МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«Национальный исследовательский ядерный университет «МИФИ»

Технологический институт –
филиал федерального государственного автономного образовательного учреждения высшего образования «Национальный исследовательский ядерный университет «МИФИ»
(ТИ НИЯУ МИФИ)

КАФЕДРА ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ И ПРИКЛАДНОЙ МАТЕМАТИКИ

ОДОБРЕНО
Ученым советом ТИ НИЯУ
Протокол № 4 от 08.07.2024 г.

АДАПТИРОВАННАЯ РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ

(для лиц с инвалидностью и ограниченными возможностями здоровья с общим заболеванием)

Защита информации

(наименование дисциплины)

Направление подготовки **09.03.01 Информатика и вычислительная техника**

Профиль подготовки **Программирование, информационные системы и телекоммуникации**

Квалификация (степень) выпускника **бакалавр**

Форма обучения **очная**

Семестр	7	Итого
Трудоемкость, кред.	4	4
Общий объем курса, час.	144	144
Лекции, час.	16	16
Практич. занятия, час.	16	16
Лаборат. работы, час.	8	8
В форме практической подготовки, час.	24	24
СРС, час.	68	68
КСР, час.	-	-
Форма контроля – экзамен	36	36

г. Лесной – 2024 г.

АННОТАЦИЯ

Адаптированная рабочая программа учебной дисциплины для обучающихся инвалидов и обучающихся с ограниченными возможностями здоровья с общим заболеванием учитывает особенности их психофизического развития, индивидуальных возможностей и необходимость создания специальных условий их обучения.

В ходе освоения дисциплины «Защита информации» студенты знакомятся с различными угрозами безопасности в сфере информационных технологий, изучают различные алгоритмы шифрования, используемые при передаче конфиденциальной информации. В процессе обучения студенты получают практические навыки работы с программным обеспечением, позволяющим организовывать безопасные каналы связи. В результате освоения курса у выпускников формируется ответственное отношение к вопросам информационной безопасности в профессиональной деятельности.

1. ЦЕЛЬ ОСВОЕНИЯ УЧЕБНОЙ ДИСЦИПЛИНЫ

Целью учебной дисциплины «Защита информации» является изучение современных методов и средства защиты информации и их использование при проектировании комплексных систем защиты программного обеспечения для безопасного функционирования объектов атомной отрасли.

Главной **задачей** дисциплины является получение базовых знаний и навыков в области информационной безопасности, необходимые студентам в их дальнейшей профессиональной деятельности.

Учебные задачи дисциплины:

- изучение методов криптографической защиты информации и разработки шифров;
- знакомство с правовыми основами защиты информации и методами анализа безопасности компьютерных систем;
- изучение и практическое использование современных методов криптографии для защиты информации, хранящейся в информационных системах или передаваемой по каналам связи;
- изучение методов защиты информации и программного обеспечения от несанкционированного доступа;
- создание электронной цифровой подписи;
- изучение формальных моделей политик безопасности, политик управления доступом в компьютерных системах.

2. МЕСТО УЧЕБНОЙ ДИСЦИПЛИНЫ В СТРУКТУРЕ ООП ВО

Дисциплина «Защита информации» изучается студентами четвертого курса, входит в профессиональный модуль раздела Б.1 вариативной части учебного плана по направлению подготовки «Информатика и вычислительная техника» профиля подготовки «Программирование, информационные системы и телекоммуникации».

Дисциплина основывается на знаниях, полученных в результате освоения дисциплин «Информатика», «Алгоритмизация и программирование», «Системное программное обеспечение».

Изучение дисциплины необходимо для прохождения преддипломной практики, а также практической работы выпускников по специальности.

Указанные связи и содержание дисциплины «Защита информации» дают обучающемуся системное представление о комплексе изучаемых дисциплин в соответствии ОС ВО НИЯУ МИФИ, что обеспечивает соответственный теоретический

уровень и практическую направленность в системе обучения будущей деятельности бакалавра.

3. ФОРМИРУЕМЫЕ КОМПЕТЕНЦИИ И ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОБУЧЕНИЯ

Процесс изучения дисциплины «Защита информации» направлен на формирование следующих компетенций: ОПК-3; ПК-6.3; УКЦ-2.

