МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«МОСКОВСКИЙ ПОЛИТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ»
(МОСКОВСКИЙ ПОЛИТЕХ)

Факультет машиностроения

УТВЕРЖДАЮ
Декан факультета машиностроения
_____ /Е.В. Сафонов/
«15» февраля 2024 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

«Информационная безопасность и защита информации»

Направление подготовки
09.03.02 «Информационные системы и технологии»

Образовательная программа (профиль подготовки)
«Интеллектуальные информационно-измерительные системы»

Квалификация (степень) выпускника
Бакалавр

Форма обучения
Очная

Москва, 2024 г.

Разработчик(и):
доцент, к.т.н. /М.А.Иванько/

Согласовано:
Заведующий кафедрой «Информатики и информационных технологий», к.т.н. _____/Е.В. Булатников/

Согласовано:
Заведующий кафедрой «Стандартизация, метрология и сертификация»,
к.э.н., доцент / Т.А. Левина /

Содержание

1. Цели, задачи и планируемые результаты обучения по дисциплине

Целью освоения дисциплины «Информационная безопасность и защита информации» является знакомство обучающихся с основными алгоритмами и методами защиты информации, а также применение различных подходов к защите информации на практике.

Задачи дисциплины:

- изучение современных алгоритмов шифрования информации;
- изучение современных алгоритмов хэширования;
- изучение вирусов и методов борьбы с ними;
- изучение вопросов социальной инженерии;
- изучение методов построения комплексной системы безопасности.

Обучение по дисциплине «Информационная безопасность и защита информации» направлено на формирование у обучающихсяследующих компетенций:

Код и наименование компетенций	Индикаторы достижения компетенции
ОПК-3 Способен решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и сучетом основных требований информационной безопасности	ИОПК-3.1. знает принципы, методы и средства решения стандартных задач профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности ИОПК-3.2. умеет решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности ИОПК-3.3. имеет навыки подготовки обзоров, аннотаций, составления рефератов, научных докладов, публикаций и библиографии по научно-исследовательской работе с учетом требований информационной безопасности

2. Место дисциплины в структуре образовательной программы

Дисциплина «Информационная безопасность и защита информации» входит в образовательную программу подготовки бакалавра по направлению подготовки 09.03.02 «Информационные системы и технологии» и профилю подготовки «Интеллектуальные информационно-измерительные системы» для очной формы обучения.

3. Структура и содержание дисциплины

Общая трудоемкость дисциплины составляет 2 зачетных(е) единиц(ы) (72часов). Изучается на 5 семестре обучения. Форма промежуточной аттестации – зачет.

3.1 Виды учебной работы и трудоемкость

3.1.1.Очная форма обучения

№ п/п	Вид учебной работы	Количество часов	Семестры	
			5 семестр	
1	**Аудиторные занятия**	**36**	**36**	
	В том числе:			
1.1	Лекции	18	18	
1.2	Семинарские/практические занятия	18	18	
1.3	Лабораторные занятия			
2	**Самостоятельная работа**	**36**	**36**	
	В том числе:			
2.1	Подготовка и защита курсовой работы	0	0	
2.2	Самостоятельное изучение	36	36	
3	**Промежуточная аттестация**			
	Зачет/диф.зачет/экзамен		зачет	
	Итого	**72**	72	

3.2 Тематический план изучения дисциплины

(по формам обучения)

Тематический план размещён в приложении 1 к рабочей программе.

3.3 Содержание дисциплины

Тема 1.Понятие "информационная» безопасность и уровни ее обеспечения.

Проблема информационной безопасности общества. Определение понятия «информационная безопасность».

Тема 2.Составляющие информационной безопасности. Доступность информации. Целостность информации. Конфиденциальность информации.

Тема 3.Система формирования режима информационной безопасности. Задачи информационной безопасности общества. Уровни формирования режима информационной безопасности.

Тема 4. Нормативно-правовые основы информационной безопасности в РФ. Правовые основы информационной безопасности общества.Основные положения важнейших

законодательных актов РФ в области информационной безопасности и защиты информации. Ответственность за нарушения в сфере информационной безопасности.

Тема 5. Стандарты информационной безопасности: "Общие критерии". Требования безопасности к информационным системам. Принцип иерархии: класс – семейство – компонент – элемент. Функциональные требования. Требования доверия.

