Федеральное государственное бюджетное образовательное учреждение высшего образования
РОССИЙСКАЯ АКАДЕМИЯ НАРОДНОГО ХОЗЯЙСТВА И ГОСУДАРСТВЕННОЙ СЛУЖБЫ при ПРЕЗИДЕНТЕ РОССИЙСКОЙ ФЕДЕРАЦИИ
Среднерусский институт управления – филиал
ФАКУЛЬТЕТ «Технологии, товароведение и сервис»
КАФЕДРА «Математика и информационные технологии»

Меркулов Павел Александрович

Подписан: Меркулов Павел Александрович
DN: C=RU, S=Орловская область, L=пр. Орел, T=Директор, OU="СРЕДНЕРУССКИЙ ИНСТИТУТ УПРАВЛЕНИЯ - ФИЛИАЛ ФЕДЕРАЛЬНОГО ГОСУДАРСТВЕННОГО БЮДЖЕТНОГО ОБРАЗОВАТЕЛЬНОГО УЧРЕЖДЕНИЯ ВЫСШЕГО ОБРАЗОВАНИЯ ""РОССИЙСКАЯ АКАДЕМИЯ НАРОДНОГО ХОЗЯЙСТВА И ГОСУДАРСТВЕННОЙ СЛУЖБЫ ПРИ ПРЕЗИДЕНТЕ РОССИЙСКОЙ ФЕДЕРАЦИИ""", O="ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ ""РОССИЙСКАЯ АКАДЕМИЯ НАРОДНОГО ХОЗЯЙСТВА И ГОСУДАРСТВЕННОЙ СЛУЖБЫ ПРИ ПРЕЗИДЕНТЕ РОССИЙСКОЙ ФЕДЕРАЦИИ""", СНИЛС=00482216008, ИНН=575206486423, E=it@orel.ranepa.ru, G=Павел Александрович, SN=Меркулов, CN=Меркулов Павел Александрович
Основание: я подтверждаю этот документ своей удостоверяющей подписью
Местоположение: Среднерусский институт управления

УТВЕРЖДЕНО
Директор Среднерусского института управления – филиала РАНХ и ГС
П.А. Меркулов

ПРОГРАММА БАКАЛАВРИАТА

ИНФОРМАЦИОННЫЕ СИСТЕМЫ И ТЕХНОЛОГИИ В БИЗНЕСЕ

(наименование образовательной программы)

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ,
реализуемой без применения электронного (онлайн) курса

Б1.О.17 Информационная безопасность

(код и наименование РПД)

09.03.02 Информационные системы и технологии

(код и наименование направления подготовки/специальности)

очная, очно-заочная, заочная

(форма (формы) обучения)

Год набора: 2022

Орел, 2022 г.

Автор–составитель:
к.п.н., доцент кафедры математики и информационных технологий А.А. Музалевская

И.о. заведующего кафедрой
математики и информационных технологий, доктор экономических наук, профессор Л.И. Малявкина

РПД Б1.О.17 «Информационная безопасность» одобрена на заседании кафедры математики и информационных технологий, протокол от 26 августа 2022 г., №1.

СОДЕРЖАНИЕ

1. Перечень планируемых результатов обучения по дисциплине, соотнесенных с планируемыми результатами освоения образовательной программы 4
2. Объем и место дисциплины в структуре образовательной программы 5
3. Содержание и структура дисциплины 5
4. Материалы текущего контроля успеваемости обучающихся 9
5. Оценочные материалы промежуточной аттестации по дисциплине 18
6. Методические указания для освоения дисциплины 21
7. Учебная литература и ресурсы информационно-телекоммуникационной сети Интернет 23
8. Материально-техническая база, информационные технологии, программное обеспечение и информационные справочные системы 24

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

1.1 Дисциплина Б1.О.17 «Информационная безопасность» обеспечивает овладение следующими компетенциями:

Код компетенции	Наименование компетенции	Код компонента компетенции	Наименование компонента компетенции
УК-10	Способен формировать нетерпимое отношение к проявлениям экстремизма, терроризма, коррупционному поведению и противодействовать им в профессиональной деятельности	УК-10.2	Способен противодействовать проявлениям экстремизма, терроризма, коррупционному поведению в профессиональной деятельности
ОПК-3	Способен решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно- коммуникационных технологий и с учетом основных требований информационной безопасности	ОПК-3.1	Способен решать стандартные задачи профессиональной деятельности с учетом основных требований информационной безопасности

1.2 В результате освоения дисциплины у студентов должны быть сформированы:

ОТФ/ТФ/ трудовые или профессиональные действия	Код компонента компетенции	Результаты обучения
	УК-10.2	на уровне знаний: знает основные требования информационной безопасности
		на уровне умений: умеет противодействовать проявлениям экстремизма, терроризма в профессиональной деятельности
		на уровне навыков: демонстрирует навыки противодействия проявлениям экстремизма, терроризма в профессиональной деятельности

	ОПК-3.1	на уровне знаний: знает основные требования информационной безопасности при решении стандартных задач профессиональной деятельности
		на уровне умений: умеет решать стандартные задачи профессиональной деятельности с учетом основных требований информационной безопасности
		на уровне навыков: демонстрирует навыки решения стандартных задач профессиональной деятельности с учетом основных требований информационной безопасности

2. Объем и место дисциплины в структуре образовательной программы

Объем дисциплины

Общий объем дисциплины в зачетных единицах (академических/астрономических часах): 4 ЗЕ (144/108).
Количество академических/астрономических часов, выделенных на контактную работу:
– по очной форме обучения – 52/39 (в т.ч. лекц. – 18 ч., практ. – 34 ч.); на самостоятельную работу обучающихся – 92/69;
– по очно-заочной форме обучения – 14/10,5 (в т.ч. лекц. – 4 ч., практ. – 10 ч.); на самостоятельную работу обучающихся – 126/94,5;
– по заочной форме обучения – 14/10,5 (в т.ч. лекц. – 4 ч., практ. – 10 ч.); на самостоятельную работу обучающихся – 126/94,5.

Место дисциплины в структуре образовательной программы

Дисциплина относится к дисциплинам обязательной части Блока 1. «Дисциплины (модули)» учебного плана образовательной программы.

Дисциплина изучается: очная форма обучения – 4 курс, 7 семестр; очно-заочная форма обучения – 4 курс; заочная форма обучения – 4 курс.

Освоение дисциплины опирается на содержание учебных дисциплин: Информатика; Основы национальной безопасности; Правовое регулирование в профессиональной деятельности, Информационные системы и технологии.