Код компетенции	Компетенция
ОПК-3	Способен решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности
ПК-6.3	Способен проектировать, внедрять и администрировать компьютерные сети, анализировать возможные угрозы безопасности компьютерных систем и сетей
УКЦ-2	Способен искать нужные источники информации и данные, воспринимать, анализировать, запоминать и передавать информацию с использованием цифровых средств, а также с помощью алгоритмов при работе с полученными из различных источников данными с целью эффективного использования полученной информации для решения задач

Индикаторами достижения компетенций являются:

Код компетенции	Код индикатора	Индикатор
ОПК-3	З-ОПК-3	Знать: 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
	У-ОПК-3	Уметь: решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности
	В-ОПК-3	Владеть: навыками подготовки обзоров, аннотаций, составления рефератов, научных докладов, публикаций и библиографии по научно-исследовательской работе с учетом требований информационной безопасности
ПК-6.3	З-ПК-6.3	Знать: современные методы и средства защиты информации, возможности различных ОС, архитектуру и устройство вычислительных и информационных систем, основные принципы построения и администрирования компьютерных сетей
	У-ПК-6.3	Уметь: определять возможные угрозы безопасности компьютерным системам и техническим устройствам,

Код компетенции	Код индикатора	Индикатор
		анализировать и обосновывать выбор программных средств технических устройств, строить и администрировать компьютерные сети
	В-ПК-6.3	Владеть: способами и навыками обнаружения возможных угроз безопасности компьютерным системам, методами обнаружения и устранения угроз безопасности в компьютерных сетях
УКЦ-2	З-УКЦ-2	Знать: методики сбора и обработки информации с использованием цифровых средств, а также актуальные российские и зарубежные источники информации в сфере профессиональной деятельности, принципы, методы и средства решения стандартных задач профессиональной деятельности с использованием цифровых средств и с учетом основных требований информационной безопасности
	У-УКЦ-2	Уметь: применять методики поиска, сбора и обработки информации; с использованием цифровых средств, осуществлять критический анализ и синтез информации, полученной из разных источников, и решать стандартные задачи профессиональной деятельности с использованием цифровых средств и с учетом основных требований информационной безопасности
	В-УКЦ-2	Владеть: методами поиска, сбора и обработки, критического анализа и синтеза информации с использованием цифровых средств для решения поставленных задач, навыками подготовки обзоров, аннотаций, составления рефератов, научных докладов, публикаций и библиографии по научно-исследовательской работе с использованием цифровых средств и с учетом требований информационной безопасности

4. ВОСПИТАТЕЛЬНАЯ РАБОТА

Код	Направление/цели	Создание условий, обеспечивающих:	Использование воспитательного потенциала учебных дисциплин
В21	Профессиональное воспитание	формирование способности и стремления следовать в профессии нормам поведения, обеспечивающим нравственный характер трудовой деятельности и неслужебного поведения	Использование воспитательного потенциала дисциплин профессионального модуля для развития навыков коммуникации, командной работы и лидерства, творческого инженерного мышления, стремления следовать в профессиональной деятельности нормам поведения, обеспечивающим нравственный характер

Код	Направление/цели	Создание условий, обеспечивающих:	Использование воспитательного потенциала учебных дисциплин
			трудовой деятельности и неслужебного поведения, ответственности за принятые решения через подготовку практических заданий, решение кейсов.
В23		формирование культуры информационной безопасности	Использование воспитательного потенциала дисциплин профессионального модуля для формирование базовых навыков информационной безопасности через изучение последствий халатного отношения к работе с информационными системами, базами данных (включая персональные данные), приемах и методах злоумышленников, потенциальном уроне пользователям.
В25		формирование навыков цифровой гигиены	Использование воспитательного потенциала дисциплин профессионального модуля для формирования навыков цифровой гигиены, а также системности и гибкости мышления, посредством изучения методологических и технологических основ обеспечения информационной безопасности и кибербезопасности
В27		формирование профессионально значимых установок: не производить, не копировать и не использовать программные и технические средства, не приобретённые на законных основаниях; не нарушать признанные нормы авторского права; не нарушать тайны передачи сообщений, не практиковать вскрытие информационных систем	Использование воспитательного потенциала профильных дисциплин для формирования культуры обращения с информацией, а также формирования ответственного отношения к соблюдению социально-правовых норм в профессиональной среде