Тема 6. Стандарты информационной безопасности распределенных систем. Сервисыбезопасности в вычислительных сетях. Механизмы безопасности. Администрирование средств безопасности.

Тема 7. Стандарты информационной безопасности в РФ. Гостехкомиссия и ее роль в обеспечении информационной безопасности в РФ. Документы по оценке защищенности автоматизированных систем в РФ.

Тема 8. Административный уровень обеспечения информационной безопасности. Цели,задачи и содержание административного уровня. Разработка политики информационной безопасности.

Тема 9. Классификация угроз "информационной безопасности". Классы угроз информационной безопасности. Каналы несанкционированного доступа к информации.

Тема 10. Компьютерные вирусы и защита от них. Вирусы как угроза информационной безопасности. Компьютерные вирусы и информационная безопасность. Характерные черты компьютерных вирусов. Классификация компьютерных вирусов. Классификация компьютерных вирусов по среде обитания. Классификация компьютерных вирусов по особенностям алгоритма работы. Классификация компьютерных вирусов по деструктивным возможностям.

Тема 11. Антивирусные программы. Особенности работы антивирусных программ. Классификация антивирусных программ. Факторы, определяющие качество антивирусных программ. Профилактика компьютерных вирусов. Характеристика путей проникновения вирусов в компьютеры. Правила защиты от компьютерных вирусов.

3.4 Тематика семинарских/практических и лабораторных занятий

3.4.1.Семинарские/практические занятия

1. Понятие «информационная» безопасность и уровни ее обеспечения.

. Проблема информационной безопасности общества. Определение понятия «информационная безопасность».

2. Составляющие информационной безопасности. Доступность информации. Целостность информации. Конфиденциальность информации.

3. Система формирования режима информационной безопасности. Задачи информационной безопасности общества. Уровни формирования режима информационной безопасности.

4. Нормативно-правовые основы информационной безопасности в РФ. Правовые основы информационной безопасности общества. Основные положения важнейших законодательных актов РФ в области информационной безопасности и защиты информации. Ответственность за нарушения в сфере информационной безопасности.

5. Стандарты информационной безопасности: «Общие критерии». Требования безопасности к информационным системам. Принцип иерархии: класс – семейство – компонент – элемент.

Функциональные требования. Требования доверия.

6. Стандарты информационной безопасности распределенных систем. Сервисы безопасности в вычислительных сетях.

Механизмы безопасности. Администрирование средств безопасности.

7. Стандарты информационной безопасности в РФ. Гостехкомиссия и ее роль в обеспечении информационной безопасности в РФ. Документы по оценке защищенности автоматизированных систем в РФ.

8. Административный уровень обеспечения информационной безопасности. Цели, задачи и содержание административного уровня. Разработка политики информационной безопасности.

9.Классификация угроз "информационной безопасности".

Классы угроз информационной безопасности. Каналы несанкционированного доступа к информации.

10. Компьютерные вирусы и защита от них. Вирусы как угроза информационной безопасности. Компьютерные вирусы и информационная безопасность. Характерные черты компьютерных вирусов. Классификация компьютерных вирусов. Классификация компьютерных вирусов по среде обитания.

Классификация компьютерных вирусов по особенностям алгоритма работы. Классификация компьютерных вирусов по деструктивным возможностям.

11. Антивирусные программы. Особенности работы антивирусных программ. Классификация антивирусных программ. Факторы, определяющие качество антивирусных программ. Профилактика компьютерных вирусов. Характеристика путей проникновения вирусов в компьютеры. Правила защиты от компьютерных вирусов.

3.4.2.Лабораторные занятия
Отсутствуют

3.5 Тематика курсовых проектов (курсовых работ)

Курсовые работы/проекты отсутствуют

4. Учебно-методическое и информационное обеспечение

4.1 Нормативные документы и ГОСТы

1. Федеральный закон от 29 декабря 2012 года No 273-ФЗ «Об образовании в Российской Федерации» (с изменениями и дополнениями);

2. Федеральный государственный образовательный стандарт высшего образования - бакалавриат по направлению подготовки 09.03.02 Информационные системы и технологии, утвержденный Приказом Министерства образования и науки РФ от 19

сентября 2017 г. N 929 "Об утверждении федерального... Редакция с изменениями N 1456 от 26.11.2020;

3. Приказ Министерства образования и науки РФ от 05 апреля 2017 г. No 301 «Об утверждении Порядка организации и осуществления образовательной деятельности по образовательным программам высшего образования – программам бакалавриата, программам специалитета, программам магистратуры.

