Федеральное государственное бюджетное образовательное учреждение инклюзивного высшего образования

«МОСКОВСКИЙ ГОСУДАРСТВЕННЫЙ ГУМАНИТАРНО-ЭКОНОМИЧЕСКИЙ УНИВЕРСИТЕТ»

Факультет Прикладная математика и информатика

Кафедра Информационных технологий и прикладной математики

УТВЕРЖДАЮ
И.о. проректора по ООД
_____ Пузанкова Е.Н.
«30» августа 2019 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ
ТЕОРЕТИЧЕСКИЕ ОСНОВЫ КОМПЬЮТЕРНОЙ БЕЗОПАСНОСТИ

образовательная программа направления подготовки
09.04.03 "Прикладная информатика"
Блок Б1.В.02 «Дисциплины (модули)», часть формируемая участниками образовательных отношений

Профиль подготовки
Интеллектуальные биоинформационные технологии

Квалификация (степень) выпускника

Магистр

Форма обучения: очная

Курс 1 семестр 1

Москва
2019

Рабочая программа составлена на основании федерального государственного образовательного стандарта высшего образования по направлению подготовки 09.04.03 «Прикладная информатика (уровень магистратуры)», утвержденного приказом Министерства образования и науки Российской Федерации № 916 от 19 сентября 2017 г. Зарегистрировано в Минюсте России 10 октября 2017 г. №48495.

Составители рабочей программы: МГГЭУ, доцент кафедры ИТиПМ
место работы, занимаемая должность

_____ Белоглазов А.А. «20» августа 2019 г.
подпись Ф.И.О. Дата

Рецензент: МГГЭУ, профессор кафедры ИТиПМ
место работы, занимаемая должность

_____ Истомина Т.В. «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» августа 2019 г. _____ И.Г. Дмитриева
(дата) (подпись) (Ф.И.О.)

СОГЛАСОВАНО
Декан факультета
«26» августа 2019 г. _____ Е.В. Петрунина
(дата) (подпись) (Ф.И.О.)

СОГЛАСОВАНО
Заведующий
библиотекой

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

РАССМОТРЕНО И ОДОБРЕНО УЧЕБНО-МЕТОДИЧЕСКИМ СОВЕТОМ МГГЭУ
ПР.№ 8 «3» 09 2019 г.

1. ОРГАНИЗАЦИОННО-МЕТОДИЧЕСКИЙ РАЗДЕЛ

1.1. Цели и задачи изучения дисциплины

Цели освоения дисциплины:

- освоение общих принципов, методов и механизмов обеспечения компьютерной безопасности;
- изучение политики и моделей безопасности информации в компьютерных системах.

Задачи освоения дисциплины:

- обобщение базовых знаний по субъектно-объектной модели компьютерной системы в механизмах и процессах коллективного доступа к информационным ресурсам;
- изучение понятия информационной безопасности, её цели, механизмы, инструментарий и основные направления;
- изучение моделей дискреционного доступа, мандатного доступа, моделей разграничения доступа на основе функционально-ролевых отношений;
- изучение источников угроз информационной безопасности, изложение основных принципов защиты компьютерной информации и их оценки.

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**
ПК-6 Способен применять современные методы и инструментальные средства прикладной информатики для автоматизации и информатизации решения прикладных задач различных классов и создания ИС	ПК-6.1 Знает различные методы решения задач при создании экономических информационных систем; методы проектирования автоматизированных и информационных систем для решения прикладных задач; информационные технологии, применяемые на этапах разработки, производства, испытаний и эксплуатации продукции.
	ПК-6.2 Умеет осуществлять выбор способа представления информации в соответствии с поставленной задачей; видеть и формулировать проблему информационной безопасности и надежности, ее анализировать, подбирать средства и методы для ее решения и ликвидации; использовать программные средства, применяемые на этапах разработки, производства, испытаний и эксплуатации продукции.
	ПК-6.3 Владеет навыками применения типовых подходов, применяемых при анализе, планировании и оперативном управлении деятельностью промышленного предприятия; навыками исследования применения различных научных подходов к автоматизации информационных процессов и информатизации предприятий и организаций на основе приобретенных знаний и умений и их применения в нетипичных ситуациях.

