

Федеральное государственное бюджетное образовательное учреждение
инклюзивного высшего образования

«МОСКОВСКИЙ ГОСУДАРСТВЕННЫЙ ГУМАНИТАРНО-
ЭКОНОМИЧЕСКИЙ УНИВЕРСИТЕТ»

Факультет Прикладной математики и информатики
Кафедра Информационных технологий и прикладной математики

УТВЕРЖДАЮ

И.о. проректора по ООД



Пузанкова Е.Н.

« 30 » августа 2019 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ
СОВРЕМЕННЫЕ МЕТОДЫ И СРЕДСТВА ЗАЩИТЫ ИНФОРМАЦИИ

образовательная программа направления подготовки
01.04.02 «Прикладная математика и информатика»
Блок Б1.О.10 «Дисциплины (модули)», обязательная часть

Профиль подготовки
Математическое и программное обеспечение информационных систем в
прикладных областях

Квалификация
Магистр


Форма обучения: очная

Курс 1 семестр 2

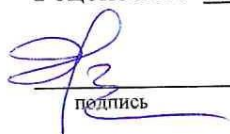
Москва 2019

Рабочая программа составлена на основании федерального государственного образовательного стандарта высшего образования по направлению подготовки 01.04.02 «Прикладная математика и информатика (уровень магистратуры)», утвержденного приказом Министерства образования и науки Российской Федерации № 13 от 10 января 2018 г. Зарегистрировано в Минюсте России 06 февраля 2018 г. №49939.

Составители рабочей программы: МГТЭУ, доцент кафедры ИМиПМ
место работы, занимаемая должность

 Петрунина Е.В. «20» августа 2019 г.
подпись Ф.И.О. Дата

Рецензент: МГТЭУ, доцент кафедры ИТиПМ
место работы, занимаемая должность


 Никольский А.Е. «21» августа 2019 г.
подпись Ф.И.О. Дата

Рабочая программа утверждена на заседании кафедры Информационных технологий и прикладной математики (протокол № 1 от «26» августа 2019 г.)

/Зав. кафедрой ИТиПМ/  Петрунина Е.В. «26» августа 2019 г.
подпись Ф.И.О. Дата


СОГЛАСОВАНО

Начальник
Учебного отдела

«27» август 2019 г.  И.Г. Дмитриева
(дата) (подпись) (Ф.И.О.)

СОГЛАСОВАНО

Декан факультета

«28» август 2019 г.  Е.В. Петрунина
(дата) (подпись) (Ф.И.О.)

СОГЛАСОВАНО

Заведующий
библиотекой

«26» август 2019 г.  В.А. Ахтырская
(дата) (подпись) (Ф.И.О.)

РАССМОТРЕНО
ОДОБРЕНО
УЧЕБНО-МЕТОДИЧЕСКИМ
СОВЕТОМ МГТЭУ
Пр. № 8 «30» август 2019 г.

1. ОРГАНИЗАЦИОННО-МЕТОДИЧЕСКИЙ РАЗДЕЛ

1.1. Цель изучения дисциплины: формирование теоретических знаний и практических навыков по обеспечению защиты информации.

Задачи:

- получить представление о роли защиты информации и информационной безопасности;
- знать современные методы и средства защиты информации;
- знать особенности защиты информации в персональных компьютерах.

1.2. Требования к результатам освоения дисциплины

Изучение данной дисциплины направлено на формирование следующих компетенций:

Код и содержание компетенции	Планируемые результаты обучения по дисциплине (модулю), характеризующие этапы формирования компетенций
ОПК-4 Способен комбинировать и адаптировать существующие информационно-коммуникационные технологии для решения задач в области профессиональной деятельности с учетом требований информационной безопасности	ОПК-4.1 Знает основные методы получения новых знаний с помощью информационных технологий для решения задач в области профессиональной деятельности с учетом требований информационной безопасности; стандарты оформления программной документации и причины нарушения компьютерной безопасности.
	ОПК-4.2 Умеет применять информационные технологии в практической деятельности и анализировать полученные решения вычислительных задач; на основе анализа применяемых математических методов и алгоритмов оценивать эффективность средств защиты информации; ориентироваться в современных и перспективных математических методах защиты информации.
	ОПК-4.3 Владеет информационными технологиями как средством получения новых знаний; методами информационной и кадровой безопасности в коммуникационной деятельности.