Код	Направление/цели	Создание условий, обеспечивающих:	Использование воспитательного потенциала учебных дисциплин
		и сетей передачи данных; соблюдать конфиденциальность доверенной информации	

Организация интерактивных мероприятий и реализация специализированных заданий с воспитательным и социальным акцентом:

- основные принципы защиты информации в информационных системах (круглый стол);
- основные угрозы информационной безопасности и как их избежать (дискуссия);
- криптографические методы защиты информации: использование шифров в повседневной жизни (круглый стол);
- электронная цифровая подпись: возможно ли полностью отказаться от «живой» подписи? (дискуссия);
- компьютерные атаки и технологии их обнаружения (круглый стол);
- технические каналы утечки информации (анализ ситуаций).

Перечисленные мероприятия направлены на:

- формирование ответственного отношения при обращении с цифровой информацией;
- формирование личной ответственности за соблюдение правовых норм в области защиты информации;
- развитие способности работать в группе и коллективно решать поставленные задачи.

Воспитательная работа с инвалидами и лицами с ограниченными возможностями здоровья осуществляется инклюзивно, с предоставлением возможности участия во всех университетских мероприятиях, направленных на развитие нравственно-эстетического и патриотического воспитания. Организация воспитательной работы со студентами-инвалидами формируется на основе психолого-педагогической поддержки.

Основные задачи психолого-педагогической поддержки:

- формирование у обучающихся с ограниченными возможностями здоровья навыков эффективного обучения;
- развитие мотивации самообразования и личностного самосовершенствования у студентов с ОВЗ;
- психологическая подготовка студента-инвалида к осуществлению профессии и связанным с ней взаимодействиям;

совершенствование у учащегося с ограниченными возможностями профессионально-значимых личностных свойств.

5. СТРУКТУРА И СОДЕРЖАНИЕ УЧЕБНОЙ ДИСЦИПЛИНЫ

Общая трудоемкость дисциплины составляет 4 зачетные единицы, 144 часа.

№ п/п	Наименование раздела учебной дисциплины	Недели	Виды учебной деятельности, включая самостоятельную работу студентов и трудоемкость в ак.часах	Обязат. текущий контроль успеваемости (*форма,*	Аттестация раздела (*форма, неделя*)	Максимальный балл за раздел

			Лекции	Практические занятия	Лабораторные работы	Самостоятельная работа	*неделя*) [1]		
1	Раздел 1. Основные понятия в области защиты информации	1-11	13	11	8	52	ЛР1-2 (20 б.), Т1 (8 нед. – 15 б.)	КИ1	55
2	Раздел 2. Способы атак и технологии их обнаружения	12-16	3	5	0	16	Т2 (15 нед. – 15 б.)	КИ2	15
	Экзамен								30
	ИТОГО:		**16**	**16**	**8**	**68**			**100**

НАИМЕНОВАНИЕ ТЕМ И СОДЕРЖАНИЕ ЛЕКЦИОННЫХ ЗАНЯТИЙ

Раздел 1. Основные понятия в области защиты информации

1. Основные понятия в области технической защиты информации (понятие информации, основные свойства – целостность, конфиденциальность, доступность, виды защиты – правовая, физическая, организационная, техническая и т.д.);
2. Концептуальные основы защиты информации. Система документов по технической защите информации (стратегия национальной безопасности Российской Федерации, доктрина информационной безопасности)
3. Законодательные и иные правовые акты в области технической защиты информации.
4. Органы по технической защите информации в РФ. Государственные органы в области защиты информации. ФСБ и ФСТЭК России.
5. Лицензирование деятельности в области ТЗИ (какие государственные органы выдают лицензии по ТЗИ, порядок получения лицензий, осуществление государственного надзора в области ТЗИ).
6. Сертификация средств защиты информации (общий порядок сертификации средств защиты информации, порядок сертификации во ФСТЭК России).
7. Аттестация объекта информатизации по требованиям безопасности информации.
8. Классификация угроз и объектов защиты.
9. Методы оценки опасности угроз (количественный, качественный).
10. Объект информатизации. Классификация объектов защиты.
11. Классификация информации.

