская некоторые неточности (малосущественные ошибки), которые самостоятельно обнаруживает и быстро исправляет;
«удовлетворительно»	обучающийся обладает удовлетворительными теоретическими знаниями, демонстрирует выполнение практических умений, допуская некоторые ошибки, которые может исправить при коррекции их преподавателем;
«неудовлетворительно»	обучающийся не обладает достаточным уровнем теоретических знаний и т.п. и/или не может самостоятельно продемонстрировать практические умения или выполняет их, допуская грубые ошибки.

Критерии и шкалы для интегрированной оценки уровня сформированности компетенций

Индикаторы компетенции	Оценка сформированности компетенций			
	Не сформирована	Сформирована на уровне		
		пороговом	базовом	продвинутом
Системность и полнота знаний в отношении изучаемых объектов	Уровень знаний ниже минимальных требований. Отсутствие знаний теоретического материала. Невозможность оценить полноту знаний вследствие отказа, обучающегося от ответа	Минимально допустимый уровень знаний. Допущено много негрубых ошибки.	Уровень знаний в объеме, соответствующем программе подготовки. Допущено несколько негрубых ошибок	Уровень знаний в объеме, соответствующем программе подготовки либо превышающий программу, без ошибок.
Наличие умений	При решении стандартных задач не продемонстрированы основные умения. Имели место грубые ошибки.	Продемонстрированы основные умения. Решены типовые задачи с негрубыми ошибками. Выполнены все задания, но не в полном объеме.	Продемонстрированы все основные умения. Решены все основные задачи *с негрубыми ошибками.* Выполнены все задания, в полном объеме, но некоторые с недочетами.	Продемонстрированы все основные умения. Решены все основные задачи. Выполнены все задания, в полном Объеме без недочетов
Наличие владения (Владение опытом, освоение стандартных алгоритмов решения профессиональных задач)	При решении стандартных задач не продемонстрированы базовые навыки. Имели место грубые ошибки.	Имеется минимальный набор навыков для решения стандартных задач с некоторыми недочетами	Продемонстрированы базовые навыки при решении стандартных задач без ошибок и недочетов.	Не только владеет алгоритмом и понимает его основы, но и предлагает новые решения в рамках поставленной задачи Продемонстрирован творческий подход к решению нестандартных задач
Мотивация (личностное	*Учебная активность и*	*Учебная активность и*	*Учебная активность и*	*Учебная активность и*

Индикаторы компетенции	**Оценка сформированности компетенций**			
	Не сформирована	**Сформирована на уровне**		
		пороговом	**базовом**	**продвинутом**
отношение)	*мотивация слабо выражены, готовность решать поставленные задачи качественно отсутствуют*	*мотивация низкие, слабо выражены, стремление решать задачи качественно*	*мотивация проявляются на уровне выше среднего, демонстрируется готовность выполнять большинство поставленных задач на высоком уровне качества*	*мотивация проявляются на высоком уровне, демонстрируется готовность выполнять нестандартные дополнительные задачи на высоком уровне качества*
Дескрипторы уровня сформированности компетенций				
Характеристика сформированности компетенций	Компетенция не сформирована. Имеющихся знаний, умений, владений недостаточно для решения практических (профессиональных) задач. Требуется повторное обучение	Сформированность компетенции соответствует минимальным требованиям. Имеющихся знаний, умений, владений в целом достаточно для решения практических (профессиональных) задач, но требуется дополнительная практика по большинству практических задач.	Сформированность компетенции в целом соответствует требованиям. Имеющихся знаний, умений, владений и мотивации в целом достаточно для решения стандартных практических (профессиональных) задач.	Сформированность компетенции полностью соответствует требованиям либо превышает стандартные требования. Имеющихся знаний, умений, владений и мотивации в полной мере достаточно для применения творческого подхода к решению сложных практических (профессиональных) задач
Критерии оценивания				
	«2»	«3»	«4»	«5»
	«Не зачтено»	«зачтено»	«зачтено»	«зачтено»
Системность и полнота знаний в отношении изучаемых объектов	Не знает	Слабо знает понятия (определения)	Знает основные понятия (определения)	Знает в полном объеме
Наличие умений	Не умеет	Частично умеет	Выполняет в соответствии с требованиями	Умеет обосновать стратегию…. Способен

Индикаторы компетенции	**Оценка сформированности компетенций**			
	Не сформирована	**Сформирована на уровне**		
		пороговом	**базовом**	**продвинутом**
				обосновать….
Наличие владений (Владение опытом)	Не владеет	Частично владеет	В целом владеет	Свободно владеет
Мотивация (личностное отношение)	Не мотивирован	Низкая учебная активность	Понимает необходимость получения образования	Проявляет активность в получении качественного образования
Оценка выставляется на основании преобладающего количества критериев При наличии критерия, соответствующего «2» общая оценка выставляется «2».				