1.3. Место дисциплины (модуля) в структуре образовательной программы направления подготовки 01.04.02 «Прикладная математика и информатика»

Учебная дисциплина «Современные методы и средства защиты информации» относится к обязательной части блока Б1. «Дисциплины (модули)». Изучение учебной дисциплины «Современные методы и средства защиты информации» базируется на знаниях, умениях и навыках, полученных обучающимися при изучении дисциплин «Современные проблемы прикладной математики и информатики» и «Практикум по программированию».

Изучение учебной дисциплины «Современные методы и средства защиты информации» необходимо для изучения дисциплин «Нечеткое моделирование», «Интеллектуальные технологии обработки информации», «Компьютерные методы анализа больших объемов данных» и «Современные методы и средства разработки программного обеспечения».

2. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

2.1. Объем дисциплины и виды учебной работы в соответствии с формами обучения

Объем дисциплины «Современные методы и средства защиты информации» составляет 4 з.е./144 часа:

Вид учебной работы	Всего, часов	Очная форма
		Курс, часов
		1 курс, 2 сем.
Аудиторная работа обучающихся с преподавателем (по видам учебных занятий), всего в том числе:	46	46
Лекции	18	18
Практические занятия	28	28
Лабораторные занятия		
Самостоятельная работа обучающихся	62	62
Промежуточная аттестация (подготовка и сдача), всего:		
Контрольная работа		
Курсовая работа		
Зачет с оценкой		
Экзамен	36	36
Итого: Общая трудоемкость учебной дисциплины (в часах, зачетных единицах)	144/4	144/4

2.2. Содержание дисциплины по темам (разделам)

№ п/п	Наименование раздела (темы)	Содержание раздела (тематика занятий)	Формируемые компетенции (индекс)
1.	Раздел 1. Введение	Основные понятия курса. Организационно-правовые вопросы защиты информации	ОПК-4
2.	Раздел 2. Защита информации от ПЭМИН	Каналы утечки информации из компьютерных систем; пассивные и активные методы защиты	ОПК-4
3.	Раздел 3. Основы теории защиты информации в компьютерных системах	Критерии информационной безопасности. Основные понятия теории защиты информации; угрозы безопасности; математические модели политики безопасности; общие критерии безопасности информационных технологий	ОПК-4
4.	Раздел 4. Основы криптографии	Понятия и определения; классификация шифров; блочные и поточные шифры	ОПК-4
5.	Раздел 5. Применение симметричных криптосистем для защиты компьютерной информации	Поля Фейстеля; стандарт шифрования данных DES; отечественный стандарт шифрования данных	ОПК-4
6.	Раздел 6. Инфраструктура открытых ключей	Концепция криптосистемы с открытым ключом; однонаправленные функции; криптосистемы шифрования данных RSA и Эль Гамала	ОПК-4

7.	Раздел 7. Методы идентификации и аутентификации пользователей компьютерных систем	Аутентификация данных; алгоритмы безопасного хеширования; ЭЦП криптосистем RSA и Эль Гамала; алгоритм цифровой подписи DSA; отечественные алгоритмы цифровой надписи	ОПК-4
8.	Раздел 8. Защита компьютерных систем от удаленных атак через сеть Internet	Применение межсетевых экранов для организации виртуальных корпоративных сетей; системы организации защищенного документооборота; криптопротоколы.	ОПК-4
9.	Раздел 9. Методы защита программ от изучения и разрушающих программных воздействий (программных закладок и вирусов)	Методы внедрения программных закладок; компьютерные вирусы и антивирусные программы; классификация вирусов; защита от разрушающих программных воздействий	ОПК-4
10.	Раздел 10. Заключение	Проблемы компьютерной безопасности; перспективные направления исследований	ОПК-4

2.3. Разделы дисциплин и виды занятий

№ п/п	Наименование темы дисциплины	Лекционные занятия	Практические занятия	Самостоятельная работа	Всего часов	Формы текущего контроля успеваемости
1.	Введение	2		6	8	Устный опрос
2.	Защита информации от ПЭМИН	2	4	6	12	Устный опрос
3.	Основы теории защиты информации в компьютерных системах	2	2	8	12	Устный опрос
4.	Основы криптографии	2	2	8	12	Устный опрос
5.	Применение симметричных криптосистем для защиты компьютерной информации	2	4	6	12	Устный опрос
6.	Инфраструктура открытых ключей	2	4	6	12	Устный опрос
7.	Методы идентификации и аутентификации пользователей компьютерных систем	2	4	6	12	Устный опрос
8.	Защита компьютерных систем от удаленных атак через сеть Internet	2	4	8	14	Устный опрос
9.	Методы защита программ от изучения и разрушающих программных воздействий (программных закладок и вирусов)	2	4	8	14	Устный опрос
Экзамен		36				
Итого:		18	28	62	144	