Основные положения дисциплины используются в дальнейшем при изучении следующих дисциплин: Комплексная система защиты информации, а также во время проведения государственной итоговой аттестации.

Форма аттестации: зачет.

3. Содержание и структура дисциплины

3.1. Структура дисциплины

Очная форма обучения

№ п/п	Наименование тем и/или разделов	Объем дисциплины (модуля), час.			Форма текущего контроля
		Всего	Контактная работа обучающихся с преподавателем	СРО	

			по видам учебных занятий					успеваемости*, промежуточной аттестации**
			Л/ ДОТ	ЛР/ ДОТ	ПЗ/ ДОТ	КСР		
Тема 1	Основы информационной безопасности и защиты информации	14	2		2		10	О
Тема 2	Понятие и классификация угроз информационной безопасности	18	2		4		12	О
Тема 3	Стандарты информационной безопасности	16	4		2		10	О
Тема 4	Правовая защита информационных ресурсов	14	2		2		10	О
Тема 5	Программные средства защиты информации	32	2		12		18	Т,К
Тема 6	Инженерно-технические методы защиты информации	14	2		2		10	О
Тема 7	Безопасность операционных систем и баз данных	20	2		6		12	О
Тема 8	Организация защиты информации в вычислительной сети	16	2		4		10	Т
Промежуточная аттестация								З
Всего:		144	18		34		92	

Примечание:
** формы заданий текущего контроля успеваемости: (контрольные работы (К), опрос (О), тестирование (Т), коллоквиум (Кол) и т.п.), кейс-задания (КЗ) и виды учебных заданий (эссе (Эс), реферат (Реф), диспут (Д) и др.),*
** форма промежуточной аттестации: экзамен (Экз), зачет(З), зачет с оценкой (ЗО)*

Очно-заочная форма обучения

№ п/п	Наименование тем и/или разделов	Объем дисциплины (модуля), час.						Форма текущего контроля успеваемости*, промежуточной аттестации**
		Всего	Контактная работа обучающихся с преподавателем по видам учебных занятий				СРО	
			Л/ ДОТ	ЛР/ ДОТ	ПЗ/ ДОТ	КСР		
Тема 1	Основы информационной безопасности и защиты информации	17	1				16	О

Тема 2	Понятие и классификация угроз информационной безопасности	17	1				16	О
Тема 3	Стандарты информационной безопасности	18					18	О
Тема 4	Правовая защита информационных ресурсов	22			2		20	О
Тема 5	Программные средства защиты информации	31	1		6		24	Т,К
Тема 6	Инженерно-технические методы защиты информации	10					10	О
Тема 7	Безопасность операционных систем и баз данных	13	1		2		10	О
Тема 8	Организация защиты информации в вычислительной сети	12					12	Т
Промежуточная аттестация								З
Всего:		140	4		10		126	

Примечание:
** формы заданий текущего контроля успеваемости: (контрольные работы (К), опрос (О), тестирование (Т), коллоквиум (Кол) и т.п.), кейс-задания (КЗ) и виды учебных заданий (эссе (Эс), реферат (Реф), диспут (Д) и др.),*
** форма промежуточной аттестации: экзамен (Экз), зачет(З), зачет с оценкой (ЗО)*

Заочная форма обучения

№ п/п	Наименование тем и/или разделов	Объем дисциплины (модуля), час.						Форма текущего контроля успеваемости*, промежуточной аттестации**
		Всего	Контактная работа обучающихся с преподавателем по видам учебных занятий				СРО	
			Л/ ДОТ	ЛР/ ДОТ	ПЗ/ ДОТ	КСР		
Тема 1	Основы информационной безопасности и защиты информации	17	1				16	О
Тема 2	Понятие и классификация угроз информационной безопасности	17	1				16	О
Тема 3	Стандарты информационной безопасности	18					18	О
Тема 4	Правовая защита информационных ресурсов	22			2		20	О

Тема 5	Программные средства защиты информации	31	1		6		24	Т,К
Тема 6	Инженерно-технические методы защиты информации	10					10	О
Тема 7	Безопасность операционных систем и баз данных	13	1		2		10	О
Тема 8	Организация защиты информации в вычислительной сети	12					12	Т
Промежуточная аттестация								З
Всего:		140	4		10		126	

Примечание:
** формы заданий текущего контроля успеваемости: (контрольные работы (К), опрос (О), тестирование (Т), коллоквиум (Кол) и т.п.), кейс-задания (КЗ) и виды учебных заданий (эссе (Эс), реферат (Реф), диспут (Д) и др.),*
** форма промежуточной аттестации: экзамен (Экз), зачет(З), зачет с оценкой (ЗО)*

3.2.Содержание дисциплины

Тема 1. Основы информационной безопасности и защиты информации

Информационные ресурсы и информационные системы. Информационные ресурсы открытые и ресурсы ограниченного доступа и использования. Классификация информации по степени конфиденциальности. Понятие информационной безопасности и защиты информации. Цели, задачи, направления исследования и практической реализации информационной безопасности. Объекты и субъекты информационной защиты. Основные задачи в организации защиты информации.

Тема 2. Виды и особенности угроз информационной безопасности

Риски угроз информационным ресурсам. Уязвимость информации. Понятие угрозы информации. Виды угроз безопасности информации.

Понятие несанкционированного канала утраты конфиденциальной информации. Классификация организационных каналов разглашения (оглашения, утраты) конфиденциальной информации. Экономические последствия утечки информации.

Тема 3. Стандарты информационной безопасности

Понятие политики безопасности. Критерии безопасности: европейские, федеральные и единые. Принципы создания систем информационной безопасности: системный подход, принцип непрерывного развития, разделение полномочий, полнота контроля, надежность системы. Оценка безопасности информационной системы. Классификация информационных систем по уровню защищенности. Структура систем информационной безопасности.

Тема 4. Правовая защита информационных ресурсов.

Информационный характер интеллектуальной и материальной собственности. Законодательные акты, охраняющие вещную собственность на документированную информацию. Защита информации институтом государственной тайны. Субъекты и объекты информационных правоотношений в области государственной тайны. Предпринимательская (коммерческая) тайна как форма защиты ценной деловой и производственной пред-

принимательской информации. Производственная тайна. Служебная тайна. Профессиональная тайна. Банковская тайна.

Тема 5. Программные средства защиты информации в компьютерах, локальных сетях и средствах связи

Программно-технические методы обеспечения информационной безопасности. Идентификация и аутентификация. Разграничение доступа. Протоколирование и аудит. Межсетевые экраны как средство защиты от несанкционированного доступа.

Понятие и классификация вредоносных программ. Троянские программы, взломщики паролей, логические бомбы, черви, вирусы. Методы и средства борьбы с вирусами. Классификация антивирусных программ. Методика применения антивирусных программ.