[1] ЛР – лабораторная работа, Т – тест.

12. Классификация автоматизированных систем.
13. Классификация средств вычислительной техники.

Раздел 2. Способы атак и технологии их обнаружения

1. Угрозы несанкционированного доступа к информации.
2. Понятие несанкционированного доступа.
3. Модель потенциального нарушителя.
4. Основные классы атак в сетях на базе TCP/IP.
5. Программно-математическое воздействие.
6. Вредоносные программы и их классификация.
7. Недекларированные возможности программного обеспечения.
8. Антивирусные программы.
9. Межсетевой экран.
10. Система обнаружения вторжений.
11. Требования и рекомендации по защите информации, обрабатываемой средствами вычислительной техники.
12. Порядок обеспечения защиты информации в АС.
13. Требования и рекомендации в зависимости от типа АС.
14. Защита конфиденциальной информации на автоматизированных рабочих местах на базе автономных ПЭВМ.
15. Защита информации в локальных вычислительных сетях.
16. Защита информации при межсетевом взаимодействии.
17. Защита информации при работе с системами управления базами данных.
18. Порядок обеспечения защиты информации при взаимодействии с информационными сетями общего пользования.
19. Основные требования и рекомендации по защите служебной тайны и персональных данных.
20. Основные рекомендации по защите информации, составляющей коммерческую тайну.
21. Технические каналы утечки акустической информации.
22. Основные понятия в области акустики. Классификация акустических каналов утечки информации.
23. Побочные электромагнитные излучения и наводки.
24. Методы защиты информации от утечки через ПЭМИН.
25. Средства и методы обнаружения технических каналов утечки информации.
26. Мероприятия по выявлению технических каналов утечки информации. Оценка защищенности информации от утечки по ТКУИ.

Аудиторные занятия и бюджет времени на самостоятельную подготовку студента

№п/п	Наименование раздела, краткое наименование темы	Аудиторные занятия (час.)	Практическая подготовка	Самостоятельная работа

		Лекции	Практические занятия	Лабораторные работы		
1	**Основные понятия в области защиты информации.** Основные понятия в области технической защиты информации.	1	1	-	1	4
2	**Основные понятия в области защиты информации.** Концептуальные основы защиты информации.	1	1	-	1	10
3	**Основные понятия в области защиты информации.** Органы по технической защите информации в РФ.	1	1	-	1	4
4	**Основные понятия в области защиты информации.** Лицензирование деятельности в области ТЗИ.	2	2	-	2	6
5	**Основные понятия в области защиты информации.** Сертификация средств защиты информации.	2	1	-	1	6
6	**Основные понятия в области защиты информации.** Классификация угроз и объектов защиты.	2	1	-	1	6
7	**Основные понятия в области защиты информации.** Методы оценки опасности угроз.	2	2	4	6	6
8	**Основные понятия в области защиты информации.** Классификация объектов защиты.	2	2	4	6	6
9	**Способы атак и технологии их обнаружения.** Угрозы несанкционированного доступа к информации.	1	1	-	1	6
10	**Способы атак и технологии их обнаружения.** Порядок обеспечения защиты информации в АС.	1	2	-	2	4
11	**Способы атак и технологии их обнаружения.** Технические каналы утечки информации.	1	2	-	2	6
	Итого	**16**	**16**	**8**	**24**	**68**

6. ОБРАЗОВАТЕЛЬНЫЕ ТЕХНОЛОГИИ

В образовательном процессе используются социально-активные и рефлексивные методы обучения, технологии социокультурной реабилитации с целью оказания помощи в установлении полноценных межличностных отношений с другими студентами, создании комфортного психологического климата в студенческой группе.