2.4. Планы теоретических (лекционных) занятий

№	Наименование тем лекций	Кол-во часов во 2 семестре
РАЗДЕЛ 1. Введение		
1.	Основные понятия курса. Организационно-правовые вопросы защиты информации	2
РАЗДЕЛ 2. Защита информации от ПЭМИН		
1.	Каналы утечки информации из компьютерных систем	2
2.	Пассивные и активные методы защиты	
РАЗДЕЛ 3. Основы теории защиты информации в компьютерных системах		
1.	Критерии информационной безопасности. Основные понятия теории защиты информации; угрозы безопасности	2
2.	Математические модели политики безопасности; общие критерии безопасности информационных технологий	
РАЗДЕЛ 4. Основы криптографии		
1.	Классификация шифров; блочные и поточные шифры	2
РАЗДЕЛ 5. Применение симметричных криптосистем для защиты компьютерной информации		
1.	Поля Фейстеля; стандарт шифрования данных DES	2
2.	Отечественный стандарт шифрования данных	
РАЗДЕЛ 6. Инфраструктура открытых ключей		
1.	Концепция криптосистемы с открытым ключом; однонаправленные функции	2
2.	Криптосистемы шифрования данных RSA и Эль Гамала	
РАЗДЕЛ 7. Методы идентификации и аутентификации пользователей компьютерных систем		
1.	Аутентификация данных; алгоритмы безопасного хеширования	2
2.	ЭЦП криптосистем RSA и Эль Гамала. Алгоритм цифровой подписи DSA; отечественные алгоритмы цифровой надписи	
РАЗДЕЛ 8. Защита компьютерных систем от удаленных атак через сеть Internet		
1.	Применение межсетевых экранов для организации виртуальных корпоративных сетей	2
2.	Системы организации защищенного документооборота; криптопротоколы.	
РАЗДЕЛ 9. Методы защита программ от изучения и разрушающих программных воздействий (программных закладок и вирусов)		
1.	Методы внедрения программных закладок	2
2.	Компьютерные вирусы и антивирусные программы; классификация вирусов; защита от разрушающих программных воздействий	

2.5. Планы практических (семинарских) занятий

№	Наименование практических занятий	Кол-во часов во 2 семестре
РАЗДЕЛ 2. Защита информации от ПЭМИН		
1.	Пассивные и активные методы защиты	4
РАЗДЕЛ 3. Основы теории защиты информации в компьютерных системах		
1.	Математические модели политики безопасности; общие критерии безопасности информационных технологий	2
РАЗДЕЛ 4. Основы криптографии		
1.	Блочные и поточные шифры	2
РАЗДЕЛ 5. Применение симметричных криптосистем для защиты компьютерной информации		
1.	Стандарт шифрования данных DES; отечественный стандарт шифрования	4

	данных	
РАЗДЕЛ 6. Инфраструктура открытых ключей		
1.	Однонаправленные функции	2
2.	Криптосистемы шифрования данных RSA и Эль Гамала	2
РАЗДЕЛ 7. Методы идентификации и аутентификации пользователей компьютерных систем		
1.	Алгоритмы безопасного хеширования; ЭЦП криптосистем RSA и Эль Гамала	2
2.	Алгоритм цифровой подписи DSA; отечественные алгоритмы цифровой подписи	2
РАЗДЕЛ 8. Защита компьютерных систем от удаленных атак через сеть Internet		
1.	Системы организации защищенного документооборота	2
2.	Криптопротоколы	2
РАЗДЕЛ 9. Методы защита программ от изучения и разрушающих программных воздействий (программных закладок и вирусов)		
1.	Компьютерные вирусы и антивирусные программы	4
Экзамен		36

2.6. Планы лабораторных работ – не предусмотрено.

2.7. Планы самостоятельной работы обучающегося по дисциплине (модулю).

