ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ

«РОССИЙСКАЯ ГОСУДАРСТВЕННАЯ АКАДЕМИЯ ИНТЕЛЛЕКТУАЛЬНОЙ СОБСТВЕННОСТИ»

УТВЕРЖДАЮ
Ректор РГАИС
А.О. Аракелова
22 мая 2025 г.

РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ

«МЕТОДЫ И СРЕДСТВА ЗАЩИТЫ ИНФОРМАЦИИ»

Направление подготовки: 09.04.02 «Информационные системы и технологии»
Профиль: «Информационные системы и технологии»
Квалификация (степень) выпускника: магистр
Форма обучения: очная

Москва – РГАИС – 2025

Разработчик: доцент кафедры Информационных технологий Трухманов В.Б. // Рабочая программа учебной дисциплины предназначена для обучающихся по направлению 09.04.02 «Информационные системы и технологии». — М.: Российская государственная академия интеллектуальной собственности (РГАИС), кафедра «Информационных технологий».

© ФГБОУ ВО РГАИС, 2025

1. ПЕРЕЧЕНЬ ПЛАНИРУЕМЫХ РЕЗУЛЬТАТОВ ОБУЧЕНИЯ ПО ДИСЦИПЛИНЕ (МОДУЛЮ), СООТНЕСЕННЫЕ С ПЛАНИРУЕМЫМИ РЕЗУЛЬТАТАМИ ОСВОЕНИЯ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

1.1. Цель и задачи дисциплины

Изучение дисциплины «Методы и средства защиты информации» направлено на получение знаний в области защиты информации с использованием современных средств и методов, получение представления у обучающихся о вызовах и угрозах в области информационной безопасности, организационном и правом обеспечении информационной безопасности, в политике безопасности компании и возможных последствиях ее нарушения, современных методах и средствах защиты информации от несанкционированного доступа, криптографических методах защиты информации, медах и средствах защиты от вредоносных программ и несанкционированного копирования. Изучение дисциплины «Методы и средства защиты информации» нацелено на понимание основных принципов компьютерной и информационной безопасности: какую информацию необходимо защищать, а какую следует держать на открытом доступе или использовать в рекламных целях; как обеспечить доступность конфиденциальной информации для сотрудников и не допустить ее утечку; как обеспечить достоверность и целостность данных в условиях многопользовательской работы.

Целью дисциплины «Методы и средства защиты информации» является формирование у обучающихся теоретических знаний, практических навыков и умений, способствующих эффективному обеспечению защиты информации и целостности данных в профессиональной деятельности.

Для достижения поставленной цели решаются следующие задачи:

– изучить основные понятия защиты информации;

– изучить основные угрозы информационной безопасности и каналов утечки информации;

– изучить организационно-правовое обеспечение информационной безопасности;

– рассмотреть инженерно-технические, программные, программно-аппаратные методы и средства защиты информации от несанкционированного доступа;

– изучить криптографические методы и средства защиты информации;

– рассмотреть различные аспекты защиты компьютерных систем от вредоносных программ;

– рассмотреть возможности современных методов и средств от несанкционированного копирования.

1.2. Место дисциплины в структуре образовательной программы

Дисциплина «Методы и средства защиты информации» (МиСЗИ) изучается в обязательной части учебного плана и реализуется на первом году обучения (1 семестр).

Место дисциплины «Методы и средства защиты информации» определено важностью проблемы информационной безопасности в современной жизни общества, необходимостью формирования знаний, умений и навыков в области противодействия угрозам информационной безопасности и защиты информации, которые необходимы современному IT-специалисту.

Содержание дисциплины «Методы и средства защиты информации» тесно связано с дисциплинами «Компьютерные сети и телекоммуникации», «Современные технологии управления проектами», «Право в индустрии компьютерных игр и киберспорте», «Международные коллаборации в сфере интеллектуальной собственности», «Цифровизация: генезис и тенденции».

2. ОБЪЕМ ДИСЦИПЛИНЫ (МОДУЛЯ) В ЗАЧЕТНЫХ ЕДИНИЦАХ С УКАЗАНИЕМ КОЛИЧЕСТВА АКАДЕМИЧЕСКИХ (АСТРОНОМИЧЕСКИХ) ЧАСОВ ПО ВИДАМ УЧЕБНЫХ ЗАНЯТИЙ

Виды занятий	Объем дисциплины		
	Форма обучения		
	Очная форма обучения	Очно-заочная форма обучения	Заочная форма обучения
Объем зачетных единиц	4	–	–
Общая трудоемкость в часах	144	–	–
Аудиторные занятия	68	–	–
Лекции	34	–	–
Практические занятия (семинары)	34	–	–
Самостоятельная работа	49	–	–
Контроль	27	–	–
Форма контроля	Экзамен	–	–

3. СОДЕРЖАНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ), СТРУКТУРИРОВАННОЕ ПО ТЕМАМ (РАЗДЕЛАМ) С УКАЗАНИЕМ КОМПЕТЕНЦИЙ, ФОРМИРУЕМЫХ В ПРОЦЕССЕ ОСВОЕНИЯ ДИСЦИПЛИНЫ (МОДУЛЯ)

3.1. Учебно-тематический план курса и распределение компетенций по темам занятий

Наименование темы	Формируемые компетенции (или их части)		
	ОПК-3	ОПК-8	ПК-5
Тема 1. Основные понятия защиты информации. Угрозы информационной безопасности и каналы утечки информации.	+		
Тема 2. Организационно-правовое обеспечение информационной безопасности.	+		
Тема 3. Инженерно-технические методы и средства защиты информации	+		
Тема 4. Программные и программно-аппаратные методы и средства защиты информации. Требования к комплексным системам защиты информации.	+	+	
Тема 5. Способы несанкционированного доступа к информации в компьютерных системах и защиты от него.	+		
Тема 6. Аутентификация пользователей на основе паролей и модели «рукопожатия».	+	+	
Тема 7. Аутентификация пользователей по их биометрическим характеристикам, клавиатурному почерку и росписи мышью.	+	+	
Тема 8. Программно-аппаратная защита информации от локального несанкционированного доступа.	+	+	+
Тема 9. Аутентификация пользователей при удаленном доступе. Защита информации от несанкционированного доступа в сетях	+		+
Тема 10. Основные понятия криптологии. Симметричные и асимметричные криптосистемы.	+	+	
Тема 11. Способы создания симметричных криптосистем. Абсолютно стойкий шифр.	+		
Тема 12. Принципы построения асимметричных криптографических систем. Электронная цифровая подпись и ее применение.	+		
Тема 13. Вредоносные программы и их классификация. Загрузочные и файловые вирусы.	+		

Тема 14. Методы обнаружения и удаления вирусов.	+		
Тема 15. Программные закладки и методы защиты от них.	+	+	
Тема 16. Основные принципы построения систем защиты от копирования. Защита инсталляционных дисков от копирования.	+	+	+
Тема 17. Методы настройки устанавливаемого программного обеспечения под характеристики компьютера. Противодействие исследованию алгоритма работы системы защиты.	+	+	+

3.2. Содержание разделов дисциплины (модуля) и контрольные вопросы для самостоятельной работы (самоконтроля обучающихся

РАЗДЕЛ 1. ОСНОВНЫЕ ПОНЯТИЯ ТЕОРИИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Тема 1. Основные понятия теории информационной безопасности. Угрозы информационной безопасности и каналы утечки информации.

Основные понятия защиты информации: информация, речевая информация, телекоммуникационная информация, документы, информационные процессы, информационные ресурсы, информатизация, собственник информации, владелец информации, пользователь информации, защищаемая информация, защита информации, утечка информации, разглашение информации, несанкционированный доступ, несанкционированное воздействие, непреднамеренное воздействие, цель защиты информации, качество информации, конфиденциальность информации, целостность информации, доступность информации, информационная безопасность, политика безопасности.