Криптографические средства защиты. Симметричные и асимметричные методы шифрования. Стандарты шифрования, их сравнительная характеристика. Электронная цифровая подпись.

Тема 6. Инженерно-технические методы защиты информации

Угрозы безопасности собственности фирмы и персоналу. Виды охраняемых объектов, категории защищаемых помещений. Виды, назначение, задачи и организационные формы охраны объектов, функции персонала охраны. Порядок доступа в помещения различных категорий персонала. Физические средства защиты. Классификация и характеристика классификационных групп технических средств охраны. Системы контроля доступа. Классификация экстремальных (чрезвычайных) ситуаций.

Тема 7. Безопасность операционных систем и баз данных

Сравнительная характеристика различных версий ОС с точки зрения обеспечения безопасности информации. Разграничение доступа пользователей. Ограничение доступа к отдельным файлам.

Понятие безопасности баз данных. Угрозы безопасности информации в базах данных. Подход к реализации безопасности в системах управления базами данных. Защита персональных данных.

Тема 8. Организация защиты информации в вычислительной сети

Общая характеристика организационных методов защиты информации в компьютерной сети (КС). Защита информации в КС от случайных угроз. Обеспечение конфиденциальности информации. Организация работ с конфиденциальными информационными ресурсами на объектах. Защита информации в каналах связи.

4. Материалы текущего контроля успеваемости обучающихся

4.1. В ходе реализации дисциплины Б1.О.17 «Информационная безопасность» используются следующие **методы текущего контроля успеваемости** обучающихся:

Тема и/или раздел	Методы текущего контроля успеваемости
Тема 1. Основы информационной безопасности и защиты информации	Опрос
Тема 2. Понятие и классификация угроз информационной безопасности	Опрос
Тема 3. Стандарты информационной безопасности	Опрос
Тема 4. Правовая защита информационных ресурсов	Опрос
Тема 5. Программные средства защиты информации	Тест, контрольная работа

Тема 6. Инженерно-технические методы защиты информации	Опрос
Тема 7. Безопасность операционных систем и баз данных	Опрос
Тема 8. Организация защиты информации в вычислительной сети	Тест

4.2. Типовые материалы текущего контроля успеваемости обучающихся

Примерные вопросы для опроса

Тема 1:

1. Какие компоненты входят в информационную безопасность?
2. Почему возникла необходимость в защите компьютеров?
3. Почему организации сталкиваются с проблемами при обеспечении информационной безопасности?
4. Дайте понятие объекта защиты информации.
5. Что называют информационными ресурсами?

Тема 2:

1. Что понимают под угрозой информации, дайте понятие искусственных и естественных угроз, приведите примеры.
2. Каково соотношение форм и видов уязвимости информации?
3. Дайте определение понятию «утечка информации».
4. Какова роль человеческого фактора в раскрытии информации посторонним?
5. Назовите причины и источники случайных воздействий на информационные системы.
6. Дайте характеристику преднамеренным угрозам.
7. Перечислите каналы несанкционированного доступа.

Тема 3:

1. С какой целью разрабатывались международные стандарты ИБ?
2. Назовите основные международные стандарты ИБ.
3. Какие критерии определяют степень доверия в стандарте «Оранжевая книга»?
4. Определите назначения и виды классов безопасности в «Оранжевой книге».
5. Как определяются составляющие ИБ в гармозированных критериях Европейских стран.
6. Приведите составляющие германского стандарта BSI.
7. Почему Британский стандарт BS 7799 используется наиболее часто?
8. В чем отличие применения международных стандартов ISO 15408 и ISO 17799?
9. Назовите основные этапы проведения аудита ИБ при использовании стандарта CoBiT.

Тема 4:

1. С принятием каких законов началось формирование законодательства в информационной сфере?
2. Какие общественные отношения являются предметом правового регулирования в информационной сфере?
3. Какие документы составляют правовую базу в информационной сфере?
4. В каких документах представлены нормы правового обеспечения защиты информации в компьютерных сетях?
5. Что представляет собой документ «Политика безопасности»?
6. Назовите органы, осуществляющие контроль за соблюдением требований к защите

информации.
7. На каком законе РФ основывается система защиты государственных секретов?
8. Какую информацию относят к сведениям, составляющим государственную тайну?
9. Кем установлен порядок рассекречивания и продления сроков засекречивания архивных документов?
10. Нормативно-правовое регулирование профессиональной тайны в РФ.
11. Признаки и объекты профессиональной тайны.
12. Какие сведения относятся к служебной тайне?
13. На каких правовых актах основана защита служебной и коммерческой информации на предприятии?
14. Каким законом регулируется защита персональных данных?

Тема 6:

1. Задачи и принципы инженерно-технической защиты информации.
2. Основные методы защиты информации техническими средствами.
3. Общие положения по инженерно-технической защите информации в организациях.
4. Организационные и технические меры по инженерно-технической защите информации.
5. Методические рекомендации по разработке мер инженерно-технической защиты информации
6. Общая структура системы охраны объектов.
7. Подсистема инженерной защиты.
8. Основные средства нейтрализации угроз.
9. Средства управления системой охраны. Назначение, основные характеристики.

Тема 7:

1. На какие системные параметры ОС можно повлиять с помощью реестра?
2. Что такое файл с расширением reg и для чего он нужен? Какой формат записей должен соблюдаться в этом файле?
3. Какие стандартные политики IP-безопасности предлагаются в Windows 7?
4. Как защититься от угроз, связанных с сервисами электронной почты и доставки файлов.
5. Для чего используется Центр обеспечения безопасности Windows?
6. Перечислите основные методы защиты базы данных
7. Каким образом установить защиту БД с помощью пароля?
8. Учетные записи. Алгоритм создания новой учетной записи.
9. Каким образом устанавливается защита на уровне пользователя в СУБД Access.
10. Каков порядок разработки модели угроз безопасности персональных данных?
11. Что представляет собой типовая модель угроз персональным данным, обрабатываемым в информационных системах?
12. Какова процедура определения актуальных угроз безопасности персональных данных при их обработке в информационных системах?
13. Как должны храниться персональные данные при их неавтоматизированной обработке?

Тема 8:

1. Как осуществляется стратегическое планирование автоматизации?
2. Какие существуют подходы к организации работ по автоматизации и каковы их преимущества и недостатки?
3. Как осуществляется управление рисками проекта автоматизации?
4. Какие существуют риски ИС и каковы методы реагирования на них?
5. Чем определяется качество управления проектом?