Учитываются индивидуальные психофизические особенности обучающихся при организации учебного процесса и контроле знаний:

- операциональные характеристики деятельности (темп, продуктивность, работоспособность, истощаемость, объем предполагаемых заданий);

- использовать дозирование нагрузок с учетом индивидуальных особенностей;
- использовать чередование видов деятельности; короткие четко сформулированные задания; текстовую информацию, представленную в виде печатных таблиц на стендах или электронных носителях;
- при предъявлении нового и закрепление изученного материала использовать вариативное повторение, пошаговые инструкции. Оказывать дозированную помощь;
- использовать закрепление и многократное повторение материала с переносом на аналогичный материал, в продуктивных видах деятельности. Повторять действия для выработки умений и навыков;
- проявлять особый педагогический такт. Использовать индивидуальный подход при оценивании деятельности понятное обучающемуся;
- использовать замедленный темп обучения; упрощать структуру знаний, умений и навыков в соответствии с психофизическими возможностями обучающегося;
- максимально опираться на практическую деятельность и опыт обучающегося, на наиболее развитые его способности; осуществлять дифференцированное руководство учебной деятельностью обучающегося;
- подбор индивидуального темпа работы и нагрузки обучающегося; давать предельно развернутые инструкции, увеличить количество практических проб.

Тьютор организует процесс индивидуального обучения инвалида; организует персональное сопровождение в образовательном пространстве. Совместно с обучающимся-инвалидом распределяет и оценивает имеющиеся ресурсы всех видов для реализации поставленных целей. Тьютор также выполняет посреднические функции между студентом-инвалидом и преподавателями с целью организации консультаций или дополнительной помощи преподавателей в освоении учебных дисциплин.

Работа педагога-психолога с инвалидами в образовательных организациях заключается в создании благоприятного психологического климата, формировании условий, стимулирующих личностный и профессиональный рост, обеспечении психологической защищённости студентов-инвалидов, поддержке и укреплении их психического здоровья.

Комплексное сопровождение образовательного процесса:

- контроль обучения инвалидов и лиц с ОВЗ в соответствии с календарным учебным графиком;
- контроль за посещаемостью занятий такими лицами;
- оказание помощи в организации самостоятельной работы в случае заболевания инвалидов и лиц с ОВЗ;
- организацию индивидуальных консультаций при длительном отсутствии студентов инвалидов и лиц с ОВЗ;
- контроль аттестаций, сдачи зачетов, экзаменов, ликвидации академических задолженностей студентов-инвалидов и лиц с ОВЗ;
- коррекция взаимодействия преподаватель – студент-инвалид в учебном процессе;
- консультирование преподавателей и сотрудников по психофизическим особенностям студентов-инвалидов, коррекция ситуаций затруднения при общении со студентами инвалидами и лицами с ОВЗ преподавателей.

7. ОЦЕНОЧНЫЕ СРЕДСТВА ДЛЯ ВХОДНОГО, ТЕКУЩЕГО КОНТРОЛЯ И ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ

Фонд оценочных средств по дисциплине обеспечивает проверку освоения планируемых результатов обучения (компетенций и их индикаторов) посредством мероприятий текущего, рубежного и промежуточного контроля по дисциплине.

Форма проведения текущей и промежуточной аттестации для обучающихся с ограниченными возможностями здоровья и инвалидов устанавливается с учетом индивидуальных психофизических особенностей (устно, письменно на бумаге, письменно на компьютере, в форме тестирования и т.п.). При необходимости обучающимся предоставляется дополнительное время для подготовки ответа.

Связь между формируемыми компетенциями и формами контроля их освоения представлена в следующей таблице:

Код	Проектируемые результаты освоения дисциплины и индикаторы формирования компетенций			Средства и технологии оценки
	Знать (З)	Уметь (У)	Владеть (В)	
ОПК-3	З-ОПК-3	У-ОПК-3	В-ОПК-3	ЛР1-2, Т1-2, Э
ПК-6.3	З-ПК-6.3	У-ПК-6.3	В-ПК-6.3	ЛР1-2, Т1-2, Э
УКЦ-2	З-УКЦ-2	У-УКЦ-2	В-УКЦ-2	ЛР1-2, Т1-2, Э

Шкала оценки за текущую аттестацию

Раздел	Форма текущего контроля	Максимальный балл	Максимальный балл за раздел
Раздел 1. Методы защиты информации.			55
Тест	Т1	15	
Лабораторные работы	ЛР1-2	20	
Раздел 2. Способы атак и технологии их обнаружения.			15
Тест	Т2	15	
Итого			70

Шкала оценки за промежуточную аттестацию (экзамен)