Угрозы информационной безопасности и каналы утечки информации. Угроза безопасности информации. Уязвимость информации. Атака на компьютерную систему. Естественные и искусственные угрозы, непреднамеренные и умышленные. Угроза нарушения конфиденциальности, целостности и доступности информации. Утечка информации, каналы утечки информации. Непосредственные, косвенные и потенциальные каналы утечки информации.

Контрольные вопросы:

1. В каких формах может быть представлена информация?
2. Что такое конфиденциальность информации?
3. Что такое информационная безопасность?
4. Что такое утечка информации?
5. Что понимается под несанкционированным воздействием на

защищаемую информацию?

6. Что такое политика безопасности?

7. Что понимается под угрозой безопасности информации в компьютерной системе?

8. Что такое уязвимость информации?

9. Что такое умышленные угрозы?

10. Какие существуют каналы утечки конфиденциальной информации?

11. Что такое несанкционированное искажение информации?

12. Что понимается под потенциальным каналом утечки информации?

13. В чем сущность системно-концептуального подхода к защите ин формации в компьютерных системах?

14. Почему проблема защиты информации не может быть решена с помощью только формальных методов и средств?

Тема 2. Организационно-правовое обеспечение информационной безопасности.

Организационная защита информации. Методы и средства организационной защиты информации. Мероприятия по защиты информации на различных этапах жизненного цикла. Четыре уровня правового обеспечения информационной безопасности: международные договоры; подзаконные акты, указы Президента РФ, Правительства РФ, письма высшего арбитражного суда и постановления пленумов Верховного суда; ГОСТы в области защиты информации, руководящие документы, нормы, методики и классификаторы; локальные нормативные акты, положения, инструкции по комплексной защите информации в КС конкретной организации.

Контрольные вопросы:

1. В чем сущность организационной защиты информации?
2. Что включают в себя методы и средства организационной защиты?
3. Какие основные мероприятия по защите информации должны проводиться на различных этапах жизненного цикла компьютерной системы?
4. Какие существуют уровни правового обеспечения информационной безопасности?
5. Какие законодательные акты составляют основу российского информационного права?

Тема 3. Инженерно-технические методы и средства защиты информации.

Инженерно-технические средства защиты информации. Технические средства охраны. Методы и средства защиты информации по каналам ПЭМИН (перехват побочных электромагнитных излучений и наводок): снижение уровня излучения сигнала в каналах связи; постановка помех. Средства обнаружения электронных подслушивающих устройств. Требования к проверочным мероприятиям по инженерно-технической защиты информации.

Контрольные вопросы:

1. Что относится к средствам инженерно-технической защиты ин формации и для чего они предназначены?
2. Какие существуют методы и средства защиты информации от утечки по каналам электромагнитных излучений и наводок?
3. Что такое технические средства охраны?
4. Что представляют собой электронные подслушивающие (радио закладные) устройства?
5. Какие существуют средства обнаружения электронных подслушивающих устройств?
6. Какие требования предъявляются к проверочным мероприятиям по инженерно-технической защиты информации?

Тема 4. Программные и программно-аппаратные методы и средства защиты информации. Требования к комплексным системам защиты информации.

Аппаратные средства защиты информации. Основные аппаратные средства защиты информации. Вспомогательные аппаратные средства защиты информации. Программные средства защиты информации. Программы идентификации и аутентификации пользователей, программы разграничения доступа пользователей к ресурсам компьютерных систем, программы шифрования информации, программы защиты информационных ресурсов. Преимущества и недостатки программных средств защиты информации.

Комплексная защита информации в компьютерных системах. Основные требования к комплексной системе защиты информации. «Оранжевая книга». Семь классов защищенности компьютерных систем. Руководящие документы Гостехкомиссии России по защите информации от несанкционированного доступа. Европейские «Критерии оценки безопасности информационных технологий», американские «Федеральные критерии безопасности информационных технологий», канадские «Критерии

оценки безопасности компьютерных продуктов». ГОСТ (ГОСТ РИСО/МЭК 15408–2001 «Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий».

Контрольные вопросы:

1. Что представляют собой аппаратные средства защиты информации?
2. Что такое программные средства защиты информации, каковы их достоинства и недостатки?
3. Что представляют собой программы идентификации и аутентификации пользователей?
4. Что представляют собой программы разграничения доступа пользователей к ресурсам компьютерных систем?
5. Что представляют собой программы шифрования информации?
6. Что представляют собой программы защиты информационных ресурсов?
7. Какие требования предъявляются к комплексным системам защиты информации?
8. Какие существуют международные и российские стандарты в области безопасности компьютерных систем и информационных технологий?

РАЗДЕЛ 2. МЕТОДЫ И СРЕДСТВА ЗАЩИТЫ ИНФОРМАЦИИ ОТ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА

Тема 1. Способы несанкционированного доступа к информации в компьютерных системах и защиты от него.

Основные способы несанкционированного доступа к информации в компьютерных системах. Модель нарушителя. Уровни возможностей нарушителя. Вспомогательные способы несанкционированного доступа к информации в компьютерных системах. Системы разграничения доступа субъектов к объектам доступа. Основные функции систем разграничения доступа. Аутентификация. Авторизация. Шифрование информации. Протокол идентификации пользователя. Способы аутентификации пользователей в компьютерных системах.

Контрольные вопросы:

1. Какие существуют способы несанкционированного доступа к ин формации в компьютерных системах?
2. Что такое модель нарушителя?
3. Какие уровни возможностей нарушителей выделяет Гостехкомиссия

России?

4. Какие вспомогательные способы несанкционированного доступа к информации в компьютерных системах выделяет Гостехкомиссия России?

5. Что представляют собой средства разграничения доступа?

6. Что такое протокол идентификации пользователя?

7. Какие способы аутентификации пользователей могут применяться в компьютерных системах?

8. Какой должна быть длина пароля согласно документам Гостехкомиссии России?

Тема 2. Аутентификация пользователей на основе паролей и модели «рукопожатия».

Основные правила выбора паролей. Сложность подбора паролей. Политика безопасности компании и сложность паролей безопасности. Срок действия паролей. Не повторяемость паролей. Генерация паролей. Противодействие системы попыткам подбора паролей. Реакция системы на неудачную попытку входа. Блокировка. Виды блокировок. Постоянная блокировка. Шифрование паролей. Хеширование паролей. Одноразовые пароли, их достоинства и недостатки. Аутентификацию пользователей на основе модели «рукопожатия». Преимущества аутентификации на основе модели «рукопожатия» перед парольной аутентификацией. Недостатки аутентификации на основе модели «рукопожатия»

Контрольные вопросы:

1. Что представляют собой основные правила выбора паролей?

2. Как определяется сложность подбора паролей?

3. Как взаимосвязаны политика безопасности компании и сложность подбора паролей?

4. Как взаимосвязаны политика безопасности компании, срок действия паролей и не повторяемость паролей?

5. В чем заключаются основные недостатки парольной аутентификации и как она может быть усилена?

6. Что представляет собой блокировка паролей?

7. Что такое шифрование паролей?

8. Что такое хеширование паролей?

9. В чем сущность аутентификации на основе модели «рукопожатия»?

10. Каковы достоинства и недостатки аутентификации на основе модели «рукопожатия»?

Тема 3. Аутентификация пользователей по их биометрическим характеристикам, клавиатурному почерку и росписи мышью.

Основные биометрические характеристики пользователей компьютерных систем. Программно-аппаратные средства аутентификации пользователей по их отпечаткам пальцев. Средства аутентификации пользователей, основанные на характеристиках глаза. Средства аутентификации по геометрической форме и размеру лица пользователя. Средства аутентификации по тембру голоса. Достоинства и недостатки аутентификации пользователей по их биометрическим характеристикам. Аутентификации пользователей по особенностям их работы с клавиатурой и мышью (клавиатурного почерка). Аутентификация пользователя, основанная на особенности росписи мышью. Достоинства и недостатки метода аутентификации пользователя на основе особенности росписи мышью.