6. Назовите цели и задачи стратегического планирования ИС
7. Какой фактор оказывает наибольшее влияние на ход выполнения проекта
8. Что такое «программа проектов»?

Примерные вопросы теста

Тема 5:

1) Пароль, придуманный пользователем, который не изменяется от сеанса к сеансу называется…
а) простым
б) сложным
в) динамическим
2) Способ заражения программ, при котором код вируса приписывается к концу файла заражаемой программы, и тем или иным способом осуществляется переход вычислительного процесса на команды этого фрагмента, называется методом…
а) приписывания
б) оттеснения
в) вытеснения
3) Пароль пользователя, который изменяется для каждого нового сеанса работы или нового периода действия, называется…
а) статическим
б) динамическим
в) простым
4) Присоединяемое к тексту его криптографическое преобразование, которое позволяет при получении текста другим пользователем проверить авторство и подлинность сообщения, называется…
а) идентификатором
б) ключом
в) электронной подписью
5) Сообщение, которое необходимо передать отправителю в стеганографических системах, встраивается в…
а) контейнер
б) пароль
в) алфавит
6) Система считается безопасной, если…
а) она абсолютно недоступна для взлома
б) она управляет доступом к информации так, что только должным образом авторизованные лица или же действующие от их имени процессы получают право доступа
в) все пользователи удовлетворены работой системы
7) Наука, занимающаяся проблемой защиты информации путем ее преобразования – это…
а) криптология
б) криптография
в) криптоанализ
г) шифрование
8) Способ заражения программ, при котором код вируса располагается в начале зараженной программы, а тело самой программы приписывается к концу, называется методом…
а) оттеснения
б) вытеснения
в) стирания
9) При использовании метода «запрос-ответ» система для подтверждения подлинности пользователя…

а) последовательно задает ему ряд случайно выбранных вопросов, на которые он должен дать ответ
б) использует аппаратную проверку биометрических характеристик пользователя
в) последовательно задает ему ряд вопросов на сообразительность

10) Процесс преобразования открытых данных в зашифрованные при помощи шифра называется…
а) зашифрованием
б) расшифрованием
в) декодированием

11) Совокупность средств и методов, которые используются для формирования скрытого канала передачи информации – это…
а) система электронных ключей
б) стеганографическая система
в) система контроля

12) Защита от несанкционированного получения информации – это…
а) конфиденциальность
б) целостность
в) доступность

13) Система считается надежной, если…
а) она обеспечивает одновременную обработку информации разной степени секретности (конфиденциальности) группой пользователей без нарушения прав доступа
б) она абсолютно недоступна для взлома
в) администратор удовлетворен работой системы

14) Наука о методах защиты информации с помощью шифров – это…
а) криптология
б) криптоанализ
в) криптография

15) Для обеспечения информационной безопасности при решении стандартных задач профессиональной деятельности необходимо использовать антивирусное ПО. Какие программы относятся к антивирусным?
а) Norton AntiVirus, AVP, DrWeb
б) MS-DOS, MS Word, AVP
в) MS Word, MS Excel, Norton Commander

16) Stealth-вирусы…
а) это макровирусы
б) используют механизм перехвата управления при возникновении прерывания
в) заражают все программы на диске

17) Система шифрования Российский стандарт ГОСТ 28147-89 является системой шифрования…
а) симметричной
б) с открытым ключом
в) асимметричной

18) Из перечисленных: 1) симметричные, 2) асимметричные, 3) открытые 4) закрытые – различают системы шифрования…
а) 1, 2
б) 1, 3
в) 1, 4

19) Защита от несанкционированного изменения информации – это…
а) целостность
б) конфиденциальность
в) доступность

20) Защита от несанкционированного блокирования доступа к информационным ресурсам – это…
а) целостность
б) доступность
в) безопасность
21) Троянские кони – это…
а) программы, содержащие дополнительные скрытые функции, с помощью которых используются законные полномочия субъекта для осуществления несанкционированного доступа к информации
б) текстовые файлы, распространяемые по сети
в) все программы, содержащие ошибки
22) Некоторая последовательность символов, сохраняемая в секрете и предъявляемая пользователем при обращении к компьютерной системе – это…
а) идентификатор
б) пароль
в) шифр
23) Система шифрования DES является системой шифрования…
а) симметричной
б) с открытым ключом
в) с закрытым ключом
24) Системы шифрования, в которых для зашифрования и расшифрования используется один и тот же ключ, называются системами шифрования…
а) симметричными
б) асимметричными
в) открытыми
25) Основными составляющими информационной безопасности являются…
а) конфиденциальность, целостность, доступность
б) своевременность, актуальность, полнота
в) релевантность, толерантность
26) Из перечисленного: 1) организационно-правовая основа, 2) технико-математические аспекты, 3) юридические аспекты – организационно-правовое обеспечение защиты информации включает в себя…
а) 1, 2, 3
б) 2, 3
в) 1, 3
27) На законодательном уровне информационной безопасности особого внимания заслуживают…
а) правовые акты и стандарты
б) разделение обязанностей и минимизация привилегий
в) документирование и регламентные работы
28) Процесс преобразования зашифрованных данных в открытые при помощи ключа называется…
а) кодированием
б) расшифрованием
в) зашифрованием
29) В асимметричных системах шифрования…
а) открытый ключ доступен всем желающим, а секретный ключ известен только получателю сообщения
б) для зашифрования и расшифрования используется один ключ
в) секретный и открытый ключи доступны всем желающим

Тема 8:

1) При поиске информации в сети Интернет, необходимой для решения учебных и практических задач, необходим доступ к к файлу, созданному в прикладном программном обеспечении. Некоторая последовательность символов, сохраняемая в секрете и предъявляемая пользователем при обращении– это…
а) пароль
б) идентификатор
в) шифр
2) Что такое аутентификация при использовании поискового аппарата электронных библиотечных систем?
а) правила выбора и использования пароля
б) объекты идентификации и установления подлинности в информационной системе
в) особенности разделения привилегий и разграничения доступа
3) Для реализации требований информационной безопасности при поиске информации в сети Интернет, необходимой для решения учебных и практических задач, необходимо использовать…
а) антивирусные программы
б) операционную систему
в) прикладное ПО
4) Программные средства, применяемые для реализации требований информационной безопасности при поиске и представлении информации – это…
а) специальные программы и системы защиты информации в информационных системах различного назначения
б) текстовые, табличные и графические редакторы
в) системное программное обеспечение
5) При доступе к информационным массивам идентификация позволяет…
а) субъекту назвать себя (сообщить свое имя)
б) выявлять нетипичное поведение пользователей
в) разграничивать сетевой доступ путем фильтрации
6) Установка лицензионного программного обеспечения является …
а) обязательным критерием информационной безопасности
б) необязательным критерием информационной безопасности
бесполезной тратой корпоративных денежных средств
7) Из перечисленных: 1) аутентификация и авторизация, 2) цифровая подпись, 3) межсетевые экраны, 4) мониторинг и аудит - для защиты информационных ресурсов операционных систем используются средства…
а) 1, 4
б) 1, 2, 3, 4
в) 3, 4
8) Динамические средства, следящие за событиями в сети и фиксирующие аномалии в работе, предупреждающие администратора об угрозах, анализирующие полученную информацию и восстанавливающие разрушенные данные, называют средствами…
а) мониторинга
б) сканирования
в) экранирования
9) При ролевом управлении доступом…
а) роли могут быть приписаны многие пользователи; один пользователь может быть приписан нескольким ролям
б) роли не определяются
в) роли могут быть приписаны многие пользователи; один пользователь может быть приписан только к одной роли
10) Федеральный закон «О персональных данных» от 27 июля 2006 г. не регулирует отношения, возникающие при…