4.2 Основная литература

1. Фаронов, А. Е. Основы информационной безопасности при работе на компьютере : учебное пособие / А. Е. Фаронов. — 3-е изд. — Москва, Саратов : Интернет-Университет Информационных Технологий (ИНТУИТ), Ай Пи Ар Медиа, 2020. — 154 с. — ISBN 978-5-4497-0338-5. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: https://www.iprbookshop.ru/89453.html(дата обращения: 23.03.2024)

2. Фомин, Д. В. Информационная безопасность : учебно- методическое пособие по дисциплине «Информационная безопасность» для студентов экономических специальностей заочной формы обучения / Д. В. Фомин. — Саратов : Вузовское образование, 2018. — 54 с. — ISBN 978-5-4487-0298-3. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: https://www.iprbookshop.ru/77320.html (дата обращения: 23.03.2024)

3. Защита информации с использованием механизмов электронной цифровой подписи: учебно-метод. пособие / Д.Г. Демидов, О.Г. Швечкова, О.А. Москвитина, А.Н. Пылькин, К.А. Майков, К.Г. Смирнова ; Моск. гос. ун-т печати имени Ивана Федорова. — М. : МГУП имени Ивана Федорова, 2014. — 53 с. [Электронный ресурс] URL: http://elib.mgup.ru/showBook.php?id=99. (дата обращения: 23.03.2024)

4.3 Дополнительная литература

1. Галатенко, В. А. Основы информационной безопасности : учебное пособие / В. А. Галатенко. — 3-е изд. — Москва : Интернет-Университет Информационных Технологий (ИНТУИТ), Ай Пи Ар Медиа, 2020. — 266 с. — ISBN 978-5-4497-0675-1. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: https://www.iprbookshop.ru/97562.html (дата обращения: 23.03.2024)

Электронные образовательные ресурсы

Проведение занятий и аттестаций возможно в дистанционном формате с применением системы дистанционного обучения университета (СДО-LMS) на основе разработанных кафедрой электронных образовательных ресурсов (ЭОР) по всем Темам программы:.

Название ЭОР	
Информационная безопасность и защита информации	https://online.mospolytech.ru/course/view.php?id=11843

Разработанные ЭОР включают тренировочные и итоговые тесты.

Порядок проведения работ в дистанционном формате устанавливается отдельными распоряжениями проректора по учебной работе и/или центром учебно-методической работы.

Интернет-ресурсы включают учебно-методические материалы в электронном виде, представленные на сайте mospolytech.ru

Каждый студент обеспечен индивидуальным неограниченным доступом к электронным библиотекам университета

(elib.mgup; lib.mami.ru/lib/content/elektronyy-katalog) к электронно-библиотечным системам (электронным библиотекам)

4.4 Лицензионное и свободно распространяемое программное обеспечение

Отсутствует

4.5 Современные профессиональные Информационная безопасность и защита информации и информационные справочные системы

Перечень ресурсов сети Интернет, доступных для освоения дисциплины:

№	Наименование	Ссылка на ресурс	Доступность
Информационно-справочные системы			
	Информационные ресурсы Сети КонсультантПлюс	http:// www.consultant.ru	Доступно
Электронно-библиотечные системы			
	Лань	https://e.lanbook.com/	Доступна в сети Интернет без ограничений
	IPR Books	https://www.iprbookshop.ru/	Доступна в сети Интернет без ограничений
Профессиональные Информационная безопасность и защита информации			
	База данных научной электронной библиотеки	http://www.elibrary.ru	Доступно

	(eLIBRARY.RU)		
	WebofScienceCoreCollection – политематическая реферативно-библиографическая и наукометрическая (библиометрическая) база данных	http://webofscience.com	Доступно

5. Материально-техническое обеспечение

Лекционная аудитория общего фонда, переносной мультимедийный комплекс (проектор, ноутбук)

6. Методические рекомендации

Методика преподавания дисциплины и реализация компетентностного подхода в изложении и восприятии материала предусматривает использование следующих активных и интерактивных форм проведения аудиторных и внеаудиторных занятий:

– аудиторные занятия: лекции, лабораторные работы, тестирование;

– внеаудиторные занятия: самостоятельное изучение отдельных вопросов, подготовка к лабораторным работам.