№	Название разделов и тем	Виды самостоятельной работы	Трудоемкость	Формируемые компетенции	Формы контроля
1.	Введение	Работа с источниками	6	ОПК-4	Устный опрос
2.	Защита информации от ПЭМИН	Составление отчетов	6	ОПК-4	Устный опрос
3.	Основы теории защиты информации в компьютерных системах	Составление отчетов	8	ОПК-4	Устный опрос
4.	Основы криптографии	Составление отчетов	8	ОПК-4	Устный опрос
5.	Применение симметричных криптосистем для защиты компьютерной информации	Составление отчетов	6	ОПК-4	Устный опрос
6.	Инфраструктура открытых ключей	Составление отчетов	6	ОПК-4	Устный опрос
7.	Методы идентификации и аутентификации пользователей компьютерных систем	Составление отчетов	6	ОПК-4	Устный опрос
8.	Защита компьютерных систем от удаленных атак через сеть Internet	Составление отчетов	8	ОПК-4	Устный опрос
9.	Методы защита программ от изучения и разрушающих программных воздействий (программных закладок и вирусов)	Составление отчетов	8	ОПК-4	Устный опрос

3. ОСОБЕННОСТИ ОБУЧЕНИЯ ЛИЦ С ИНВАЛИДНОСТЬЮ И ОВЗ

При организации обучения студентов с инвалидностью и ОВЗ обеспечиваются следующие необходимые условия:

- учебные занятия организуются исходя из психофизического развития и состояния здоровья лиц с ОВЗ совместно с другими обучающимися в общих группах, а также индивидуально, в соответствии с графиком индивидуальных занятий;

- при организации учебных занятий в общих группах используются социально-активные и рефлексивные методы обучения, технологии социокультурной реабилитации с целью оказания помощи в установлении полноценных межличностных отношений, создания комфортного психологического климата в группе;

- в процессе образовательной деятельности применяются материально-техническое оснащение, специализированные технические средства приема-передачи учебной информации в доступных формах для студентов с различными нарушениями, электронные образовательные ресурсы в адаптированных формах.

- подбор и разработка учебных материалов преподавателями производится с учетом психофизического развития и состояния здоровья лиц с ОВЗ;

- использование элементов дистанционного обучения при работе со студентами, имеющими затруднения с моторикой;

- обеспечение студентов текстами конспектов (при затруднении с конспектированием);

- использование при проверке усвоения материала методик, не требующих выполнения рукописных работ или изложения вслух (при затруднениях с письмом и речью) – например, тестовых бланков.

При проведении процедуры оценивания результатов обучения инвалидов и лиц с ограниченными возможностями здоровья по дисциплине обеспечивается выполнение следующих дополнительных требований в зависимости от индивидуальных особенностей обучающихся:

1. Инструкция по порядку проведения процедуры оценивания предоставляется в доступной форме (устно, в письменной форме, на электронном носителе, в печатной форме увеличенным шрифтом и т.п.);

2. Доступная форма предоставления заданий оценочных средств (в печатной форме, в печатной форме увеличенным шрифтом, в форме электронного документа);

3. Доступная форма предоставления ответов на задания (письменно на бумаге, набор ответов на компьютере, устно, др.).

При необходимости для обучающихся с ограниченными возможностями здоровья и инвалидов процедура оценивания результатов обучения по дисциплине может проводиться в несколько этапов.

В освоении дисциплины инвалидами и лицами с ограниченными возможностями здоровья большое значение имеет индивидуальная работа. Под индивидуальной работой подразумевается две формы взаимодействия с преподавателем: индивидуальная учебная работа (консультации), т.е. дополнительное разъяснение учебного материала и углубленное изучение материала с теми обучающимися, которые в этом заинтересованы, и индивидуальная воспитательная работа. Индивидуальные консультации по предмету являются важным фактором, способствующим индивидуализации обучения и установлению воспитательного контакта между преподавателем и обучающимся инвалидом или обучающимся с ограниченными возможностями здоровья.

4. УЧЕБНО-МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ САМОСТОЯТЕЛЬНОЙ РАБОТЫ ОБУЧАЮЩИХСЯ

Учебно-методическое обеспечение дисциплины для организации самостоятельной работы студентов (содержит перечень основной литературы, дополнительной литературы, программного обеспечения и Интернет-ресурсы).