а) обработке персональных данных физическими лицами исключительно для личных и семейных нужд
б) хранении, комплектовании, учете и использовании архивных документов
в) включении в Единый государственный реестр индивидуальных предпринимателей

11) Какому принципу обеспечения безопасности персональных данных при решении стандартных задач профессиональной деятельности соответствует то, что система обеспечения информационной безопасности должна обеспечивать разделение прав и ответственности между пользователями?
а) принцип превентивности
б) принцип оптимальной и разумной разнородности
в) принцип персональной ответственности

12) Программы тестирования систем на предмет наличия в них «дыр» в механизме безопасности называют…
а) сканерами
б) аудиторами
в) мониторами

13) Контроль защищенности – это…
а) установка сигнализации
б) попытка «взлома» информационной системы, осуществляемая силами самой организации или уполномоченными лицами
в) создание вирусов и запуск их в Интернет

14) Несанкционированное отправление данных от имени другого пользователя относится к атакам на…
а) протоколы информационного обмена
б) сменные элементы системы защиты
в) постоянные элементы системы защиты

15) Присоединяемое к тексту его криптографическое преобразование, которое позволяет при получении текста другим пользователем проверить авторство и подлинность сообщения, называется…
а) идентификатором
б) ключом
в) электронной подписью

16) Задача логического управления доступом состоит в том, чтобы…
а) для каждой пары «субъект-объект» определить множество допустимых операций
б) проверять подлинность пользователя
в) фильтровать сообщения, передаваемые по каналам связи

17) Уровень безопасности данных, определяющий, каким пользователям или процессам разрешен доступ к данным, называют…
а) меткой безопасности
б) первичным ключом
в) вторичным ключом

18) Активный аудит безопасности – это…
а) оперативный аудит с автоматическим реагированием на выявленные нештатные ситуации
б) проверка бухгалтерской отчетности компьютерного центра
в) помощь правоохранительных органов

19) Совокупность соглашений относительно способа представления данных, обеспечивающего их передачу в нужных направлениях и правильную интерпретацию, называется…
а) протоколом
б) уставом
в) конституцией

20) Фоновое резервирование информации обеспечивает…
а) восстановление любых потерянных данных после реализации как случайных, так и преднамеренных угроз
б) восстановление только системной информации
в) восстановление только информации пользователей
21) Пассивный аудит – это…
а) помощь правоохранительных органов
б) анализ последствий нарушения информационной безопасности и выявление злоумышленников
в) проверка бухгалтерской отчетности компьютерного центра
22) Средства защиты объектов файловой системы основаны на…
а) определении прав пользователя на операции с файлами и каталогами
б) задании атрибутов файлов и каталогов, независящих от прав пользователей
в) управлении данными
23) Подсистема управления доступом выполняет функции…
а) бесперебойного питания устройств в сети
б) подключения устройств к сети
в) по работе с идентификаторами и паролями
24) Из перечисленных: 1) перехват передаваемых данных, 2) подключение к линии связи, 3) внедрение несанкционированного маршрутизатора - к нападениям на протоколы информационного обмена относятся…
а) 1, 2, 3
б) 1, 2
в) 3
25) Бомбардировка запросами, когда программа злоумышленника постоянно направляет ОС запросы, реакция на которые требует привлечения значительных ресурсов, относится к атакам типа…
а) отказ в обслуживании
б) сбор «мусора»
в) подбор пароля
26) Защищенные виртуальные каналы связи, представляющие собой соединение, проведенное через открытую сеть, по которому передаются криптографически защищенные пакеты сообщений виртуальной сети, называются…
а) межсетевыми экранами
б) криптозащищенными туннелями
в) бастионами
27) При решении задач профессиональной деятельности может возникнуть необходимость в обработке персональных данных. В чем заключаются законодательные меры при их защите?
а) В исполнении существующих в стране или введении новых законов, положений, постановлений и инструкций, регулирующих юридическую ответственность должностных лиц-пользователей и обслуживающего технического персонала за утечку, потерю или модификацию доверенной ему информации, подлежащей защите, в том числе за попытки выполнить аналогичные действия за пределами своих полномочий, а также ответственности посторонних лиц за попытку преднамеренного несанкционированного доступа к аппаратуре и информации
б) В разделении информации, циркулирующей в объекте защиты, на части и организации доступа к ней должностных лиц в соответствии с их функциональными обязанностями и полномочиями
в) В преобразовании информации с помощью специальных алгоритмов либо аппаратных решений и кодов ключей, т.е. в приведении ее к неявному виду

Примерный вариант контрольной работы

1. Письменный ответ на теоретический вопрос «Программно-аппаратные технологии обеспечения защиты информации в сети Интернет»

2. Решить задачи

2.1. Используя шифр перестановки, заданные ключ и алгоритм зашифровать сообщение

Номер варианта	Открытый текст	Ключ	АЛГОРИТМ
1	Информационная безопасность	КРУТО	прямой порядок следования символов ключа в алфавите

2.2. Запишите шифрограмму по следующим условиям:

- Открытый текст «шифрование сообщения»;
- Ключевое слово «ключ»;
- Алгоритм – шифр Вижинера.

Примерная тематика рефератов

1. Формирование плана работ по разработке систем защиты информации.
2. Выбор методов и средств построения систем информационной безопасности.
3. Разработка административно-организационного обеспечения информационной безопасности
4. Способы и средства защиты информации
5. Построение модели угроз информационной систем предприятия
6. Выбор средств криптографической защиты
7. Поддержка политики безопасности в стандартных программных пакетах
8. Выбор программно-аппаратных средств обеспечения информационной безопасности.
9. Построение модели нарушителя для информационной системы предприятия
10. Реализация инженерно-технической защиты информации.