Образовательные технологии

Возможно проведение занятий и аттестаций в дистанционном формате с применением системы дистанционного обучения университета (СДО-LMS) на основе разработанных электронных образовательных ресурсов (ЭОР) (см. п.4.4).

Порядок проведения работ в дистанционном формате устанавливается отдельными распоряжениями проректора по учебной работе и/или центром учебно-методической работы.

6.1 Методические рекомендации для преподавателя по организации обучения

6.1.1. Преподаватель организует преподавание дисциплины в соответствии с требованиями "Положения об организации образовательного процесса в московском политехническом университете и его филиалах", утверждённым ректором университета.

6.1.2. На первом занятии преподаватель доводит до сведения студентов содержание рабочей программы дисциплины (РПД) и предоставляет возможность ознакомления с программой.

6.1.3. Преподаватель особенно обращает внимание студентов на:

- виды и формы проведения занятий по дисциплине, включая порядок проведения занятий с применением технологий дистанционного обучения и системы дистанционного обучения университета (СДО мосполитеха);

- виды, содержание и порядок проведения текущего контроля успеваемости в соответствии с фондом оценочных средств;

- форму, содержание и порядок проведения промежуточной аттестации в соответствии с фондом оценочных средств, предусмотренным РПД.

6.1.4. Доводит до сведения студентов график выполнения учебных работ, предусмотренных РПД.

6.1.5. Необходимо с самого начала занятий рекомендовать студентам основную и дополнительную литературу и указать пути доступа к ней.

6.1.6. Вначале или в конце семестра дать список вопросов для подготовки к промежуточной аттестации (экзамену или зачёту).

6.1.7. Рекомендуется факт ознакомления студентов с РПД и графиком работы письменно зафиксировать подписью студента в листе ознакомления с содержание РПД.

6.1.8. Преподаватели, ведущий лекционные и практические занятия, должны согласовывать тематический план практических занятий, использовать единую систему обозначений, терминов, основных понятий дисциплины.

6.1.9. При подготовке **к семинарскому занятию** по перечню объявленных тем преподавателю необходимо уточнить план их проведения, продумать формулировки и содержание учебных вопросов, выносимых на обсуждение, ознакомиться с перечнем вопросов по теме семинара.

В ходе семинара во вступительном слове раскрыть практическую значимость темы семинарского занятия, определить порядок его проведения, время на обсуждение каждого учебного вопроса. Применяя фронтальный опрос дать возможность выступить всем студентам, присутствующим на занятии.

В заключительной части семинарского занятия следует подвести его итоги: дать оценку выступлений каждого студента и учебной группы в целом. Раскрыть положительные стороны и недостатки проведенного семинарского занятия. Ответить на вопросы студентов. Выдать задания для самостоятельной работы по подготовке к следующему занятию.

6.1.10. Целесообразно в ходе защиты **лабораторных работ** задавать выступающим и аудитории дополнительные и уточняющие вопросы с целью выяснения их позиций по существу обсуждаемых проблем.

Возможно проведение занятий и аттестаций в дистанционном формате с применением системы дистанционного обучения университета (СДО-LMS). Порядок проведения работ в дистанционном формате устанавливается отдельными распоряжениями проректора по учебной работе и/или центром учебно-методической работы.

6.2 Методические указания для обучающихся по освоению дисциплины

1.2.1. Студент с самого начала освоения дисциплины должен внимательно ознакомится с рабочей программой дисциплины.

1.2.2. Студенту необходимо составить для себя график выполнения учебных работ, предусмотренных РПД с учётом требований других дисциплин, изучаемых в текущем семестре.

1.2.3. При проведении занятий и процедур текущей и промежуточной аттестации с использованием инструментов информационной образовательной среды дистанционного образования университета (LMSмосполитеха), как во время контактной работы с преподавателем так и во время самостоятельной работы студент должен обеспечить техническую возможность дистанционного подключения к системам дистанционного обучения. При отсутствии такой возможности обсудить ситуацию с преподавателем дисциплины.