1.3. Место дисциплины (модуля) в структуре образовательной программы направления подготовки 09.04.03 Прикладная информатика (уровень магистратуры).

Учебная дисциплина «Теоретические основы компьютерной безопасности» относится к части, формируемой участниками образовательных отношений блока «Дисциплин (модулей)» блока Б1. Изучение этой учебной дисциплины базируется на знаниях, умениях и навыках, полученных обучающимися при изучении предшествующих курсов: «Математические инструментальные методы и модели систем поддержки принятия решений», «Современные технологии разработки программного обеспечения», «Стандартизация и лицензирование в сфере биоинформационных технологий». Изучение учебной дисциплины необходимо для освоения такой дисциплины как «Современные методы разработки биомедицинских систем», прохождения производственной и преддипломной практик.

2. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

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

Объем дисциплины «Теоретические основы компьютерной безопасности» составляет 4 з.е./144 часа:

Вид учебной работы	Всего, часов	Очная форма
		Курс, часов
		1 курс, 1 сем.
Аудиторная работа обучающихся с преподавателем (по видам учебных занятий), всего в том числе:	**40**	**40**
Лекции	12	12
Практические занятия	28	28
Лабораторные занятия		
Самостоятельная работа обучающихся	**68**	**68**
Промежуточная аттестация (подготовка и сдача), всего:		
Контрольная работа		
Курсовая работа		
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. Основные понятия теории компьютерной безопасности.	Основные понятия теории компьютерной безопасности. Язык. Объекты. Субъекты. Доступ. Ценность информации. Аддитивная модель. Порядковая шкала. Решетка ценности. Анализ угроз информацион-ной безопасности. Угрозы конфиденциальности, целостности, доступности информации, раскрытия параметров информационной системы. Структура теории компьютерной	ПК-6

		безопасности. Основные уровни защиты информации. Защита машинных носителей информации и средств взаимодействия. Защита представления информации. Защита содержания информации. Основные виды атак на автоматизированные системы обработки информации. Классификация основных атак и вредоносных программ.	
2.	Раздел 2. Политики безопасности	Понятие политики безопасности. Политика (стратегия) безопасности. Дискреционная политика разграничения доступа. Мандатная (полномочная) политика разграничения доступа. Политика безопасности информационных потоков. Политика ролевого разграничения доступа. Политика изолированной программной среды. Разработка и реализация политики безопасности. Модели безопасности. Описание систем защиты с помощью матрицы доступа.	ПК-6
3.	Раздел 3. Дискреционная политика разграничения доступа	Модель Харрисона-Руззо-Ульмана. Модель распространения прав доступа Take-Grant. Разрешимость проблемы безопасности. Расширенная модель Take-Grant. Анализ информационных каналов.	ПК-6
4.	Раздел 4. Мандатная политика разграничения доступа	Классическая модель Белла-ЛаПадулы. Свойства безопасности системы в классической модели Белла-ЛаПадула. Базовая теорема безопасности в классической модели Белла-ЛаПадула. Эквивалентные подходы к определению безопасности модели Белла-Лападулы. Политика low-watermark в модели Белла-ЛаПадула. Условия и результаты выполнения операций при реализации политики low-watermark в модели Белла-ЛаПадула. Безопасность переходов в классической модели Белла-ЛаПадула. Функция переходов и ее безопасность в смысле администрирования в классической модели Белла-ЛаПадула. Модель мандатной политики целостности информации Биба.	ПК-6
5.	Раздел 5. Активный аудит моделей безопасности	Активный аудит. Общая архитектура системы и методы анализа. Сигнатурный анализ. Теорема Клини. Статистический анализ. Алгоритм NIDES. Состоятельность оценки числа ребер случайного графа.	ПК-6

		Модели безопасности в базах данных. Понятие реляционной базы данных и реляционных операторов. Декомпозиция и восстановление многоуровневой базы данных. Теорема Эрдёша-Реньи.	
6.	Раздел 6. Модель систем военных сообщений	Общие положения и основные понятия модели систем военных сообщений. Модель CBC (MMS). Неформальное описание модели систем военных сообщений. Формальное описание модели систем военных сообщений. Безопасное состояние в модели систем военных сообщений. Безопасность переходов в модели систем военных сообщений. Определения смыслов безопасности функции переходов в модели систем военных сообщений. Базовая теорема безопасности (BST) в модели систем военных сообщений. Теорема о безопасности системы в модели систем военных сообщений.	ПК-6