Контрольные вопросы:

1. Какие биометрические характеристики пользователей могут применяться при их аутентификации?
2. Что представляют собой программно-аппаратные средства аутентификации пользователей по их отпечаткам пальцев?
3. Что представляют собой средства аутентификации пользователей, основанные на характеристиках глаза?
4. Что представляют собой средства аутентификации пользователей по геометрической форме и размеру лица?
5. Что представляют собой средства аутентификации пользователей по тембру голоса?
6. Что представляют собой средства аутентификации пользователей по особенностям их работы с клавиатурой и клавиатурному почерку?
7. Что представляют собой средства аутентификации пользователей, основанная на особенности росписи мышью?

Тема 4. Программно-аппаратная защита информации от локального несанкционированного доступа.

Двухфакторная аутентификация. Элементы аппаратного обеспечения двухфакторной аутентификации. Порядок работы программ после включения питания компьютера и до загрузки операционной системы. Средства защиты от несанкционированной загрузки операционной системы. Проект комплекса программно-аппаратных средств для защиты от локального несанкционированного доступа. Модель нарушителя. Методы

организационной защиты информации.

Контрольные вопросы:

1. Что представляют собой двухфакторная аутентификация?
2. Какие аппаратные элементы используются при двухфакторной аутентификации?
3. Каков порядок работы программ после включения питания компьютера и до загрузки операционной системы?
4. Какие существуют средства защиты от несанкционированной загрузки операционной системы?
5. Каким может быть проект комплекса программно-аппаратных средств для защиты от локального несанкционированного доступа?
6. Какие существуют методы организационной защиты информации?

Тема 5. Аутентификация пользователей при удаленном доступе. Защита информации от несанкционированного доступа в сетях.

Протокол удаленного доступа пользователя к компьютерной системе PAP (Password Authentication Protocol). Протокол удаленного доступа S/Key. Процедура аутентификации по протоколу S/Key. Протокол удаленной аутентификации CHAP (Challenge Handshake Authentication Protocol), основанный на модели «рукопожатия». Протокол Kerberos. Основные причины, облегчающие нарушителю реализацию угроз безопасности информации в распределенных КС. Методы создания безопасных распределенных КС. Межсетевые экраны (брандмауэры, firewall). Шлюзы сеансового уровня. Шлюзы прикладного уровня. Криптомаршрутизаторы.

Контрольные вопросы:

1. Что представляет собой протокол удаленного доступа пользователя к компьютерной системе PAP (Password Authentication Protocol)?
2. Что представляет собой протокол удаленного доступа S/Key?
3. Как работает процедура аутентификации по протоколу S/Key?
4. Что представляет собой протокол CHAP (Challenge Handshake Authentication Protocol)?
5. Что представляет собой протокол Kerberos?
6. Каковы причины, облегчающие нарушителю реализацию угроз безопасности информации в распределенных КС?
7. Какие существуют методы создания безопасных распределенных КС?
8. Что представляет собой Межсетевые экраны?
9. Что такое шлюзы сеансового и прикладного уровней?

10. Что представляет собой криптомаршрутизатор?

РАЗДЕЛ 3. СОВРЕМЕННЫЕ МЕТОДЫ И СРЕДСТВА ЗАЩИТЫ ИНФОРМАЦИИ

Тема 1. Криптографические методы и средства защиты информации.

Основные понятия криптологии. Открытый текст. Шифрование открытого текста. Функция шифрования. Ключ шифрования. Расшифрование. Криптосистема. Симметричная криптосистема. Ассиметричная криптосистема. Криптосистема с открытым ключом. Криптография. Дешифрование. Криптоанализ. Криптостойкость. Способы создания симметричных криптосистем. Перестановки. Подстановки. Гамирование. Абсолютно стойкий шифр. Криптографическая система DES и ее модификации. Криптографическая система ГОСТ 28147–89. Принципы построения асимметричных криптографических систем. Электронная цифровая подпись и ее применение. Компьютерная стеганография и ее применение.

Контрольные вопросы:

1. В чем разница между симметричными и асимметричными крипто графическими системами?
2. Какие основные способы применяются при создании алгоритмов симметричной криптографии?
3. В чем разница между потоковыми и блочными шифрами?
4. Какой, шифр может считаться идеальным (по К. Шеннону)?
5. Какие симметричные криптосистемы используются сегодня?
6. В каких режимах может использоваться криптосистема DES?
7. Какие из режимов DES могут использоваться для проверки аутентичности и целостности шифротекста?
8. В каких режимах может использоваться криптосистема ГОСТ 28147—89? Как в ней обеспечивается аутентичность и целостность шифротекстов?
9. Что лежит в основе асимметричной криптографии?
10. В чем особенности и основные сферы применения асимметричных криптосистем?
11. Что такое электронная цифровая подпись, как она получается и проверяется?
12. Какова роль в системах электронной цифровой подписи функций

хеширования?

13. Какую роль исполняют удостоверяющие центры? Что такое сертификат открытого ключа?

14. В чем заключаются принципы и методы компьютерной стеганографии?

15. Для решения каких задач применяются методы компьютерной стеганографии?

16. В чем разница между криптографией и стеганографией?

Тема 2. Защита компьютерных систем от вредоносных программ.

Вредоносные программы и их классификация. Компьютерные вирусы. Загрузочные и файловые вирусы. комбинированные вирусы. Вирусы спутники, паразитирующие вирусы, вирусы-невидимки, вирусы-призраки. Вирусы на основе макросов. Методы обнаружения и удаления вирусов. Программные мониторы. Антивирусные программы. Программные закладки и методы защиты от них.

Контрольные вопросы:

1. Какие программы относят к разряду вредоносных?

2. Что такое компьютерный вирус?

3. Какие существуют виды компьютерных вирусов?

4. В чем разница между загрузочными и файловыми вирусами?

5. Как происходит заражение и функционирование загрузочных вирусов?

6. Какие типы файлов могут заражаться файловыми вирусами?

7. Как происходит заражение программных файлов?

8. Почему файлы документов могут содержать вирусы?

9. Как обеспечивается автоматическое получение управления макровирусами?

10. В чем особенность макровирусов в базах данных Microsoft Access?

11. Как включить встроенную защиту от вирусов в макросах в программах Microsoft Office? В чем недостатки этой защиты?

12. Какие существуют основные каналы заражения вирусами объектов компьютерной системы?

13. Какие существуют методы автоматического обнаружения и удаления вирусов? В чем их достоинства и недостатки?

14. В чем заключается профилактика заражения компьютерными вирусами?

15. Какие виды программных закладок существуют?

16. Как может происходить проникновение программной закладки в

компьютерную систему?

17. Как осуществляется взаимодействие внедренной в КС программной закладки и нарушителя?

18. Какие существуют методы защиты от программных закладок? Что такое изолированная программная среда?

Тема 3. Защита программных средств от несанкционированного копирования.

Основные принципы построения систем защиты от копирования. Защита инсталляционных дисков от копирования. Не копируемая метка. Методы настройки устанавливаемого программного обеспечения под характеристики компьютера. Минимальный набор характеристик компьютера для настройки и их хеширование. Получение электронной подписи с помощью секретного ключа пользователя. Противодействие исследованию алгоритма работы системы защиты. Использование программ отладчиков и программ мониторинга. Возможные виды реакции программ под управлением отладчика.

Контрольные вопросы:

1. Что называется защитой программных продуктов от несанкционированного копирования?
2. На каких принципах должна основываться разработка системы за щиты от копирования?
3. Какие требования предъявляются к системам защиты от копирования?
4. Из каких основных компонентов состоит типовая система защиты от копирования?