1.2.4. Самостоятельная работа является одним из видов учебных занятий. Цель самостоятельной работы – практическое усвоение студентами вопросов, рассматриваемых в процессе изучения дисциплины.

Виды внеаудиторной самостоятельной работы:

- самостоятельное изучение отдельных тем дисциплины;

- подготовка к лекционным занятиям;
- подготовка к семинарам и практическим занятиям;
- оформление отчетов по выполненным лабораторным работам и подготовка к их защите.

Для выполнения любого вида самостоятельной работы необходимо пройти следующие этапы:

- определение цели самостоятельной работы;
- конкретизация познавательной задачи;
- самооценка готовности к самостоятельной работе;
- выбор адекватного способа действия, ведущего к решению задачи;
- планирование работы (самостоятельной или с помощью преподавателя) над заданием;
- осуществление в процессе выполнения самостоятельной работы самоконтроля (промежуточного и конечного) результатов работы и корректировка выполнения работы;
- рефлексия;
- презентация самостоятельной работы или защита лабораторной работы.

7. Фонд оценочных средств

Фонд оценочных средств представлен в Приложении 2 к рабочей программе и включает темы:

7.1. Методы контроля и оценивания результатов обучения
7.2 Шкала и критерии оценивания результатов обучения
7.3. Оценочные средства
7.3.1. Текущий контроль
7.3.2. Промежуточная аттестация

Приложение 2

Тема 7 РПД - ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

ПО ДИСЦИПЛИНЕ

«Информационная безопасность и защита информации»

Направление подготовки

09.03.02 Информационные системы и технологии

Образовательная программа (профиль подготовки)

«Интеллектуальные информационно-измерительные системы»

7. Фонд оценочных средств

В процессе обучения в течение семестра используются оценочные средства текущего контроля успеваемости и промежуточных аттестаций. Применяются следующие оценочные средства: тест, защита лабораторных работ, экзамен.

Обучение по дисциплине **«Информационная безопасность и защита информации»** направлено на формирование у обучающихся следующих компетенций:

Код и наименование компетенций	Индикаторы достижения компетенции
ОПК-3 Способен решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и сучетом основных требований информационной безопасности	ИОПК-3.1. знает принципы, методы и средства решения стандартных задач профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности ИОПК-3.2. умеет решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности ИОПК-3.3. имеет навыки подготовки обзоров, аннотаций, составления рефератов, научных докладов, публикаций и библиографии по научно-исследовательской работе с учетом требований информационной безопасности

7.1 Методы контроля и оценивания результатов обучения

№ ОС	Наименование оценочного средства	Краткая характеристика оценочного средства	Представление оценочного средства в ФОС
1	Лабораторные работы (ПрР)	Оформленные отчеты (журнал) лабораторных работ, предусмотренных рабочей программой дисциплины с отметкой преподавателя «зачтено», если выполнены и оформлены все работы.	Перечень лабораторных работ
2	Тесты (Т)	Студентам предлагается ответить на тесты в течении 45 минут. Критерием успешной сдачи тестирования считается процент правильных ответов более 65% процентов.	Банк вопросов

7.2 Шкала и критерии оценивания результатов обучения

Форма промежуточной аттестации: зачет.

Обязательными условиями подготовки студента к промежуточной аттестации является выполнение и защита студентом лабораторных работ, предусмотренных рабочей программой и прохождение всех промежуточных тестов не ниже, чем на 70% правильных ответов. Промежуточные тестирования могут проводится как в аудитории Университета под контролем преподавателя, так и дистанционном формате на усмотрение преподавателя.

Шкала оценивания для зачета:

Шкала оценивания	Описание
Зачтено	Выполнены все виды учебной работы, предусмотренные РПД. Студент демонстрирует соответствие знаний, умений, навыков приведенным в таблицах показателей, оперирует приобретенными знаниями, умениями, навыками, применяет их в ситуациях повышенной сложности. При этом могут быть допущены незначительные ошибки, неточности, затруднения при аналитических операциях, переносе знаний и умений на новые, нестандартные ситуации.

Не зачтено	Не выполнен один или более видов учебной работы, предусмотренных РПД. Студент демонстрирует неполное соответствие знаний, умений, навыков приведенным в таблицах показателей, допускаются значительные ошибки, проявляется отсутствие знаний, умений, навыков по ряду показателей, студент испытывает значительные затруднения при оперировании знаниями и умениями при их переносе на новые ситуации.