В распоряжении преподавателей и обучающихся имеется основное необходимое материально-техническое оборудование, Интернет-ресурсы, доступ к полнотекстовым

электронным базам, книжный фонд библиотеки Московского государственного гуманитарно-экономического университета.

5. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЯ УЧЕБНОЙ ДИСЦИПЛИНЫ (МОДУЛЯ)

5.1 Перечень основной литературы

1. Информационная безопасность. История специальных методов криптографической деятельности: Учебное пособие / Баранова Е.К., Бабаш А.В., Ларин Д.А. - Москва :ИЦ РИОР, НИЦ ИНФРА-М, 2019. - 236 с.: - Текст : электронный. - URL: <https://new.znanium.com/catalog/product/987215>

2. Информационная безопасность: Учебное пособие / Ковалев Д.В., Богданова Е.А. - Ростов-на-Дону:Южный федеральный университет, 2016. - 74 с.: ISBN 978-5-9275-2364-1 - Текст : электронный. - URL: <https://new.znanium.com/catalog/product/997105>

3. Менеджмент риска информационной безопасности: Учебное пособие / Веселов Г.Е., Абрамов Е.С., Шилов А.К. - Таганрог:Южный федеральный университет, 2016. - 107 с.: ISBN 978-5-9275-2327-5 - Текст : электронный. - URL: <https://new.znanium.com/catalog/product/997108>

4. Разработка высоконадежных интегрированных информационных систем управления предприятием/КапулинД.В., ЦаревР.Ю., ДроздО.В. и др. - Краснояр.: СФУ, 2015. - 184 с.: ISBN 978-5-7638-3227-3 - Текст : электронный. - URL: <https://new.znanium.com/catalog/product/549904>

5.2 Перечень дополнительной литературы

1. Внуков, А. А. Защита информации : учебное пособие для бакалавриата и магистратуры / А. А. Внуков. — 2-е изд., испр. и доп. — Москва : Издательство Юрайт, 2019. — 240 с. — (Высшее образование). — ISBN 978-5-534-01678-9. — Текст : электронный // ЭБС Юрайт [сайт]. — URL: <https://biblio-online.ru/bcode/444046>

2. Бабенко, Л. К. Криптографическая защита информации: симметричное шифрование : учебное пособие для вузов / Л. К. Бабенко, Е. А. Ищукова. — Москва : Издательство Юрайт, 2019. — 220 с. — (Университеты России). — ISBN 978-5-9916-9244-1. — Текст : электронный // ЭБС Юрайт [сайт]. — URL: <https://biblio-online.ru/bcode/437667>

3. Щеглов, А. Ю. Защита информации: основы теории : учебник для бакалавриата и магистратуры / А. Ю. Щеглов, К. А. Щеглов. — Москва : Издательство Юрайт, 2019. — 309 с. — (Бакалавр и магистр. Академический курс). — ISBN 978-5-534-04732-5. — Текст : электронный // ЭБС Юрайт [сайт]. — URL: <https://biblio-online.ru/bcode/433715>

4. Казарин, О. В. Программно-аппаратные средства защиты информации. Защита программного обеспечения : учебник и практикум для вузов / О. В. Казарин, А. С. Забабурин. — Москва : Издательство Юрайт, 2019. — 312 с. — (Специалист). — ISBN 978-5-9916-9043-0. — Текст : электронный // ЭБС Юрайт [сайт]. — URL: <https://biblio-online.ru/bcode/437163>

5.3 Программное обеспечение

1. Сетевой компьютерный класс, оснащенный современной техникой
2. Офисный программный пакет (например, Microsoft Office 2003 или более поздних версий).
3. Web-браузер Mozilla Firefox или Google Chrome
4. Экран для проектора

5.4 Электронные ресурсы

1. Национальный открытый университет ИНТУИТ [Электронный ресурс]. URL: <http://www.intuit.ru>
2. Хабрахабр [Электронный ресурс]. URL: <http://habrahabr.ru/>.
3. <http://www.lessons-tva.info/> - На сайте представлены различные учебные материалы, в том числе онлайн учебники (авторские курсы) по дисциплинам: экономическая информатика, компьютерные сети и телекоммуникации, основы электронного бизнеса, информатика и компьютерная техника.
4. Электронно-библиотечная система Юрайт - <https://biblio-online.ru/>
5. Электронно-библиотечная система Znanium - <https://new.znanium.com/>

6. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ УЧЕБНОЙ ДИСЦИПЛИНЫ (МОДУЛЯ)

№ п/п	Наименование оборудованных учебных кабинетов, лабораторий	Перечень оборудования и технических средств обучения
1.	Аудитория №109	Учебная аудитория 1-109 Кол-во посадочных мест – 24 Оснащена учебной мебелью Рабочее место преподавателя Мультимедийный проектор Epson EH-TW535W Интерактивная доска Smart Board 11 компьютеров Системный блок: Процессор Intel(R) Core(TM) i5-6400 CPU @ 2.70GHz 4096 МБ ОЗУ SSD Объем: 120 ГБ

		<p>Монитор Philips PHL 243V5 - 24 дюйма Акустическая система Sven</p> <p>Лицензионное программное обеспечение: Microsoft Office 2007 (гос. Контракт № 14/09 от 14.04.2009); Microsoft Windows 7 Professional (Сублицензионный договор № Tr000419452); Консультант Плюс (Договор № 40814-64034/01.2020 от 22.01.2020); Kaspersky Endpoint Security 10 (Сублицензионный договор № 11-05/19); Visual Studio 2017 (Сублицензионный договор № Tr000419452); Свободно распространяемое программное обеспечение: 1С Предприятие 8 (учебная версия); AnyLogic 7; Bloodshell Dev C++; Cisco Packet Tracer; Oracle VM VirtualBox; PSPP; Python 3.7; scilab 5.5.2; Scribus 1.4.7; Turbo Pascal 7; Vmware Workstation.</p>
2.	Аудитория №308	<p>Учебная аудитория 1-308 Кол-во посадочных мест – 24 Оснащена учебной мебелью Рабочее место преподавателя Экран Интерактивная доска Elite Panaboard UB-T880W с акустической системой Проектор Epson EB-440W</p> <p>11 компьютеров Системный блок: Процессор Intel(R) Core(TM) i5-2400 CPU @ 3.10GHz 8192 ОЗУ HDD Объем: 500 ГБ Монитор DELL EX231W - 24 дюйма Лицензионное программное обеспечение: Консультант Плюс (Договор № 40814-64034/01.2020 от 22.01.2020); Visual Studio 2017 (Сублицензионный договор № Tr000419452); Microsoft Office 2007 (гос. Контракт № 14/09 от 14.04.2009); Microsoft Windows 7 Professional (Сублицензионный договор № Tr000419452); Kaspersky Endpoint Security 10 (Сублицензионный договор № 11-05/19); Свободно распространяемое программное обеспечение: Oracle VM VirtualBox; scilab 5.5.2.</p>
3.	Аудитория №306	<p>Учебная аудитория 1-306 Кол-во посадочных мест – 19 Оснащена учебной мебелью Рабочее место преподавателя Интерактивная доска Elite Panaboard UB-T880W с акустической системой Проектор Epson EB-440W</p> <p>12 компьютеров Системный блок: Процессор Intel(R) Core(TM) i5-2400 CPU @ 3.10GHz 8192 ОЗУ</p>

		<p>HDD Объем: 500 ГБ Монитор DELL EX231W – 24 дюйма</p> <p>Лицензионное программное обеспечение: Adobe Design Standart CS5.5 (Договор-оферта № Tr017922 от 06.04.2011); CorelDRAW Graphics Suite X5 Classroom License ML 15+1 (Договор-оферта № Tr017922 от 06.04.2011); Консультант Плюс (Договор № 40814-64034/01.2020 от 22.01.2020); Visual Studio 2017 (Сублицензионный договор № Tr000419452); Microsoft Office Plus 2007 (гос. Контракт № 14/09 от 14.04.2009); Microsoft Windows 7 Professional (Сублицензионный договор № Tr000419452); Kaspersky Endpoint Security 10 (Сублицензионный договор № 11-05/19); Свободно распространяемое программное обеспечение: 1С Предприятие 8 (учебная версия); Oracle VM VirtualBox; Python 3.7; Cisco Packet Tracer.</p>
4.	Аудитория №402	<p>Учебная аудитория 1-402 Кол-во посадочных мест – 34 Оснащена учебной мебелью Рабочее место преподавателя Интерактивная доска Smart Board Проектор Epson EH-TW535W</p> <p>11 компьютеров Системный блок 1: Процессор Intel(R) Core(TM) i5-4570 CPU @ 3.20GHz 8192 ОЗУ HDD Объем: 500 ГБ Монитор Viewsonic 23.6</p> <p>Системный блок 2: Процессор Intel(R) Core(TM) i5-8400 CPU @ 2.80GHz 8192 ОЗУ SSD Объем: 240 ГБ Акустическая система 2.0 Лицензионное программное обеспечение: Visual Studio 2017 (Сублицензионный договор № Tr000419452); Microsoft Office 2010 (Сублицензионный договор № Tr000419452); Microsoft Windows 10 Для образовательных учреждений (Сублицензионный договор № Tr000419452); Консультант Плюс (Договор № 40814-64034/01.2020 от 22.01.2020); Kaspersky Endpoint Security 10 (Сублицензионный договор № 11-05/19); Свободно распространяемое программное обеспечение: 1С Предприятие 8.2 (учебная версия); Bloodshell Dev C++; NetBeans; Notepad++; Python 3.7; scilab 6.0.2; Scribus 1.4.7.</p>