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.	Раздел 1. Основные понятия теории компьютерной безопасности.	2	4	8	14	Устный опрос
2.	Раздел 2. Политики безопасности	2	4	12	18	Устный опрос
3.	Раздел 3. Дискреционная политика разграничения доступа	2	4	12	18	Устный опрос
4.	Раздел 4. Мандатная политика разграничения доступа	2	4	12	18	Устный опрос
5.	Раздел 5. Активный аудит моделей безопасности	2	6	12	20	Устный опрос
6.	Раздел 6. Модель систем военных сообщений	2	6	12	20	Устный опрос
Экзамен					36	
	Итого:	12	28	68	144	

2.4. Планы теоретических (лекционных) занятий

№	Наименование тем лекций	Кол-во часов в 1 семестре
1 семестр		
Раздел 1. Основные понятия теории компьютерной безопасности.		
1.	Структура теории компьютерной безопасности. Основные уровни защиты информации.	2
Раздел 2. Политики безопасности		
1.	Политики (стратегии) безопасности.	2
Раздел 3. Дискреционная политика разграничения доступа		
1.	Модели систем разграничения, распространения доступа	2
Раздел 4. Мандатная политика разграничения доступа		
1.	Классическая модель системы безопасности	2
Раздел 5. Активный аудит моделей безопасности		
1.	Общая архитектура и методы анализа систем безопасности анализа	2
Раздел 6. Модель систем военных сообщений		
1.	Неформальное и формальное описание модели систем военных сообщений	2

2.5. Планы практических (семинарских) занятий

№	Наименование практических занятий	Кол-во часов в 1 семестре
1 семестр		
Раздел 1. Основные понятия теории компьютерной безопасности.		
1.	Язык. Объекты. Субъекты. Доступ. Ценность информации.	2
2.	Аддитивная модель. Порядковая шкала. Решетка ценности.	2
Раздел 2. Политики безопасности		
1.	Политика ролевого разграничения доступа	2
2.	Политика изолированной программной среды.	2
Раздел 3. Дискреционная политика разграничения доступа		
1.	Модель Харрисона-Руззо-Ульмана.	2
2.	Модель распространения прав доступа Take-Grant.	2
Раздел 4. Мандатная политика разграничения доступа		
1.	Модель Белла-ЛаПадулы.	2
2.	Функция переходов и ее безопасность в смысле администрирования в классической модели Белла-ЛаПадула.	2
Раздел 5. Активный аудит моделей безопасности		
1.	Сигнатурный анализ. Теорема Клини	2
2.	Статистический анализ. Алгоритм NIDES	2
3.	Декомпозиция и восстановление многоуровневой базы данных	2
Раздел 6. Модель систем военных сообщений		
1.	Неформальное описание модели систем военных сообщений.	2
2.	Формальное описание модели систем военных сообщений.	2
3.	Безопасность переходов в модели систем военных сообщений.	2

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.	Раздел 1. Основные понятия теории компьютерной безопасности.	Самоподготовка по теме: Анализ угроз информационной безопасности. Угрозы конфиденциальности, целостности, доступности информации, раскрытия параметров информационной системы. Структура теории компьютерной безопасности. Основные уровни защиты информации. Защита машинных носителей информации и средств взаимодействия. Защита представления информации.	8	ПК-6	Устный опрос
2.	Раздел 2. Политики безопасности	Самоподготовка по теме: Дискреционная политика разграничения доступа. Мандатная (пол-номочная) политика разграничения доступа.	12	ПК-6	Устный опрос
3.	Раздел 3. Дискреционная политика разграничения доступа	Самоподготовка по теме: Модель Харрисона-Руззо-Ульмана. Модель распространения прав доступа Take-Grant. Разрешимость проблемы безопасности. Расши-ренная модель Take-Grant. Анализ информационных каналов.	12	ПК-6	Устный опрос
4.	Раздел 4. Мандатная политика разграничения доступа	Самоподготовка по теме: По-литика low-watermark в модели Белла-ЛаПадула. Условия и резуль-таты выполнения операций при реализации политики low-watermark в модели Белла-ЛаПадула. Безопасность переходов в классической модели Белла-ЛаПадула. Функция переходов и ее безопасность в смысле администрирования в классической модели Белла-ЛаПадула. Модель мандатной политики целостности информации Биба.	12	ПК-6	Устный опрос
5.	Раздел 5. Активный аудит моделей безопасности	Самоподготовка по теме:	12	ПК-6	Устный опрос
6.	Раздел 6.	Самоподготовка по теме:	12	ПК-6	Устный