3.3. Активные и интерактивные формы проведения занятий

В качестве активных форм проведения занятий по дисциплине «Методы и средства защиты информации» предлагаются три формы проведения занятий: лекция-беседа, консультационная работа, практическое занятие. Выбор интерактивной формы предоставляется непосредственно преподавателю.

Лекция-беседа предполагает непосредственный контакт преподавателя с аудиторией. В начале занятия обучаемые получают материалы лекции в электронном виде.

Во время занятия преподаватель знакомит обучаемых с учебным материалом, акцентируя внимание на разборе примеров. В процессе рассмотрения учебного материала они могут задавать преподавателю уточняющие вопросы. В свою очередь, преподаватель может вносить добавления, расширяющие и углубляющие содержание учебного материала, а также задавать вопросы. Вопросы преподаватель может адресовать как всей аудитории, так и кому-то конкретно. Они могут быть как простые, способные сосредоточить внимание на отдельных важнейших элементах темы, так и проблемные. Обучающиеся, продумывая ответ на заданный вопрос, получают возможность самостоятельно прийти к тем выводам и обобщениям, которые преподаватель должен был сообщить им в качестве новых знаний, либо понять глубину и важность обсуждаемой проблемы, что повышает интерес и степень восприятия материала.

Консультационная работа преподавателя предполагает два вида консультаций: групповые и индивидуальные. Групповые консультации представляют собой своеобразную форму проведения лекционных занятий, основным содержанием которых является разъяснение отдельных, часто наиболее сложных или практически значимых вопросов изучаемой программы. Групповые консультации проводятся в случаях, когда необходимо подробно рассмотреть практические вопросы, недостаточно или совсем не освещенные в лекциях, или при проведении других видов занятий, а также с целью оказания помощи в самостоятельной работе, в подготовке к выполнению лабораторных и практических занятий, в написании рефератов или выпускных работ, сдаче экзаменов и зачетов. Проведение индивидуальных консультаций проводится преподавателем в специально отведенное время. В этом случае к нему за помощью могут обратиться

как те, кто испытывает трудности в изучении данной темы, так и обучающиеся, которые хотели бы более глубоко разобраться в вопросах семинара.

Главная цель практического занятия - закрепление учебного материала, полученных во время лекционных занятий, формирование умений применять полученные знания на практике в будущей профессиональной деятельности.

4. УЧЕБНО-МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДЛЯ САМОСТОЯТЕЛЬНОЙ РАБОТЫ ОБУЧАЮЩИХСЯ ПО ДИСЦИПЛИНЕ (МОДУЛЮ)

4.1. Методические рекомендации по самостоятельному изучению курса (дисциплины)

Самостоятельная работа обучающихся – это индивидуальная или коллективная учебная деятельность, осуществляемая без непосредственного руководства преподавателя. Самостоятельная работа есть особо организованный вид учебной деятельности, проводимый с целью повышения эффективности подготовки обучающихся к последующим занятиям, формирования у них навыков самостоятельной отработки учебных заданий, а также овладения методикой организации своего самостоятельного труда в целом.

Являясь необходимым элементом дидактической связи различных методов обучения между собой, самостоятельная работа обучающихся призвана обеспечить более глубокое, творческое усвоение понятийного аппарата дисциплины, знаний возможностей и особенностей современных технологий программирования.

Во время лекций обучающимся необходимо сосредоточить внимание на её прослушивание, уловить то главное, что скажет лектор. Основные положения лекции, отдельные важные факты и выводы из рассматриваемых вопросов обучающиеся получают в электронном виде, отдельные положения важные для обучающихся нужно записывать. Записи следует делать кратко.

Главным определяющим фактором успешной работы обучающихся является его самостоятельная работа.

Следует обратить особое внимание на самостоятельное изучение предоставленных учебных материалов и рекомендованной учебной литературы. В процессе изучения учебных материалов необходимо самостоятельно разобрать теоретический материал, разобрать примеры в тои числе и в указанной среде программирования и выполнить задания для самостоятельной работы.

Успеха в заочном обучении можно добиться только при правильной организации регулярных занятий. Поэтому обучающимся необходимо систематически заниматься.

Организация самостоятельной работы обучающихся должна строиться по системе поэтапного освоения материала. Метод поэтапного изучения включает в себя предварительную подготовку, непосредственное изучение теоретического содержания источника, обобщение полученных знаний.

Предварительная подготовка включает в себя уяснение цели изучения материала, оценку широты информационной базы анализируемого вопроса, выяснение его научной и практической актуальности. Изучение теоретического содержания заключается в выделении и уяснении ключевых понятий и положений, выявлении их взаимосвязи и систематизации. Обобщение полученных знаний подразумевает широкое осмысление теоретических положений через определение их места в общей структуре изучаемой дисциплины и их значимости для практической деятельности.

Методические рекомендации по работе с литературой.

При самостоятельном изучении основной рекомендованной литературы обучающимся необходимо обратить главное внимание на узловые положения, излагаемые в изучаемом тексте.

Необходимо внимательно ознакомиться с содержанием соответствующего блока информации, структурировать его и выделить в нем центральное звено. Обычно это бывает ключевое определение или совокупность сущностных характеристик рассматриваемого объекта. Для того, чтобы убедиться, насколько глубоко усвоено содержание темы, в конце соответствующих глав и параграфов учебных пособий обычно дается перечень контрольных вопросов, на которые обучающийся должен уметь дать четкие и конкретные ответы.

Работа с дополнительной литературой предполагает умение выделять в ней необходимый аспект изучаемой темы.

В своей совокупности изучение таких подходов существенно обогащает научный кругозор обучающихся. В данном контексте следует учесть, что дополнительную литературу целесообразно прорабатывать на базе уже освоенной основной литературы, изучать комплексно и всесторонне.

Обязательный элемент самостоятельной работы обучающихся с источниками и литературой – ведение необходимых записей. Основными общепринятыми формами записей являются конспект, выписки, тезисы, аннотации, резюме, план.

Конспект – это краткое письменное изложение содержания источника, статьи, доклада, лекции, включающее в сжатой форме основные положения и их обоснование.

Выписки – это краткие записи в форме цитат (дословное воспроизведение отрывков источника, произведения, статьи, содержащих существенные положения, мысли автора), либо лаконичное, близкое к тексту изложение основного содержания.

Тезисы – это сжатое изложение ключевых идей прочитанного источника или произведения.

Аннотации, резюме – это соответственно предельно краткое обобщающее изложение содержания текста, критическая оценка прочитанного документа или произведения.

В целях структурирования содержания изучаемой работы целесообразно составлять ее план, который должен раскрывать логику построения текста, а также способствовать лучшей ориентации обучающегося в содержании произведения.

Самостоятельная работа обучающегося будет эффективной и полезной в том случае, если она будет построена исходя из понимания обучающимися необходимости обеспечения максимально широкого охвата информационных источников, что вполне достижимо при научной организации учебного труда.

4.2. Глоссарий

Антивирусная программа – специализированная программа для обнаружения компьютерных вирусов, а также нежелательных (считающихся вредоносными) программ и восстановления заражённых (модифицированных) такими программами файлов и профилактики — предотвращения заражения (модификации) файлов или операционной системы вредоносным кодом.

Аппаратные средства защиты информации – электронные и электронно-механические устройства, включаемые в состав технических средств КС и выполняющие (самостоятельно или в едином комплексе с программными средствами) некоторые функции обеспечения информационной безопасности.

Асимметричная криптосистема – криптосистема, в которой при шифровании и расшифровании используются разные ключи.

Атака на компьютерную систему – действие, предпринимаемое нарушителем, которое заключается в поиске и использовании той или иной уязвимости.

Аутентификация – подтверждение того, что предъявленное имя соответствует данному субъекту (подтверждение подлинности субъекта).