7. ОЦЕНКА КОМПЕТЕНЦИЙ ПО ИЗУЧАЕМОЙ ДИСЦИПЛИНЕ

№	Критерии оценки			
	«неудовлетворительно»	«удовлетворительно»	«хорошо»	«отлично»
ЗНАТЬ				
1	Студент не знает правовые основы защиты компьютерной информации, организационные, технические и программные методы защиты информации, стандарты, модели и методы шифрования, методы идентификации пользователей, методы защиты программ от вирусов	Студент усвоил основное содержание материала дисциплины, но имеет пробелы в усвоении материала. Имеет несистематизированные знания об основах защиты компьютерной информации, организационных, технических и программных методах защиты информации	Студент способен самостоятельно выделять знания об основах защиты компьютерной информации, организационных, технических и программных методах защиты информации, стандартах, моделях и методах шифрования	Студент знает правовые основы защиты компьютерной информации, организационные, технические и программные методы защиты информации, стандарты, модели и методы шифрования, методы идентификации пользователей, методы защиты программ от вирусов
УМЕТЬ				
2	Студент не умеет применять методы защиты компьютерной информации в различных предметных областях; иметь представление о направлениях развития и перспективах защиты информации	Студент испытывает затруднения при использовании методов защиты компьютерной информации в различных предметных областях; имеет слабые представления о направлениях развития и перспективах защиты информации	Студент умеет пользоваться базовыми методами защиты компьютерной информации в различных предметных областях; имеет слабые представления о направлениях развития и перспективах защиты информации	Студент умеет применять методы защиты компьютерной информации в различных предметных областях; иметь представление о направлениях развития и перспективах защиты информации
ВЛАДЕТЬ				
3	Студент не владеет стандартной терминологией и положениями теории защиты информации и информационной безопасности; навыками по экспериментальным исследованиям с использованием стандартных программных	Студент владеет основными понятиями стандартной терминологии и положений теории защиты информации и информационной безопасности	Студент владеет стандартной терминологией и положениями теории защиты информации и информационной безопасности и базовыми навыками по экспериментальным исследованиям с использованием стандартных	Студент владеет стандартной терминологией и положениями теории защиты информации и информационной безопасности; навыками по экспериментальным исследованиям с использованием стандартных

	средств		программных средств	программных средств
	Компетенции или их части не сформированы.	Компетенции или их части сформированы на базовом уровне.	Компетенции или их части сформированы на среднем уровне.	Компетенции или их части сформированы на высоком уровне.

8. ОБРАЗОВАТЕЛЬНЫЕ ТЕХНОЛОГИИ

Интерактивные образовательные технологии, используемые в аудиторных занятиях и самостоятельной работе обучающихся – не предусмотрены.

9. ОЦЕНОЧНЫЕ СРЕДСТВА ДЛЯ ТЕКУЩЕГО КОНТРОЛЯ УСПЕВАЕМОСТИ И ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ

9.1. Организация входного, текущего и промежуточного контроля обучения

Входное тестирование – не предусмотрено.

Текущий контроль – устный опрос.

Промежуточная аттестация – экзамен.

9.2. Тематика рефератов, проектов, творческих заданий, эссе и т.п.

Не предусмотрены.

9.3. Курсовая работа

Не предусмотрено.