	Модель систем военных сообщений	Определения смыслов безопасности функции переходов в модели систем во-енных сообщений. Базовая теорема безопасности в модели систем военных сообщений. Теорема о безопасности системы в модели систем военных сообщений.			опрос

3. ОСОБЕННОСТИ ОБУЧЕНИЯ ЛИЦ С ОВЗ (ПОДА)

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

5.2. Перечень дополнительной литературы

1. 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
2. Внуков, А. А. Защита информации : учебное пособие для вузов / А. А. Внуков. — 3-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2020. — 161 с. — (Высшее образование). — ISBN 978-5-534-07248-8. — Текст : электронный // ЭБС Юрайт [сайт]. — URL: https://biblio-online.ru/bcode/422772
3. 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
4. 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
5. 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)
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 (дата обращения: 01.07.2019).
2. Хабрахабр [Электронный ресурс]. URL: http://habrahabr.ru/.
3. http://www.lessons-tva.info/ - На сайте представлены различные учебные материалы.
4. Электронная библиотека: https://biblio-online.ru/.
5. Электронная библиотека: 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 Монитор Philips PHL 243V5 - 24 дюйма Акустическая система Sven 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.
2.	Аудитория №308	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 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.
3.	Аудитория №306	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 12 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: 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.
4.	Аудитория №402	Учебная аудитория 1-402 Кол-во посадочных мест – 34 Оснащена учебной мебелью Рабочее место преподавателя Интерактивная доска Smart Board Проектор Epson EH-TW535W 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 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.

7. ОЦЕНКА КОМПЕТЕНЦИЙ ПО ИЗУЧАЕМОЙ ДИСЦИПЛИНЕ

№	Критерии оценки			
	«неудовлетворительно»	**«удовлетворительно»**	**«хорошо»**	**«отлично»**
	ЗНАТЬ			
1	Студент не способен самостоятельно выделять различные методы проектирования автоматизированных и информационных систем для решения прикладных задач.	Студент усвоил основное содержание материала дисциплины, но имеет пробелы в усвоении материала. Студент показывает базовые знания и понимает различные методы проектирования автоматизированных и информационных систем для решения прикладных задач.	Студент способен самостоятельно выделять главные положения в изученном материале. Знает хорошо и понимает различные методы проектирования автоматизированных и информационных систем для решения прикладных задач.	Студент знает, понимает, выделяет главные положения в изученном материале и способен дать краткую характеристику основным идеям проработанного материала дисциплины. Показывает глубокое знание и понимание различных методов проектирования автоматизированных и информационных систем для решения прикладных задач.
	УМЕТЬ			
2	Студент не умеет осуществлять выбор способа представления информации в соответствии с поставленной задачей; видеть и формулировать проблему информационной безопасности и надежности, ее анализировать, подбирать средства и методы для ее решения и ликвидации.	Студент испытывает затруднения при осуществлении выбора способа представления информации в соответствии с поставленной задачей; видеть и формулировать проблему информационной безопасности и надежности, ее анализировать, подбирать средства и методы для ее решения и ликвидации.	Студент умеет на базовом уровне, осуществлять выбор способа представления информации в соответствии с поставленной задачей; видеть и формулировать проблему информационной безопасности и надежности, ее анализировать, подбирать средства и методы для ее решения и ликвидации.	Студент системно умеет осуществлять выбор способа представления информации в соответствии с поставленной задачей; видеть и формулировать проблему информационной безопасности и надежности, ее анализировать, подбирать средства и методы для ее решения и ликвидации.
	ВЛАДЕТЬ			
3	Студент не владеет навыками применения типовых подходов, применяемых при анализе,	Студент владеет базовыми навыками применения типовых подходов, применяемых при	Студент владеет, на среднем уровне, основными навыками применения типовых	Студент, на высоком уровне, владеет навыками применения типовых подходов,