Вопросы для самостоятельного изучения:

1. Структура коммерческой тайны предприятия
2. Угрозы коммерческой тайне предприятия
3. Информационные ресурсы открытые и ресурсы ограниченного доступа и использования.
4. Субъекты и объекты информационных правоотношений в области государственной тайны
5. Виды, назначение, задачи и организационные формы охраны объектов, функции персонала охраны.
6. Защита информации при проведении деловых переговоров
7. Защищенность современных операционных систем.
8. Методы и механизмы обеспечения целостности информации в реляционных базах данных
9. Разработка требований к системе защиты персональных данных.
10. Антивирусная защита персональных данных.
11. Структура государственных организаций, контролирующих защиту информации в стране.
12. Представление политик безопасности.
13. Примеры успешных решений в области политик информационной безопасности.

5. Оценочные материалы промежуточной аттестации по дисциплине

5.1. Экзамен (зачет) проводится с применением следующих методов (средств):

Зачет принимается в устной форме, по билетам. Каждый билет содержит одно практическое задание.

5.2. Оценочные материалы промежуточной аттестации

Компонент компетенции	Ключевой индикатор оценивания	Критерии оценивания
УК-10.2	Способен противодействовать проявлениям экстремизма, терроризма, коррупционному поведению в профессиональной деятельности	Демонстрирует умение противодействовать проявлениям экстремизма, терроризма, коррупционному поведению в профессиональной деятельности
ОПК-3.1	Способен решать стандартные задачи профессиональной деятельности с учетом основных требований информационной безопасности	Демонстрирует умение решать стандартные задачи профессиональной деятельности с учетом основных требований информационной безопасности

Типовые оценочные материалы промежуточной аттестации

Варианты практических (ситуационных) заданий для проведения зачета

Вариант 1. Торговая организация ведет торговлю через магазин. В магазине имеется несколько отделов, в которых работает определенное число продавцов. На основе заявок, поступающих из отделов, составляются заказы поставщикам. На основе заявок менеджеры торговой организации выбирают поставщика, формируют заказы, в которых перечисляются наименования товаров и заказываемое их количество.

Обмен информацией с поставщиками происходит по электронной почте, пересылаются текстовые и табличные документы.

Продавцы отделов ведут продажу товаров, учитывая все сделанные продажи, фиксируя номенклатуру и количество проданного товара. Кроме того, в отделе сложной бытовой техники продажи персонифицированы, в системе сохраняются сведения о покупателях.

1) Определите объекты защиты информации локальной и глобальной сети.
2) Для каждого объекта защиты определите основные события (угрозы), которые могут нарушить конфиденциальность.
3) Определите уязвимости (способы реализации этих угроз)
4) Предложите меры защиты на программном уровне

Вариант 2. В районной поликлинике осуществляется прием пациентов. В информационной системе поликлиники хранятся сведения о врачах, расписании их работы. При каждом обращении вносятся сведения в электронную карточку пациента. Врач в обязательном порядке ведет дневник (ежедневные записи о пациентах и назначениях). Кроме того, в регистратуре ведется журнал санитарно-эпидемиологической обстановки.

1) Определите объекты защиты информации.
2) Для каждого объекта защиты определите основные события (угрозы), которые могут повлиять на целостность актива, нарушить конфиденциальность.
3) Предложите меры по защите от перечисленных угроз на физическом и организационном уровнях. Приведите пример реализации организационного уровня

Вариант 3. Компания занимается разработкой программных продуктов. Директор компании заключает договор с клиентом на разработку программного продукта согласно техническому заданию. После утверждения технического задания определяется состав и объ-

ем работ, составляется предварительная смета. На каждый проект назначается ответственный за его выполнение — куратор проекта, который распределяет нагрузку между программистами и следит за выполнением технического задания.

1) Определите объекты защиты информации - сервисы, функционирование которых критично для бизнес-процессов.
2) Для каждого объекта защиты определите основные события (угрозы), которые могут повлиять на целостность или ограничить возможность использования организацией этого актива.
3) Определите уязвимости (способы реализации этих угроз)
4) Предложите меры защиты на техническом уровне

Вариант 4. Компьютерная компания занимается продажей, ремонтом, сборкой, тестированием компьютерной техники. Также специалисты компании предоставляют услуги по разработке и монтажу локальных вычислительных сетей. Вся техника и комплектующие закупаются оптом у дилеров и хранятся на складе. По желанию клиента, специалисты компании могут выехать к клиенту для общей диагностики возникшей проблемы с техникой. По результатам своей деятельности компьютерная компания производит отчисления в налоговые органы

1) Определите объекты защиты информации.
2) Для каждого объекта защиты определите основные события (угрозы), которые могут повлиять на целостность актива.
3) Предложите меры по защите от перечисленных угроз на программном уровне. Приведите пример реализации

Вариант 5. Отдел вневедомственной охраны (ОВО) занимается охраной объектов физических и юридических лиц. ОВО является коммерческим подразделением полиции. Клиент, желающий обеспечить охрану своего имущества, обращается в ОВО и составляет договор охраны. В договоре оговариваются следующие моменты: адрес объекта; план расположения помещений; количество входов/выходов; расположение окон; список лиц, отвечающих за имущество; ответственное лицо от клиента, которое будет присутствовать в момент вскрытия помещения. После заключения договора объект подключается к сигнализации. В случае срабатывания сигнализации дежурный посылает патруль на осмотр объекта и сообщает ответственному лицу клиента о данном факте. Патруль, вместе с ответственным лицом клиента, осматривает объект, проверяет сохранность имущества и работу сигнализации (в случае ложного срабатывания). После каждого выезда составляется акт, который является основанием для возбуждения уголовного дела относительно лиц, незаконно проникшим на объект.

1) Определите объекты защиты информации.
2) Для каждого объекта защиты определите основные события (угрозы), которые могут ограничить возможность использования организацией этого актива.
3) Предложите меры по защите от перечисленных угроз на организационном уровне. Приведите пример реализации

Вариант 6. В офисе компании по торговле пластиковыми окнами два помещения: кабинет руководителя и помещение, где менеджеры работают с клиентами. В кабинете руководителя 1 компьютер, подключенный к локальной сети, с последующим доступом в Интернет по телефонному кабелю и сейф. 2 АРМ менеджера также имеют выход в локальную и глобальную сеть. На компьютере руководителя имеется база данных клиентов и хранится деловая переписка. Менеджеры имеют доступ к клиентской базе.