Шкала оценивания для экзамена:

Шкала оценивания	**Описание**
Отлично	Выполнены все виды учебной работы, предусмотренные учебным планом. Студент демонстрирует соответствие знаний, умений, навыков приведенным в таблицах показателей, оперирует приобретенными знаниями, умениями, навыками, применяет их в ситуациях повышенной сложности. При этом может быть допущена незначительная ошибка, неточность, затруднение при аналитических операциях, переносе знаний и умений на новые, нестандартные ситуации.
Хорошо	Выполнены все виды учебной работы, предусмотренные учебным планом. Студент демонстрирует неполное, правильное соответствие знаний, умений, навыков приведенным в таблицах показателей, либо если при этом были допущены 2-3 несущественные ошибки.
Удовлетворительно	Выполнены все виды учебной работы, предусмотренные учебным планом. Студент демонстрирует соответствие знаний, в котором освещена основная, наиболее важная часть материала, но при этом допущена одна значительная ошибка или неточность.
Неудовлетворительно	Не выполнен один или более видов учебной работы, предусмотренных учебным планом. Студент демонстрирует неполное соответствие знаний, умений, навыков приведенным в таблицах показателей, допускаются значительные ошибки, проявляется отсутствие знаний, умений, навыков по ряду показателей, студент испытывает значительные затруднения при оперировании знаниями и умениями при их переносе на новые ситуации.

7.3 Оценочные средства

7.3.1. Текущий контроль

Текущий контроль выполняется с применением Банка вопросов. Примеры тестов представлены ниже. Результаты текущего контроля успешно зачитываются, если при тестировании набрано не менее 75 баллов из 100 возможных.

Рекомендуемые темы рефератов

Рефераты не предусмотрены

7.3.2. Промежуточная аттестация

Промежуточная аттестация проводится на 2 семестре обучения в форме зачета.

Экзамен проводится по билетам, ответы предоставляются письменно с последующим устным собеседованием. Билеты формируются из вопросов представленного ниже перечня. Экзамен может проводиться в форме тестирования с использованием (СДО-LMS) на основе разработанных электронных образовательных ресурсов (ЭОР)

Регламент проведения зачета:

1. В билет включается 2 вопроса из разных Тем дисциплины.
2. Перечень вопросов содержит 30 вопросов по изученным темам на лекционных и лабораторных занятиях (прилагается).
3. Время на подготовку письменных ответов - до 40 мин, устное собеседование - до 10 минут.
4. Проведение аттестации (экзамена) с использованием средств электронного обучения и дистанционных образовательных технологий выполняется в соответствии с утверждённым в университете "Порядком проведения промежуточной аттестации с использованием средств электронного обучения и дистанционных образовательных технологий"

Вопросы к экзамену.

1. Криптография. Основные определения и алгоритмы.
2. Классификация криптоалгоритмов.
3. Симметричные криптоалгоритмы.
4. Скремблеры.
5. Блочные шифры.
6. Сеть Фейштеля. Блочный шифр TEA.
7. Общие сведения о конкурсе AES: шифр MARS
8. Общие сведения о конкурсе AES: шифр RC6
9. Общие сведения о конкурсе AES: шифр Serpent
10. Общие сведения о конкурсе AES: шифр TwoFish
11. Общие сведения о конкурсе AES: шифр Rijndael.
12. Симметричные криптосистемы.
13. Асимметричные криптоалгоритмы.
14. Алгоритм RSA.
15. Обмен ключами по алгоритму Диффи-Хеллмана.
16. Общая схема асимметричной криптосистемы
17. Общие сведения о вирусах.
18. Вирусы под Unix-подобные системы.