Критерий оценивания	**Шкала оценивания**
студент полностью раскрыл содержание теоретических вопросов, самостоятельно, без наводящих вопросов, решил предложенную задачу, объяснил и мотивировал решение задачи, смог разъяснить особенности применения теоретических знаний на практике, что может выражаться в уверенных ответах на дополнительные вопросы преподавателя.	27-30
студент раскрыл содержание теоретических вопросов, продемонстрировал знания основных понятий и определений, знание специфических для рассматриваемого раздела терминов и их понимание, что может выражаться в уверенном ответе на вопросы преподавателя, но не смог сразу разъяснить особенности применения теоретических знаний на практике.	23-26
студент раскрыл содержание вопросов с большими затруднениями, требовалась помощь преподавателями в форме наводящих вопросов, напоминания алгоритмов решения задачи,	19-22

Критерий оценивания	Шкала оценивания
студент затруднялся в объяснении решения задачи	
студент не смог раскрыть содержание теоретических вопросов, продемонстрировать знания в решении задачи, даже если преподаватель пытался помочь в форме наводящих вопросов и напоминания алгоритмов решения задачи	0-18

Шкала итоговой оценки за семестр

Итоговая оценка представляет собой сумму баллов, заработанных студентом при выполнении заданий в рамках текущего и промежуточного контроля и выставляется в соответствии с Положением о кредитно-модульной системе в соответствии со следующей шкалой:

Оценка по 4-балльной шкале	Сумма баллов	Оценка ECTS
5 – «отлично»	90-100	A
4 – «хорошо»	85-89	B
	75-84	C
	70-74	D
3 – «удовлетворительно»	65-69	
	60-64	E
2 – «неудовлетворительно»	Ниже 60	F

Расшифровка уровня знаний, соответствующего полученным баллам, дается в таблице, указанной ниже.

Сумма баллов	Оценка ECTS	Уровень приобретенных знаний по дисциплине
90-100	A	«Отлично» - теоретическое содержание курса освоено полностью, без пробелов, необходимые практические навыки работы с освоенным материалом сформированы, все предусмотренные программой обучения учебные задания выполнены, качество их выполнения оценено числом баллов, близким к максимальному.
85-89	B	«Очень хорошо» - теоретическое содержание курса освоено полностью, без пробелов, необходимые практические навыки работы с освоенным материалом в основном сформированы, все предусмотренные программой обучения учебные задания выполнены, качество выполнения большинства из них оценено числом баллов, близким к максимальному.
75-84	C	«Хорошо» - теоретическое содержание курса освоено полностью, без пробелов, некоторые практические навыки работы с освоенным материалом сформированы недостаточно, все предусмотренные программой обучения учебные задания выполнены, качество выполнения ни одного из них не оценено минимальным числом баллов, некоторые виды заданий выполнены с ошибками.
65-74	D	«Удовлетворительно» - теоретическое содержание курса освоено частично, но пробелы не носят существенного характера, необходимые практические навыки работы с освоенным материалом в основном сформированы, большинство предусмотренных программой обучения учебных заданий выполнено, некоторые из выполненных заданий, возможно, содержат ошибки.
60-64	E	«Посредственно» - теоретическое содержание курса освоено частично, некоторые практические навыки работы не сформированы, многие предусмотренные программой обучения учебные задания не выполнены, либо качество выполнения некоторых из них оценено числом баллов, близким к

Сумма баллов	Оценка ECTS	Уровень приобретенных знаний по дисциплине
		минимальному.
Ниже 60	F	«Неудовлетворительно» - очень слабые знания, недостаточные для понимания курса, имеется большое количество основных ошибок и недочетов.

Студент считается аттестованным по разделу, экзамену, если он набрал не менее 60% от максимального балла, предусмотренного рабочей программой.

Контрольные мероприятия, за которые студент получил 0 баллов (неявка в установленный срок), подлежат обязательной пересдаче. Сроки пересдач контрольных мероприятий в течение семестра определяет кафедра.