1) Оцените угрозы персональным данным клиентов, пути реализации этих угроз.
2) Дайте характеристику необходимой системе информационной безопасности.

Вариант 7. Определите объекты защиты информации для отеля.

Для каждого объекта защиты определите основные события (угрозы), которые могут повлиять на целостность актива, нарушить конфиденциальность либо ограничить возможность использования организацией этого актива.

1) Определите уязвимости (способы реализации этих угроз).
2) Предложите меры по защите от перечисленных угроз на физическом, организационном, техническом и программном уровнях.

Вариант 8. В офисе турагентства 4 помещения: кабинет руководителя и помещение, кабинет бухгалтера, зал работы с клиентами и пост охраны. В кабинете руководителя 1 компьютер, на котором размещена клиентская база. В зале работы с клиентами 2 компьютера. В кабинете бухгалтера – 1 компьютер с финансовой отчетностью и договорами. Все компьютеры объединены в локальную сеть, с последующим доступом в Интернет по оптоволоконному каналу.

1) Определите, в каких формах представлена информация, подлежащая защите.
2) Определите объекты защиты и носители защищаемой информации, для каждого объекта определите угрозы информационной безопасности и пути их реализации.

Вариант 9. Компания занимается оптово-розничной продажей различных товаров. Офис компании находится в арендованном помещении, вместе с офисами еще 4 компаний. Пост охраны отсутствует.

Работа менеджера автоматизирована. Компьютеры подключены к локальной сети, с последующим доступом в Интернет по телефонному кабелю.

В компанию обращаются покупатели. Для каждого из них в базе данных сохраняются стандартные данные (наименование, адрес, телефон, контактное лицо). По каждой сделке формируется документ, где указан покупатель, количество купленного им товара и дата покупки.

1) Оцените угрозы персональным данным клиентов, пути реализации этих угроз.
2) Дайте характеристику необходимой системе информационной безопасности.

Вариант 10. Филиал крупного банка имеет следующие отделы: руководство, отдел кадров, бухгалтерия, отдел работы с клиентами. Информационная система филиала представлена в следующем составе:

Руководство – 3 рабочие станции: ПК директора, ПК администратора автоматизированной банковской системы, ПК Администратора ИБ.

Отдел кадров – сервер и ПК начальника отдела кадров

Бухгалтерия – сервер и ПК бухгалтера

Отдел работы с клиентами: Веб-сервер и 3 рабочие станции ПК менеджера.

1) Определите объекты защиты информации.
2) Для каждого объекта защиты определите основные события (угрозы), которые могут повлиять на целостность актива.

6. Методические указания для освоения дисциплины

Обучение по дисциплине предполагает изучение курса на аудиторных (лекционных, практических) занятиях, самостоятельную работу обучающихся и проведение контрольных мероприятий (текущей и промежуточной аттестации).

В начале учебного курса рекомендуется ознакомиться с рабочей программой дисциплины, обратив внимание на следующие ключевые моменты:

– перечень знаний, умений и навыков, которыми обучающийся должен овладеть в результате освоения дисциплины;

– тематический план проведения занятий;

– формы и материалы для проведения текущего контроля;

– учебники и учебные пособия по дисциплине, а также электронными ресурсы;

– оценочные материалы для проведения промежуточной аттестации.

С целью обеспечения успешного освоения курса обучающийся должен готовиться к лекционным и практическим занятиям.

На лекционных занятиях рекомендуется конспектировать основные положения излагаемого преподавателем материала. При подготовке к занятиям целесообразно самостоятельно прорабатывать лекционный материал, особое внимание следует уделять возникающим при этом вопросам, выделяя или выписывая указанные моменты для дальнейшего уточнения и обсуждения на последующих занятиях. В случае необходимости обращаться к преподавателю за консультацией. Таким образом, подготовка к лекции заключается в:

– внимательном прочтении материала предыдущей лекции;

– знакомстве с темой предстоящей лекции (по тематическому плану или информации лектора);

– предварительном знакомстве с учебным материалом по учебнику и учебным пособиям;

– уяснении места изучаемой темы в своей профессиональной подготовке;

– записи возможных вопросов преподавателю.

Практические занятия предполагают их проведение в различных формах (в том числе с использованием информационно-коммуникационных технологий) с целью систематизации, углубления и конкретизации полученных теоретических знаний, а также формирования навыков их применения при решении практических задач. Подготовка к практическим занятиям заключается в:

– внимательном прочтении теоретического материала лекций, относящихся к данному занятию, изучении учебного материала в рекомендуемых учебно-методических пособиях;

– ответе на приведенные в рабочей программе дисциплины вопросы для самостоятельной подготовки к занятиям лекционного, практического (семинарского) типов, лабораторным работам;

– выполнении заданий для самостоятельной работы по соответствующей теме.

В рамках практических занятий предусмотрено проведение мероприятий текущего контроля с целью выявления уровня освоения полученных знаний, умений, навыков и компетенций. Для осуществления текущего контроля в рабочей программе предусмотрены различные формы. При подготовке к контрольным мероприятиям рекомендуется ознакомиться с представленными в рабочей программе типовыми материалами для проведения текущего контроля успеваемости обучающихся.

Изучение дисциплины предполагает самостоятельное освоение обучающимся части учебного материала в соответствии с перечнем вопросов для самостоятельного изучения.

Одной из форм самостоятельной работы является подготовка реферата в соответствии с приведенной в рабочей программе тематикой. Тематика может быть расширена с учетом интересов обучающегося.

Структура реферата:

– Введение – это вступительная часть реферата, предваряющая текст. Оно должно содержать следующие элементы:

а) краткое освещение актуальности темы

б) степень ее изученности (краткий анализ научных, экспериментальных или практических достижений в той области, которой посвящен реферат);

в) определение объекта, предмета исследования;

в) цель данной работы;

г) задачи, требующие решения.

Объем введения – 2 страницы.

– Основная часть (как правило, 2-3 раздела)

В основной части реферата обучающийся дает письменное изложение материала по предложенному плану, используя источники из библиографического списка. В этом разделе работы формулируются основные понятия, их содержание, подходы к анализу, существующие в литературе, точки зрения на суть проблемы, ее характеристики. В соответствии с поставленной задачей делаются выводы и обобщения.

– Заключение

Заключение подводит итог работы. Оно может включать повтор основных тезисов работы, чтобы акцентировать на них внимание, содержать общий вывод, к которому пришел автор реферата, предложения по дальнейшей научной и практической разработке вопроса и т.п.

– Библиографический список

Объём реферата должен составлять 25-30 страниц формата А4. Для визуализации содержания и основных выводов по реферату обучающийся может подготовить презентацию с использованием соответствующего программного обеспечения.