Биометрические характеристики пользователей компьютерной системы – отпечатки пальцев, геометрическая форма руки, узор радужной оболочки глаза, рисунок сетчатки глаза, геометрическая форма и размеры лица, тембр голоса, геометрическая форма и размеры уха и др.

Владелец информационных ресурсов, систем и технологий – субъект с полномочиями владения и пользования указанными объектами.

Двухфакторная аутентификация – аутентификация, при которой пользователь для входа в систему должен не только ввести пароль, но и предъявить элемент аппаратного обеспечения, содержащий подтверждающую его подлинность ключевую информацию.

Документированная информация, или документы – информация, представленная на материальных носителях вместе с идентифицирующими ее реквизитами.

Доступность информации – способность обеспечения беспрепятственного доступа субъектов к интересующей их информации.

Загрузочные вирусы – вирусы, которые заражают главный загрузочный сектор жесткого диска (Master Boot record, MBR) или загрузочный сектор раздела жесткого диска, системной дискеты или загрузочного компакт-диска (Boot Record, BR), подменяя находящиеся в них программы начальной загрузки и загрузки операционной системы своим кодом.

Защищаемая информация – информация, являющаяся предметом собственности и подлежащая защите в соответствии с требованиями правовых документов или требованиями, устанавливаемыми собственником информации.

Зашита информации – деятельность по предотвращению утечки защищаемой информации, несанкционированных и непреднамеренных воздействий на защищаемую информацию.

Идентификация – однозначное распознавание уникального имени субъекта компьютерной системы.

Инженерно-технические средства защиты информации – физические объекты, механические, электрические и электронные устройства, элементы конструкции зданий, средства пожаротушения и другие средства.

Информационная безопасность – состояние защищенности информационной среды, обеспечивающее ее формирование и развитие.

Информационная система – упорядоченная совокупность документов и массивов документов и информационных технологий, реализующих информационные процессы.

Информационные процессы – процессы сбора, обработки, накопления, хранения, поиска и распространения информации.

Информационные ресурсы – документы и массивы документов, существующие отдельно или в составе информационных систем.

Информатизация – процесс создания оптимальных условий для удовлетворения информационных потребностей граждан, организаций, общества и государства в целом.

Информация, применительно к задаче ее защиты – сведения о лицах, предметах, фактах, событиях, явлениях и процессах независимо от формы их представления.

Качество информации – совокупность свойств, обусловливающих пригодность информации удовлетворять определенные потребности ее пользователей в соответствии с назначением информации. Одним из показателей качества информации является ее защищенность — поддержание на заданном уровне тех параметров информации, которые характеризуют установленный статус ее хранения, обработки и использования.

Компьютерный вирус – автономно функционирующая программа, обладающую одновременно тремя свойствами: способностью к включению своего кода в тела других файлов и системных областей памяти компьютера, последующему самостоятельному выполнению, самостоятельному распространению в компьютерных системах.

Конфиденциальность информации — это известность ее содержания только имеющим соответствующие полномочия субъектам.

Криптосистема – совокупность реализуемых функциями шифрования и дешифрования алгоритмов, множества возможных ключей, множеств возможных открытых текстов и шифротекстов.

Макровирусы – вирусы в файлах документов, созданных программами пакета Microsoft Office, которые распространяются с помощью включенных в них макросов (процедур на языке программирования Visual Basic for Applications, VBA, или WordBasic, WB).

Маскарад – маскировка злоумышленника под легального пользователя с применением похищенной или полученной обманным путем (с помощью так называемой социальной инженерии) идентифицирующей информации.

Межсетевые экраны (брандмауэры, firewall) – программные средства, которые определяют условия прохождения пакетов данных из одной части распределенной компьютерной системы (открытой) в другую (защищенную) по особым правилам.

Методы и средства организационной защиты информации – организационно-технические и организационно-правовые мероприятия, проводимые в процессе создания и эксплуатации компьютерной системы для обеспечения защиты информации.

Мистификация – создание условий для связи по компьютерной сети легального пользователя с терминалом нарушителя, выдающего себя за легальный объект компьютерной системы (например, одного из ее серверов).

Некопируемая метка — совокупность информационных характеристик магнитного носителя, существенно изменяющаяся при его копировании.

Непреднамеренное воздействие на защищаемую информацию - воздействие на нее из-за ошибок пользователя, сбоя технических или программных средств, природных явлений, иных нецеленаправленных воздействий (например, уничтожение документов в результате отказа накопителя на жестком магнитном диске компьютера).

Несанкционированное воздействие на защищаемую информацию — воздействие с нарушением правил ее изменения (например, намеренное внедрение в защищаемые информационные ресурсы вредоносного программного кода или умышленная подмена электронного документа).

Несанкционированный доступ — получение защищаемой информации заинтересованным субъектом с нарушением правил доступа к ней.

Открытый текст – информация, содержание которой может быть понятно любому субъекту.

Политика безопасности — это набор документированных норм, правил и практических приемов, регулирующих управление, защиту и распределение информации ограниченного доступа.

Пользователь информации – субъект, обращающегося к информационной системе за получением необходимой ему информации и пользующегося ею.

Программная закладка – внешняя или внутренняя по отношению к атакуемой компьютерной системе программу, обладающую определенными разрушительными функциями по отношению к этой системе.

Протокол – конечная последовательность однозначно и точно определенных действий, выполняемых двумя или более сторонами компьютерной системы для достижения желаемого результата за конечное время.

Разглашение — это доведение защищаемой информации до неконтролируемого количества получателей информации (например, публикация информации на открытом сайте в сети Интернет или в открытой печати).

Расшифрование - процесс преобразования шифротекста в открытый текст.

Речевая информация – разновидность информации, которая возникает в ходе ведения в помещениях разговоров, работы систем связи, звукоусиления и звуковоспроизведения.

Симметричная криптосистема – криптосистема, в которой при шифровании и расшифровании используются одни и те же ключи.

Собственник информационных ресурсов, систем и технологий — это субъект с полномочиями владения, пользования и распоряжения указанными объектами.

Стеганография - методы, направленные на скрытие самого присутствия конфиденциальной информации.

Телекоммуникационная информация – разновидность информации, которая циркулирует в технических средствах обработки и хранения информации, а также в каналах связи при ее передаче.

Угроза безопасности информации в компьютерной системе – событие или действие, которое может вызвать изменение функционирования компьютерной системы, связанное с нарушением защищенности обрабатываемой в ней информации.

Утечка – неконтролируемое распространение защищаемой информации путем ее разглашения, несанкционированного доступа к ней и получения разведками.

Уязвимость информации — возможность возникновения на каком-либо этапе жизненного цикла компьютерной системы такого ее состояния, при котором создаются условия для реализации угроз безопасности информации.

Целостностью информации – неизменность информации в условиях ее случайного и (или) преднамеренного искажения или разрушения.

Цель защиты информации – предотвращение ущерба собственнику, владельцу или пользователю информации.

Шифрование – процесс преобразования открытого текста в шифротекст или криптограмму с целью сделать его содержание непонятным для посторонних лиц.

Электронная цифровая подпись - относительно небольшой по объему блок данных, передаваемый (хранящийся) вместе (реже — отдельно) с подписываемым с ее помощью документом. Механизм ЭЦП состоит из двух процедур: получение (простановка) подписи с помощью секретного ключа автора документа и проверка ЭЦП при помощи открытого ключа автора документа.

5. ОЦЕНОЧНЫЕ СРЕДСТВА ДЛЯ ТЕКУЩЕГО КОНТРОЛЯ УСПЕВАЕМОСТИ, ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ПО ИТОГАМ ОСВОЕНИЯ ДИСЦИПЛИНЫ (МОДУЛЯ)

Оценка качества освоения обучающимися образовательных программ включает в себя порядок, периодичность, систему оценок и формы проведения текущего контроля успеваемости и промежуточной аттестации обучающихся.