19. Классификация вирусов.
20. Классификация вирусов по среде обитания.
21. Классификация вирусов по способам заражения.
22. Классификация вирусов по наносимому вреду.
23. Классификация вирусов по особенностям алгоритма.
24. Классификация вирусов по версии DrWeb.
25. Понятие и классификация антивирусных программ.
26. Обзор современных антивирусных программ.
27. Поиск вирусов вручную.
28. Инструменты для борьбы с вирусами.
29. Понятие социальной инженерии.
30. Мотивы и методы социальной инженерии.
31. Получение конфиденциальной информации.
32. Заражение компьютера вирусом.
33. Инструменты социальной инженерии.
34. Массовые рассылки (известные так же, как спам).
35. Баннеры. Обратная социальная инженерия.
36. Безопасность в интернете
37. Общий обзор угроз, рекомендации по безопасности.
38. Безопасная работа в Интернете: анализ веб-сайтов, безопасныйпоиск, надежные пароли.
39. Безопасная работа в Интернете: электронная почта, платежи, защитное ПО.
40. Дополнительные средства повышения безопасности.
41. Резервное копирование и шифрование данных, вопросы обеспечения физической безопасности компьютера.
42. Безопасность при работе на компьютере нескольких пользователей.
43. Безопасность в социальных сетях.
44. Концепции и аспекты обеспечения информационной безопасности
45. Понятия экономической и информационной безопасности.
46. Ключевые вопросы ИБ.
47. Виды угроз информационной безопасности и классификация источников угроз.
48. Основные виды защищаемой информации.
49. Правовое обеспечение информационной безопасности.
50. Основные аспекты построения системы информационной безопасности

Приложение 1

Тематический план содержания дисциплины «Информационная безопасность и защита информации»
по направлению подготовки
09.03.02 «Информационные системы и технологии»
Профиль подготовки
Интеллектуальные информационно-измерительные системы
Форма обучения: очная
Год набора: 2024/2025
(бакалавр)

n/n	Тема	Виды учебной работы, включая самостоятельную работу студентов, и трудоемкость в часах					Виды самостоятельной работы студентов					Формы аттестации	
		Л	П/С	Лаб	СРС	КСР	К.Р.	К.П.	РГР	Реферат	К/р	Э	З
1	Тема 1.Понятие "информационная» безопасность и уровни ее обеспечения. Проблема информационной безопасности общества. Определение понятия «информационная безопасность». Тема 2.Составляющие информационной безопасности. Доступность информации. Целостность информации. Конфиденциальность информации.	2	2		+								

2	Тема 3.Система формирования режима информационной безопасности. Задачи информационной безопасности общества. Уровни формирования режима информационной безопасности.	**2**	**2**		**+**								
3	Тема 4. Нормативно-правовые основы информационной безопасности в РФ. Правовые основы информационной безопасности общества. Основные положения важнейших законодательных актов РФ в области информационной безопасности и защиты информации. Ответственность за нарушения в сфере информационной безопасности.	**2**	**2**		**+**								
4	Тема 5. Стандарты информационной безопасности: "Общие критерии". Требования безопасности к информационным системам. Принцип иерархии: класс – семейство – компонент – элемент. Функциональные требования. Требования доверия.	**2**	**2**		**+**								
5	Тема 6. Стандарты информационной безопасности распределенных систем.	**2**	**2**		**+**								

	Сервисы безопасности в вычислительных сетях. Механизмы безопасности. Администрирование средств безопасности.												
6	Тема 7. Стандарты информационной безопасности в РФ. Гостехкомиссия и ее роль в обеспечении информационной безопасности в РФ. Документы по оценке защищенности автоматизированных систем в РФ.	**2**	**2**		**+**								
7	Тема 8. Административный уровень обеспечения информационной безопасности. Цели,задачи и содержание административного уровня. Разработка политики информационной безопасности. Тема 9. Классификация угроз "информационной безопасности". Классы угроз информационной безопасности. Каналы несанкционированного доступа к информации.	**2**	**2**		**+**								
8	Тема 10. Компьютерные вирусы и защита от них. Вирусы как угроза информационной безопасности. Компьютерные вирусы и информационная безопасность.	**2**	**2**		**+**								

	Характерные черты компьютерных вирусов. Классификация компьютерных вирусов. Классификация компьютерных вирусов по среде обитания. Классификация компьютерных вирусов по особенностям алгоритма работы. Классификация компьютерных вирусов по деструктивным возможностям.												
9	Тема 11. Антивирусные программы. Особенности работы антивирусных программ. Классификация антивирусных программ. Факторы, определяющие качество антивирусных программ. Профилактика компьютерных вирусов. Характеристика путей проникновения вирусов в компьютеры. Правила защиты от компьютерных вирусов.	**2**	**2**										
	Форма аттестации												**З**
	Всего часов по дисциплине	**18**	**18**		**36**								