9.4. Вопросы к зачету

Не предусмотрены.

9.5. Вопросы к экзамену

1. Современные аспекты безопасности информационных систем.

2. Понятие «информационная безопасность» и «защита информации».

3. Назначение организационных средств защиты

4. Состав комплекса защиты территории охраняемых объектов

5. Понятие информационного права.

6. Степени секретности и виды конфиденциальности информации.

7. Понятие информации, изъятой из оборота, и ограниченной в обороте.

8. Нормативные документы по лицензированию деятельности

9. Нормативные документы по сертификации средств защиты

10. Понятие ПЭМИН

12. Методы защиты компьютеров от утечки ПЭМИН.

13. Назначение генератора шума.

14. Классификация угроз безопасности.

15. Назначение средств защиты от НДС.

16. Основные свойства защищаемой информации.

17. Понятие политики безопасности

18. Состав системы разграничения доступа

19. Матричная модель системы ЗИ.

20. Многоуровневая модель системы ЗИ.

21. Система регистрации

22. Критерии оценки безопасности компьютерных систем министерства обороны

США («Оранжевая книга»)

23. Руководящий документ (РД) Гостехкомиссии России «Классификация автоматизированных систем и требования по ЗИ»

24. Сравнительный анализ «Оранжевой книги» и РД

25. Криптографическая защита информации в каналах связи и компьютерах.

26. Основные термины и понятия криптографии.

27. Классификация криптосистем.

28. Симметричные криптосистемы. Классификация шифров

29. Блочные и поточные шифры

30. Требования к криптосистемам.

31. Гаммирование.
32. Аппаратные и программные генераторы псевдослучайных чисел (ПСЧ)
33. Составные шифры
34. Криптосистема «ЛЮЦИФЕР».
35. Поля Фейстеля
36. Алгоритм криптосистемы DES.
37. Режимы шифрования криптосистемы DES.
38. Отечественный алгоритм шифрования ГОСТ 28147-89
39. Режимы шифрования криптосистемы ГОСТ 28147-89
40. Сравнительный анализ криптосистем DES и ГОСТ 28147-89.
41. Концепция криптосистемы с открытым ключом.
42. Однонаправленные функции.
43. Классификация алгоритмов двухключевых систем.
44. Алгоритмы рюкзака.
45. Алгоритм RSA.
46. Схема шифрования Эль-Гамала.
47. ЭЦП Эль-Гамала.
48. Генерация и рассылка ключей.
49. Хранение и уничтожение ключей.
50. Понятия идентификации, аутентификации и авторизации.
51. Парольная аутентификация.
52. Взаимная проверка пользователей.
53. Система Kerberos.
54. Аутентификация удаленных пользователей.
55. Назначение однонаправленных хэш-функций.
56. Алгоритм безопасного хеширования SHA.
57. Отечественный стандарт хэш-функции.
58. Алгоритм цифровой подписи RSA.
59. Алгоритм цифровой подписи Эль Гамала (EGSA).
60. Алгоритм цифровой подписи DSA.
61. Отечественные алгоритмы ЭЦП.
62. Понятие атаки на компьютерную систему.
63. Типичные угрозы в среде Internet.
64. Программно-аппаратные методы защиты от удаленных атак в сети Internet.
65. Методика Firewall, реализуемая на базе программно-аппаратных средств.
66. Назначение Проху-сервера.
67. Сетевой монитор безопасности.
68. Назначение COB.
69. Туннелирование на канальном уровне. Протоколы PPTP и L2TP.
70. Туннелирование на сетевом уровне. Архитектура IPSec.
71. Защита соединения на сеансовом уровне. Протоколы SSL и TLS.
72. Классификация способов защиты от от изучения и разрушающих программных воздействий.
73. Методы перехвата и навязывания информации.
74. Методы внедрения программных закладок.
75. История возникновения компьютерных вирусов.
76. Классификация вирусов.
77. Детекторы, фаги, прививки.
78. Вакцины, ревизоры и мониторы.
79. Проблемы компьютерной безопасности.
80. Перспективные направления исследований в компьютерной безопасности.

9.6. Контроль освоения компетенций

Вид контроля	Контролируемые темы (разделы)	Компетенции, компоненты которых контролируются
<i>Устный опрос</i>	<i>1,2,3,4,5,6,7,8,9</i>	<i>ОПК-4</i>