	планировании и оперативном управлении деятельностью промышленного предприятия.	анализе, планировании и оперативном управлении деятельностью промышленного предприятия.	подходов, применяемых при анализе, планировании и оперативном управлении деятельностью промышленного предприятия.	применяемых при анализе, планировании и оперативном управлении деятельностью промышленного предприятия..
	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

Семестр	Вид занятия (Л, ПР, ЛР)	Используемые интерактивные образовательные технологии	Количество часов
1	Л	Проблемная лекция, лекция-визуализация, лекция-диалог	4
	ПР	Ситуационный анализ, дискуссия, круглый стол	6
	ЛР	Не предусмотрены	
Итого:			10

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

По учебному плану не предусмотрено.

9.5. Вопросы к экзамену

1. Основные понятия теории компьютерной безопасности. Язык. Объекты. Субъекты. Доступ. Информационный поток. Основная аксиома теории защиты информации.
2. Ценность информации. Модели ценности. Решетка ценности и ее свойства.
3. Общая методология построения систем защиты.
4. Принципы построения системы защиты. Каналы утечки информации.
5. Понятие политики безопасности. Субъект-объектная модель политики безопасности.
6. Дискреционная политика безопасности. Определение. Проблема безопасности при атаке вида «Троянский конь».
7. Ролевая и мандатная политика безопасности. Определения. Политика безопасности информационных потоков.
8. Реализация политики безопасности в терминах субъект-объектной модели. Базовая теорема изолированной программной среды (ИПС).
9. Базовая теорема изолированной программной среды (ИПС). Политика изолированной программной среды.
10. Модель Харрисона-Руззо-Ульмана (HRU). Анализ безопасности модели HRU. Теоремы безопасности для модели HRU.
11. Основные положения модели Take-Grant.
12. Анализ механизмов передачи прав доступа для модели Take-Grant.
13. Расширенная модель Take-Grant. Де-факто правила и определение информационных потоков.

14. Замыкание графов доступов и информационных потоков расширенной модели Take-Grant.

15. Анализ путей распространения прав доступа и информационных потоков

расширенной модели Take-Grant.

16. Классическая модель Белла-ЛаПадула. Свойства безопасности для классическоймодели Белла-ЛаПадула.

17. Базовая теорема безопасности для классической модели Белла-ЛаПадула.

18. Политика low-watermark в модели Белла-ЛаПадула.

19. Безопасность переходов для модели Белла-ЛаПадула.

20. Базовая теорема безопасности для модели Белла-ЛаПадула с функцией переходов.Безопасность в смысле администрирования.

21. Модель невлияния в детерминированном и вероятностном случае.

22. Скрытые каналы: содержательное определение и примеры.

23. Автоматная модель и достаточные условия невидимости канала.

24. Модель скрытого канала через Proxy- сервер.

25. Общая архитектура системы и методы анализа.

26. Сигнатурный анализ. Теорема Клини.

27. Статистический анализ. Алгоритм NIDES.

28. Состоятельность оценки числа ребер случайного графа системы безопасности.

29. Модель мандатной политики целостности информации Биба.

30. Модель системы военных сообщений (СВС). Неформальное описание модели.

31. Модель системы военных сообщений (СВС). Формальное описание модели.

32. Модель системы военных сообщений (СВС). Безопасность переходов.

9.6. Контроль освоения компетенций

Вид контроля	**Контролируемые темы (разделы)**	**Компетенции, компоненты которых контролируются**
Устный опрос	*1,2,3,4,5,6*	*ПК-6*

ЛИСТ РЕГИСТРАЦИИ ИЗМЕНЕНИЙ

№ п/п	Номер и дата протокола заседания УМС	Перечень измененных пунктов
1.	31.08.2020, протокол № 1	Обновлен список литературы, список современных профессиональных баз данных и информационных справочных систем, список лицензионного и свободно распространяемого программного обеспечения в п. 5.