Нормативно-методическое обеспечение текущего контроля успеваемости и промежуточной аттестации обучающихся осуществляется в соответствии с положением ФГБОУ ВО РГАИС «Об осуществлении текущего контроля успеваемости и промежуточной аттестации обучающихся».

Основными задачами текущего контроля успеваемости является систематический мониторинг за формированием компетенций, предусмотренных ФГОС ВО и ООП, повышение качества знаний обучающихся, приобретение и развитие навыков самостоятельной работы, повышение академической активности обучающихся.

Критерии оценки обучающихся

Текущая аттестация (текущий контроль) уровня усвоения содержания дисциплины возможно проводить в ходе всех видов учебных занятий методами устного и письменного опроса (работ), в процессе выступлений обучающихся на практических занятиях, защиты рефератов, а также посредством тестирования.

Качество письменных работ оценивается исходя из того, что обучающиеся:

- выбрали и использовали форму и стиль изложения, соответствующие целям и содержанию дисциплины;
- применили связанную с темой информацию, используя при этом понятийный аппарат специалиста в данной области;
- представили структурированный и грамотно написанный текст, имеющий связное содержание.

Тестовые материалы оцениваются по процентному соотношению правильных вариантов. Количество правильных ответов в пределах от 90 до 100 % - «отлично»; в пределах от 75 до 89 % - «хорошо»; в пределах от 50 до 74 % - «удовлетворительно»; менее 50 % - «неудовлетворительно».

Сдача зачета происходит в устной форме по билетам. В ходе зачета студент должен продемонстрировать знания и умения по предмету учебного

курса. Качество ответов студентов и выполнение заданий оценивается: «зачтено», «зачтено с оценкой» и/или «не зачтено», «не зачтено с оценкой».

«зачтено», «зачтено с оценкой»:

- полные, осознанные знания в рамках курса лекций и дополнительной литературы, логичное и грамотное изложение материала.

«не зачтено» «не зачтено с оценкой»:

- допускаются существенные ошибки в знании курса лекций, при ответе вскрывается ошибочное понимание основных понятий курса.

Сдача экзамена происходит в устной форме по билетам.

Качество ответов на экзамене оцениваются на «отлично», «хорошо», «удовлетворительно» и «неудовлетворительно».

Оценка «отлично» выставляется обучающемуся, если:

- даны исчерпывающие и обоснованные ответы на все поставленные вопросы, правильно решены практические задачи;
- ответы были четкими и краткими, основные мысли излагались в строгой логической последовательности;
- обучающийся продемонстрировал умение самостоятельно анализировать факты, события, явления, процессы в их взаимосвязи и диалектическом развитии.

Оценка «хорошо» выставляется обучающемуся, если:

- даны полные, достаточно обоснованные ответы на поставленные вопросы, правильно решены практические задания;
- в ответах не всегда выделялось главное, при решении практических задач не всегда использовались рациональные методики расчётов;
- ответы в основном были краткими, но не всегда четкими.

Оценка «удовлетворительно» выставляется обучающемуся, если:

- даны в основном правильные ответы на все поставленные вопросы, но без должной глубины и обоснования, при решении практических задач студент использовал прежний опыт и не применял новые методики выполнения расчётов, однако на уточняющие вопросы даны в целом правильные ответы;
- при ответах не выделялось главное;
- ответы были многословными, нечеткими и без должной логической последовательности;
- на отдельные дополнительные вопросы не даны положительные ответы.

Оценка «неудовлетворительно» выставляется обучающемуся, если не выполнены требования, соответствующие оценке «удовлетворительно».

Обучающиеся, пропустившие свыше 75% учебного времени, не аттестуются по итогам семестра. Вопрос об аттестации таких обучающихся решается в индивидуальном порядке.

5.1. Список вопросов к экзамену

1. В каких формах может быть представлена информация?
2. Какая информация называется документированной?
3. Что относится к информации ограниченного доступа?
4. Что понимается под защитой информации?
5. Что относится к основным характеристикам защищаемой информации?
6. Что такое угроза безопасности информации? Каковы основные виды угроз?
7. Какие существуют каналы утечки конфиденциальной информации?
8. В чем сущность организационной защиты информации?
9. Каковы уровни правового обеспечения информационной безопасности?
10. Какие законодательные акты составляют основу российского информационного права?
11. Что относится к средствам инженерно-технической защиты информации и для чего они предназначены?
12. В чем заключаются достоинства и недостатки программных средств защиты информации?
13. Какие требования предъявляются к комплексным системам защиты информации?
14. Какие существуют международные и российские стандарты в области безопасности компьютерных систем и информационных технологий?
15. Какие существуют способы несанкционированного доступа к информации в компьютерных системах?
16. Какие способы аутентификации пользователей могут применяться в компьютерных системах?
17. В чем заключаются основные недостатки парольной аутентификации и как она может быть усилена?
18. В чем сущность, достоинства и недостатки аутентификации на основе модели «рукопожатия»?

19. Какие биометрические характеристики пользователей могут применяться для их аутентификации? В чем преимущества подобного способа подтверждения подлинности?

20. В чем специфика аутентификации пользователей на основе их клавиатурного почерка и росписи мышью?

21. Какие элементы аппаратного обеспечения могут применяться для хранения идентифицирующей информации для пользователей компьютерных систем?

22. Что называют двухфакторной аутентификацией?

23. В чем разница между симметричными и асимметричными криптографическими системами?

24. Какие основные способы применяются при создании алгоритмов симметричной криптографии?

25. Что лежит в основе асимметричной криптографии?

26. Что такое электронная цифровая подпись, как она получается и проверяется?

27. Какова роль в системах электронной цифровой подписи функций хеширования?

28. В чем заключаются принципы и методы компьютерной стеганографии?

29. Для решения каких задач применяются методы компьютерной стеганографии?

30. В чем разница между криптографией и стеганографией?

31. Какие программы относят к разряду вредоносных?

32. Что такое компьютерный вирус и какие существуют виды компьютерных вирусов?

33. В чем разница между загрузочными и файловыми вирусами?

34. Как происходит заражение и функционирование загрузочных вирусов?

35. Как происходит заражение программных файлов?

36. Почему файлы документов могут содержать вирусы?

37. Как обеспечивается автоматическое получение управления макровирусами?

38. Какие существуют основные каналы заражения вирусами объектов компьютерной системы?

39. Какие существуют методы автоматического обнаружения и удаления вирусов? В чем их достоинства и недостатки?

40. В чем заключается профилактика заражения компьютерными

вирусами?

41. Какие виды программных закладок существуют?

42. Как может происходить проникновение программной закладки в компьютерную систему?

43. Как осуществляется взаимодействие внедренной в КС программной закладки и нарушителя?

44. Какие существуют методы защиты от программных закладок? Что такое изолированная программная среда?

5.2. Тестовые задания

1. Электронные и электронно-механические устройства, включаемые в состав технических средств компьютерной системы и выполняющие некоторые функции обеспечения информационной безопасности, называются:

a) аппаратными средствами защиты информации;
b) антивирусной программой;
c) криптографической системой защиты информации;
d) электронным сторожем.

2. Специализированная программа для обнаружения компьютерных вирусов, а также нежелательных программ, восстановления заражённых такими программами файлов и предотвращения заражения файлов или операционной системы вредоносным кодом, называется:

a) системной программой;
b) антивирусной программой;
c) лечебной программой;
d) операционной системой.

3. Криптосистема, в которой при шифровании и расшифровании используются разные ключи, называется

a) двухфазной системой;
b) ключевой системой;
c) симметричной криптосистемой;
d) асимметричной криптосистемой.

4. Подтверждение того, что предъявленное имя соответствует данному субъекту, называется

a) изоляцией;
b) аутизмом;
c) аутентификацией;
d) персонализацией.