Подготовка к промежуточной аттестации. предполагает целенаправленную, регулярную, систематическую работу при изучении дисциплины в рамках аудиторных занятий и самостоятельной работы. Систематическое выполнение учебной работы на лекциях и практических занятиях, а также в рамках самостоятельной работы позволит успешно освоить дисциплину и создать хорошую базу для успешного прохождения промежуточной аттестации. Непосредственно подготовку к процедуре аттестации рекомендуется осуществлять в соответствии с приведенным в рабочей программе перечнем типовых оценочных материалов для проведения промежуточной аттестации.

7. Учебная литература и ресурсы информационно-телекоммуникационной сети Интернет

7.1. Основная литература

1. Сычев, Ю. Н. Защита информации и информационная безопасность : учебное пособие / Ю.Н. Сычев. — Москва : ИНФРА-М, 2022. — 201 с. — (Высшее образование: Бакалавриат). — DOI 10.12737/1013711. - ISBN 978-5-16-014976-9. - Текст : электронный. - URL: https://znanium.com/catalog/product/1844364 . – Режим доступа: по подписке.

2. Баранова, Е. К. Информационная безопасность и защита информации : учебное пособие / Е.К. Баранова, А.В. Бабаш. — 4-е изд., перераб. и доп. — Москва : РИОР : ИНФРА-М, 2022. — 336 с. — (Высшее образование). — DOI: https://doi.org/10.29039/1761-6. - ISBN 978-5-369-01761-6. - Текст : электронный. - URL: https://znanium.com/catalog/product/1861657 . – Режим доступа: по подписке.

7.2. Дополнительная литература

1. Шаньгин, В. Ф. Информационная безопасность компьютерных систем и сетей : учебное пособие / В.Ф. Шаньгин. — Москва : ФОРУМ : ИНФРА-М, 2021. — 416 с. — (Среднее профессиональное образование). - ISBN 978-5-8199-0754-2. - Текст : электронный. - URL: https://znanium.com/catalog/product/1189327 . – Режим доступа: по подписке.

2. Глинская, Е. В. Информационная безопасность конструкций ЭВМ и систем : учебное пособие / Е.В. Глинская, Н.В. Чичварин. — Москва : ИНФРА-М, 2021. — 118 с. + Доп. материалы [Электронный ресурс]. — (Высшее образование: Бакалавриат). — DOI 10.12737/13571. - ISBN 978-5-16-010961-9. - Текст : электронный. - URL: https://znanium.com/catalog/product/1178152 . – Режим доступа: по подписке.

3. Информационная безопасность и вопросы профилактики кибер-экстремизма среди молодежи : сборник научных трудов / под ред., Г.Н. Чусавитиной, Л.З. Давлетки-

риевой, Е.В. Черновой. - 3-е изд., стер. - Москва : ФЛИНТА, 2019. - 161 с. - ISBN 978-5-9765-2038-7. - Текст : электронный. - URL: https://znanium.com/catalog/product/1065527 . – Режим доступа: по подписке.

7.3. Нормативные правовые документы.

1. Национальная программа «Цифровая экономика Российской Федерации» (утв. протоколом заседания президиума Совета при Президенте Российской Федерации по стратегическому развитию и национальным проектам от 4 июня 2019 г. № 7). – URL: https://digital.gov.ru/ru/activity/directions/858/?utm_referrer =https%3a%2f%2fwww.yandex.ru%2f
2. Указ Президента Российской Федерации от 09.05.2017 г. № 203 «О Стратегии развития информационного общества в Российской Федерации на 2017-2030 годы» – URL: http://www.kremlin.ru/acts/bank/41919

7.4. Интернет-ресурсы

1. Официальный портал СИУ РАНХиГС – URL: http://orel.ranepa.ru.
2. Образовательная платформа Юрайт – URL: https://urait.ru/
3. ЭБС Лань – URL: https://e.lanbook.com/
4. ЭБС Znanium – URL: https://znanium.com/
5. Официальный сайт компании «Консультант Плюс» [Электронный ресурс]. – Режим доступа: http://www.consultant.ru/, свободный.
6. Информационно-правовой портал [Электронный ресурс]. – Режим доступа: http://www.garant.ru, свободный.

7.5. Иные источники.

Не предусмотрены

8. Материально-техническая база, информационные технологии, программное обеспечение и информационные справочные системы

Материально-техническая база

Наименование специальных помещений и помещений для самостоятельной работы	Оснащенность специальных помещений и помещений для самостоятельной работы
Учебная аудитория для проведения занятий лекционного типа, семинарского типа, курсового проектирования (выполнения курсовых работ), групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации	Учебная мебель, проекционное оборудование, доска,
Учебная аудитория для проведения занятий семинарского типа, лабораторных занятий, курсового проектирования (выполнения курсовых работ), групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации	Учебная мебель, проекционное оборудование, доска.
Компьютерный класс (аудитория для выполнения самостоятельной работы) /Учебная аудитория для проведения занятий семинарского типа, курсового проектирования (выполнения курсовых работ), групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации	Учебная мебель, проекционное оборудование, компьютеры, доска. Компьютеры с выходом в сеть «Интернет» и ЭИОС СИУ РАНХиГС
Помещения для хранения и профилактического обслуживания оборудования	Комплекты специализированной мебели для хранения оборудования

Программное обеспечение

Наименование программного обеспечения	**Назначение и тип лицензии программного обеспечения**
7-Zip	Архиватор с высокой степенью сжатия Свободная лицензия
Adobe reader – Russian	Просмотр, печать и внесение аннотаций в документы PDF. Свободная лицензия
Adobe Acrobat Reader DC– Russian	Чтение, печать и рецензирование файлов PDF. Свободная лицензия
Google Chrome	Браузер Свободная лицензия
Mozilla FireFox	Браузер. Свободная лицензия
Opera	Браузер. Свободная лицензия
Yandex Браузер	Браузер Свободная лицензия
Apache Open Office	Свободный пакет офисных приложений. Свободная лицензия
Windows 7 Professional Windows 8 Pro Windows 8.1 Pro Windows 10 Pro	Операционные системы. Лицензированная версия
Office Professional Plus 2007 Office Professional Plus 2010 Office Standard 2007 Office Standard 2010 Office Standard 2013	Пакет офисных приложений. Лицензированная версия
Лицензия на право использования "КриптоАРМ Стандарт" версии 5	Работа с электронными подписями
Лицензия на право использования "КриптоПро CSP" версия 4.0.99	Работа с электронными подписями
Консультант Плюс	Справочно-правовая система