5. Способность обеспечения беспрепятственного доступа субъектов к интересующей их информации, называется:

a) **доступностью информации;**
b) защитой информации;
c) легализацией информации;
d) симметричностью информации.

6. Аутентификация, при которой пользователь для входа в систему должен не только ввести пароль, но и предъявить элемент аппаратного обеспечения, содержащий подтверждающую его подлинность ключевую информацию, называется:

a) двойной проверкой;
b) двойной защитой;
c) двухфакторной аутентификацией;
d) симметричной криптосистемой.

7. Вирусы, которые заражают главный загрузочный сектор жесткого диска (Master Boot record, MBR) или загрузочный сектор раздела жесткого диска, подменяя находящиеся в них программы начальной загрузки и загрузки операционной системы своим кодом, называются:

a) загрузочными вирусами;
b) рекламными вирусами;
c) полифагом;
d) fire wall.

8. Упорядоченная совокупность документов и массивов документов и информационных технологий, реализующих информационные процессы, называется:

a) информационной системой;
b) политикой безопасности;

c) информационной технологией;
d) информационным процессором.

9. Деятельность по предотвращению утечки защищаемой информации, несанкционированных и непреднамеренных воздействий на защищаемую информацию, называется:

a) бдительностью;
b) борьбой с утечкой;
c) зашитой информации;
d) политикой безопасности.

10. Процессы сбора, обработки, накопления, хранения, поиска и распространения информации, называются:

a) базой данных;
b) жизненным циклом информации;
c) информационными процессами;
d) информационными процессорами.

11. Вирусы в файлах документов, созданных программами пакета Microsoft Office, которые распространяются с помощью включенных в них макросов (процедур на языке программирования Visual Basic for Applications, VBA, или WordBasic, WB), называются:

a) вирусами червями;
b) макровирусами;
c) бумажными клещами;
d) полифагами.

12. Автономно функционирующая программа, обладающую одновременно тремя свойствами: способностью к включению своего кода в тела других файлов и системных областей памяти компьютера, последующему самостоятельному выполнению, самостоятельному распространению в компьютерных системах, называется:

a) компьютерным вирусом;
b) автопрограммой;
c) криптографией;
d) резидентной программой.

13. Маскировка злоумышленника под легального пользователя с применением похищенной или полученной обманным путем (с помощью так называемой социальной инженерии) идентифицирующей информации, называется:

a) мимикрией;
b) разносчиком пиццы;
c) импресарио;
d) маскарадом.

14. Получение защищаемой информации заинтересованным субъектом с нарушением правил доступа к ней, называется

a) несанкционированным доступом;
b) компьютерным шпионажем;
c) кражей информации;
d) взломом информации.

15. Набор документированных норм, правил и практических приемов, регулирующих управление, защиту и распределение информации ограниченного доступа, называется:

a) защитой информации;
b) политикой безопасности;
c) стратегией защиты информации;
d) правилами поведения.

16. Информация, содержание которой может быть понятно любому субъекту, называется:

a) сказкой;
b) инструкцией хакера;
c) криптосистемой;
d) открытым текстом.

17. Доведение защищаемой информации до неконтролируемого количества получателей информации (например, публикация информации на открытом сайте в сети Интернет или в открытой печати):

a) компьютерным шпионажем;
b) разглашением;
c) вредительством;

d) предательством.

18. Процесс преобразования шифротекста в открытый текст, называется:

a) шифрованием;
b) открытием кода;
c) расшифрованием;
d) преобразованием кода.

19. Субъект с полномочиями владения информационными ресурсами, их пользования и распоряжения, называется

a) сетевым администратором;
b) собственником информационных ресурсов;
c) программистом;
d) пользователем.

20. Криптосистема, в которой при шифровании и расшифровании используются одни и те же ключи, называется:

a) симметричной криптосистемой;
b) продольной криптосистемой;
c) простой ключевой системой;
d) однородной кодовой системой.

21. Событие или действие, которое может вызвать изменение функционирования компьютерной системы, связанное с нарушением защищенности обрабатываемой в ней информации, называется:

a) угрозой безопасности информации;
b) хакерской атакой;
c) вирусной атакой;
d) потерей протокола безопасности.

22. Неконтролируемое распространение защищаемой информации путем ее разглашения, несанкционированного доступа к ней и получения разведками:

a) расползанием информации;
b) информационным предательством;
c) вредительством;
d) утечкой.

23. Процесс преобразования открытого текста в шифротекст или криптограмму с целью сделать его содержание непонятным для посторонних лиц:

a) криптографированием;
b) дешифрованием;
c) шифрованием;
d) ниделированием.

24. Возможность возникновения на каком-либо этапе жизненного цикла компьютерной системы такого ее состояния, при котором создаются условия для реализации угроз безопасности информации, называется:

a) устареванием политики безопасности;
b) сбоем системы защиты информации;
c) уязвимостью информации;
d) обходом защиты информации.

25. Программные средства, которые определяют условия прохождения пакетов данных из одной части распределенной компьютерной системы (открытой) в другую (защищенную) по особым правилам, называются:

a) межсетевыми экранами;
b) защитными ширмами;
c) подсмотрщиками;
d) антишпионами.

26. Атрибут электронного документа, который позволяет установить авторство и неизменность после подписания, называется:

a) астрибутивом;
b) электронной подписью;
c) провайзером.

27. Действие, предпринимаемое нарушителем, которое заключается в поиске и использовании той или иной уязвимости, называется:

a) спинанием;
b) инкременцией системы;

c) атакой на компьютерную систему.

28. Однозначное распознавание уникального имени субъекта компьютерной системы, называется:

a) рекриацией;
b) идентификацией;
c) паспортеризацей.

29. Совокупность свойств, обусловливающих пригодность информации удовлетворять определенные потребности ее пользователей в соответствии с назначением информации, называется:

a) качеством информации;
b) избирательностью информации;
c) удовлетворительностью информации.

30. Воздействие на защищаемую информацию из-за ошибок пользователя, сбоя технических или программных средств, природных явлений, иных нецеленаправленных воздействий, называется:

a) непреднамеренным воздействием;
b) самоатакой;
c) глюком.

Ключ
к версии теста по дисциплине
«Методы и средства защиты информации»

1	2	3	4	5
a	b	d	c	a
6	7	8	9	10
c	a	a	c	c
11	12	13	14	15
b	a	d	a	b
16	17	18	19	20
d	b	c	b	a
21	22	23	24	25
a	d	c	c	a
26	27	28	29	30
b	c	b	a	c

6. ПЕРЕЧЕНЬ ОСНОВНОЙ И ДОПОЛНИТЕЛЬНОЙ УЧЕБНОЙ ЛИТЕРАТУРЫ, НЕОБХОДИМОЙ ДЛЯ ОСВОЕНИЯ ДИСЦИПЛИНЫ (МОДУЛЯ)

6.1. Основная и дополнительная учебная литература

Основная литература

1. Белоус, А. И. Основы кибербезопасности : стандарты, концепции, методы и средства обеспечения / А. И. Белоус, В. А. Солодуха. – Москва : Техносфера, 2021. – 482 с. : схем., ил., табл. – Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book&id=617523. – ISBN 978-5-94836-612-8. – Текст : электронный.
2. Солдаткина, М. В. Теоретико-вероятностный подход к проблемам криптографии / М. В. Солдаткина. – Москва ; Берлин : Директ-Медиа, 2021. – 60 с. – Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book&id=602506. – Библиогр.: с. 54-56. – ISBN 978-5-4499-1734-8. – Текст : электронный.
3. Технологии обеспечения безопасности информационных систем : учебное пособие / А. Л. Марухленко, Л. О. Марухленко, М. А. Ефремов [и др.]. – Москва ; Берлин : Директ-Медиа, 2021. – 210 с. : ил., схем., табл. – Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book&id=598988 . – Библиогр.: с. 196-205. – ISBN 978-5-4499-1671-6. – DOI 10.23681/598988. – Текст : электронный.

Дополнительная литература

1. Гисин, В. Б. Криптография и распределенные реестры : учебное пособие / В. Б. Гисин ; Финансовый университет при Правительстве Российской Федерации. – Москва : Прометей, 2022. – 186 с. : табл., схем. – Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book&id=700941 . – Библиогр. в кн. – ISBN 978-5-00172-257-1. – Текст : электронный.
2. Егошина, И. Л. Средства и методы обеспечения безопасности объектов и защиты информации : практикум / И. Л. Егошина ; Поволжский государственный технологический университет. – Йошкар-Ола : Поволжский государственный технологический университет, 2021. – 158 с. : схем., табл., ил. – Режим доступа: по подписке. – URL:

https://biblioclub.ru/index.php?page=book&id=696349 . – Библиогр. в кн. – ISBN 978-5-8158-2240-5. – Текст : электронный.

3. Ищейнов, В. Я. Информационная безопасность и защита информации : теория и практика : учебное пособие / В. Я. Ищейнов. – Москва ; Берлин : Директ-Медиа, 2020. – 271 с. : схем., табл. – Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book&id=571485. – Библиогр. в кн. – ISBN 978-5-4499-0496-6. – DOI 10.23681/571485. – Текст : электронный..

Библиотечный фонд Академии укомплектован печатной или электронной основной учебной литературой по дисциплинам базовой части всех циклов, изданными за последние 5 лет.

Фонд дополнительной литературы включает в себя официальные справочно-библиографические и периодические издания в расчете не менее одного экземпляра на каждые 100 обучающихся. Каждому обучающемуся обеспечен доступ к комплектам библиотечного фонда и периодическое издание из следующего перечня: Копирайт; wipo magazine; Библиотековедение; Биржа интеллектуальной собственности (БИС); Бюллетень Министерства юстиции Российской Федерации; Вестник гражданского права; Государство и право; Инновации; Интеллектуальная собственность. Авторское право и смежные права; Интеллектуальная собственность. Промышленная собственность; Международное публичное и частное право; Общество: социология, психология, педагогика; Патентный поверенный; Патенты и лицензии. Интеллектуальные права; Уголовное право; Управление проектами и программами; Хозяйство право; Экономическая политика.

7. ПЕРЕЧЕНЬ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ, ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ, ИНФОРМАЦИОННО-СПРАВОЧНЫХ СИСТЕМ И РЕСУРСОВ СЕТИ «ИНТЕРНЕТ», НЕОБХОДИМЫХ ДЛЯ ОСВОЕНИЯ ДИСЦИПЛИНЫ (МОДУЛЯ)

В процессе реализации образовательной программы в вузе применяются современные интерактивные и мультимедийные средства обучения (компьютеры, мультимедиа-проекторы, интерактивные доски и др.), тематические стенды и плакаты, а также электронные информационные образовательные ресурсы.

На основе аппаратно-программного комплекса в РГАИС функционирует и постоянно совершенствуется портал электронного обучения и дистанционных образовательных технологий (ЭОиДОТ), обеспечиваемый преимущественно авторским учебным контентом и методическими разработками профессорско-преподавательского состава Академии.

В РГАИС функционируют читальный зал и электронная библиотека. Сотрудникам и обучающимся обеспечен доступ к электронной библиотечной системе «Университетская библиотека онлайн», насчитывающей более 100 тысяч наименований изданий с доступом в режиме онлайн, а также к объектам Национальной электронной библиотеки (в соответствии с договором с ФГБУ «Российская государственная библиотека»).

Имеется компьютерный класс, возможности которого позволяют каждому из обучающихся работать на компьютере с установленным комплектом лицензионного программного обеспечения не менее 20 часов в год. Академия обеспечена необходимым комплектом лицензионного программного обеспечения

Электронная информационно-образовательная среда Академии обеспечивает:

- доступ к учебным планам, рабочим программам дисциплин (модулей), практик, к изданиям электронных библиотечных систем и электронным образовательным ресурсам, указанным в рабочих программах;
- фиксацию хода образовательного процесса, результатов промежуточной аттестации и результатов освоения программы;
- формирование электронного портфолио обучающегося, в том числе сохранение его работ и оценок за эти работы.
- доступ к современным профессиональным базам данных, информационным справочным и поисковым системам, в том числе:

справочно-правовой системе «Гарант»: www.garant.ru; справочно-правовой системе «Консультант плюс»: www.consultant.ru; библиотеке «Книгофонд»: www.knigafund.ru; Университетской библиотеке www.biblioclub.ru.

8. МАТЕРИАЛЬНО-ТЕХНИЧЕСКАЯ БАЗА, НЕОБХОДИМАЯ ДЛЯ ОСУЩЕСТВЛЕНИЯ ОБРАЗОВАТЕЛЬНОГО ПРОЦЕССА ПО ДИСЦИПЛИНЕ (МОДУЛЮ)

Для ведения образовательной деятельности по данной дисциплине Академия располагает материально-технической базой, обеспечивающей проведение всех видов лабораторной, практической и научно-исследовательской работы обучающихся, предусмотренных учебным планом РГАИС, и соответствующей действующим санитарным и противопожарным правилам и нормам.

Для организации и ведения учебного процесса Академия располагает зданием общей площадью 5936,2 кв.м, учебная и учебно-лабораторная площадь составляет 1249,6 кв.м. Для питания сотрудников и обучающихся имеется столовая площадью 130,1 кв.м.

Аудиторные занятия проводятся в специальных помещениях, представляющих собой учебные аудитории для проведения занятий лекционного типа, занятий семинарского типа, курсового проектирования (выполнения курсовых работ), групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации, а также в помещениях для самостоятельной работы. Имеются помещения для хранения и профилактического обслуживания учебного оборудования. Специальные помещения укомплектованы специализированной мебелью и техническими средствами обучения, служащими для представления учебной информации большой аудитории.

Для проведения занятий лекционного типа имеются наборы демонстрационного оборудования и учебно-наглядных пособий, обеспечивающие тематические иллюстрации, соответствующие примерным программам дисциплин (модулей), рабочим учебным программам дисциплин (модулей).

Помещения для самостоятельной работы обучающихся оснащены компьютерной техникой с возможностью подключения к сети «Интернет» и обеспечением доступа в электронную информационно-образовательную среду организации.

9. ОСОБЕННОСТИ ОБУЧЕНИЯ ЛИЦ С ОГРАНИЧЕННЫМИ ВОЗМОЖНОСТЯМИ ЗДОРОВЬЯ

Организация образовательного процесса для лиц с ограниченными возможностями здоровья осуществляется в соответствии с приказом Минобрнауки России от 9 июня 2016 г. № 694 «О внесении изменений в административные регламенты предоставления государственных услуг в части обеспечения условий доступности государственных услуг для инвалидов», «Методическими рекомендациями по организации образовательного процесса для инвалидов и лиц с ограниченными возможностями здоровья в образовательных организациях высшего образования, в том числе оснащенности образовательного процесса» Министерства образования и науки РФ от 08.04.2014 г. № АК-44/05вн.

Академия предоставляет инвалидам и лицам с ограниченными возможностями здоровья (по их заявлению) возможность обучения по образовательной программе, учитывающей особенности их психофизического развития, индивидуальных возможностей и при необходимости, обеспечивающей коррекцию нарушений развития и социальную адаптацию указанных лиц. Для инвалидов и лиц с ограниченными возможностями здоровья Академия устанавливает особый порядок освоения дисциплин (модулей).

Подбор и разработка учебных материалов для обучающихся с ограниченными возможностями здоровья производится с учетом их индивидуальных особенностей.

Предусмотрена возможность обучения по индивидуальному графику.