Вопросы к экзамену по дисциплине
«Защита информации»

1. Информация как объект защиты.
2. Актуальность и основные принципы защиты информации в информационных системах (ИС).
3. Направления защиты информации в ИС.
4. Методы и технологии защиты информации в ИС.
5. Методы и технологии защиты конфиденциальности информации.
6. Методы и технологии защиты целостности информации.
7. Методы и технологии защиты доступности информации.
8. Определение информационной безопасности.
9. Важнейшие аспекты информационной безопасности.
10. Основные угрозы информационной безопасности. Обеспечение информационной безопасности
11. Аппаратно-программные средства защиты информации.
12. Системы идентификации и аутентификации пользователей.
13. Системы шифрования дисковых данных.
14. Системы шифрования данных, передаваемых по сетям.
15. Системы аутентификации электронных данных.
16. Средства управления криптографическими ключами.
17. Перечень основных нормативных документов.
18. Политика безопасности.
19. Пассивные компоненты защиты.
20. Понятия вычислительная база и монитор обращений.
21. Основные элементы политики безопасности.
22. Архитектура системы компьютерной безопасности.
23. Произвольное управление доступом.
24. Безопасность повторного использования объектов.
25. Метки безопасности.
26. Принудительное управление доступом.
27. Классы безопасности.
28. Требования к политике безопасности.
29. Требования к подотчетности и документации.
30. Основные требования к криптографическому закрытию информации в автоматизированных системах.
31. Классификация основных методов криптографического закрытия информации.
32. Виды кодирования и шифрования.
33. Шифрование методом подстановки. Шифрование методом перестановки.

34. Шифрование методом гаммирования. Шифрование с помощью аналитических преобразований. Комбинированные методы шифрования.
35. Организационные проблемы криптозащиты.
36. Простые криптосистемы.
37. Алгоритмы шифрования данных DES, AES, RSA, ГОСТ 28147-89.
38. Проблема аутентификации данных и электронная цифровая подпись. Однонаправленные хеш-функции.
39. Основы построения хеш-функций. Однонаправленные хеш-функции на основе симметричных блочных алгоритмов.
40. Алгоритм MD5.
41. Алгоритм безопасного хеширования SHA.
42. Отечественный стандарт хэш-функции ГОСТ Р 34.11-9. Алгоритмы электронной цифровой подписи.
43. Алгоритм цифровой подписи RSA.
44. Алгоритм цифровой подписи Эль Гамаля (EGSA).
45. Алгоритм цифровой подписи DSA.
46. Отечественный стандарт цифровой подписи ГОСТ Р 34.10-94.
47. Классификация систем защиты копирования информационных носителей.
48. Механизм контроля и привязки ключа.
49. Метод привязки к диску.
50. Метод перестановки нумерации секторов.
51. Метод введения одинаковых номеров секторов на дорожке. Метод введение межсекторных связей.
52. Метод изменение длины секторов и межсекторных промежутков. Метод ведение логических дефектов в заданный сектор.
53. Изменение параметров считывающего устройства, приемника информации. Технология "ослабленных" битов.
54. Применение физического защитного устройства. Конфигурация системы и типы составляющих ее устройств.
55. Получение инженерной информации жесткого диска. Физические дефекты винчестера. Опрос справочников.
56. Метод введение ограничений на использование программного обеспечения.
57. Идентификация и аутентификация пользователя. Взаимная проверка подлинности пользователей.
58. Протоколы идентификации с нулевой передачей знаний. Упрощенная и параллельная схемы идентификации с нулевой передачей знаний.
59. Схема идентификации Гиллоу – Куискуотера.
60. Определение и классификация вирусов.
61. Троянский конь. Логическая бомба.
62. Программы с не декларированными возможностями (НДВ). Программные закладки
63. Классификация моделей компьютерных атак. Этапы реализации атак. Средства обнаружения компьютерных атак
64. Классификация систем обнаружения атак. Межсетевые экраны. Пакетные фильтры.
65. Сервера прикладного уровня
66. Сравнительные характеристики пакетных фильтров и серверов прикладного уровня. Администрирование и системы сбора статистики и предупреждения об атаке.
67. Безопасность электронной коммерции.
68. Классификация технических каналов утечки информации. Понятие информационного сигнала.

69. Модуляция сигналов. Основные показатели технического канала утечки информации. Технические каналы утечки акустической информации.
70. Зашумление. Основные требования и рекомендации по защите речевой информации.
71. Побочные электромагнитные излучения и наводки, природа их возникновения и виды.
72. Средства перехвата радиосигналов. Специальные проверки.

8. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ УЧЕБНОЙ ДИСЦИПЛИНЫ

Основная литература

1. Башлы, П. Н. Информационная безопасность и защита информации: учебное пособие / П. Н. Башлы, А. В. Бабаш, Е. К. Баранова. — Москва: Евразийский открытый институт, 2012. — 311 c. — ISBN 978-5-374-00301-7. — Текст: электронный // Цифровой образовательный ресурс IPR SMART: [сайт]. — URL: https://www.iprbookshop.ru/10677.html (дата обращения: 10.03.2024). — Режим доступа: для авторизир. пользователей.

Дополнительная литература

1. Бескид, П. П. Криптографические методы защиты информации. Часть 1. Основы криптографии: учебное пособие / П. П. Бескид, Т. М. Тагарникова. — Санкт-Петербург: Российский государственный гидрометеорологический университет, 2010. — 95 c. — Текст: электронный // Цифровой образовательный ресурс IPR SMART: [сайт]. — URL: https://www.iprbookshop.ru/17925.html (дата обращения: 10.03.2024). — Режим доступа: для авторизир. пользователей.

2. Бескид, П. П. Криптографические методы защиты информации. Часть 2. Алгоритмы, методы и средства обеспечения конфиденциальности, подлинности и целостности информации: учебное пособие / П. П. Бескид, Т. М. Тагарникова. — Санкт-Петербург: Российский государственный гидрометеорологический университет, 2010. — 104 c. — Текст: электронный // Цифровой образовательный ресурс IPR SMART: [сайт]. — URL: https://www.iprbookshop.ru/17926.html (дата обращения: 10.03.2024). — Режим доступа: для авторизир. пользователей.

3. Бурняшов, Б. А. Меры защиты информации на уровне пользователя информационно-технологическими средствами: методические указания к самостоятельной работе студентов. Учебно-методическое пособие / Б. А. Бурняшов. — Саратов: Вузовское образование, 2014. — 55 c. — Текст: электронный // Цифровой образовательный ресурс IPR SMART: [сайт]. — URL: https://www.iprbookshop.ru/23077.html (дата обращения: 10.03.2024). — Режим доступа: для авторизир. пользователей.

Программное обеспечение:

1. Mozilla Thunderburd;
2. Hyper-V.

LMS и Интернет-ресурсы:

1. Образовательный портал НИЯУ МИФИ URL: https://online.mephi.ru/.
2. Онлайн курс НИЯУ МИФИ «Введение в современную криптографию» на платформе «Открытое образование» URL: https://openedu.ru/.

3. Центр информационно-библиотечного обеспечения учебно-научной деятельности НИЯУ МИФИ URL: http://library.mephi.ru/.
4. Электронная информационно-образовательная среда ТИ НИЯУ МИФИ URL: http://stud.mephi3.ru/.
5. Электронно-библиотечная система IPR SMART URL: https://www.iprbookshop.ru/.

9. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ УЧЕБНОЙ ДИСЦИПЛИНЫ

Аудитория для проведения занятий лекционного типа, занятий семинарского типа, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации, для самостоятельной работы:
проектор Nec + экран (настенный), компьютер: процессор IntelPentium 4; оперативная память 4GBDDR3; монитор ЖК Benq 19,5”, клавиатура, мышь, Adobe Reader

Для проведения лабораторных работ необходима компьютерная лаборатория, оснащенная рабочими местами для каждого студента, а также рабочим местом преподавателя. Рабочее место оснащено компьютером: процессор IntelPentium 4; оперативная память 4GBDDR3; монитор ЖК Benq 19,5”, клавиатура, мышь.

Каждый студент имеет свой логин и пароль для входа в Электронную информационно-образовательную среду ТИ НИЯУ МИФИ (http://stud.mephi3.ru/).

Каждый студент имеет доступ к электронно-библиотечной системе IPR SMART.

Программа составлена в соответствии с требованиями ОС ВО НИЯУ МИФИ по направлению подготовки 09.03.01 «Информатика и вычислительная техника».

Автор: старший преподаватель кафедры «Информационных технологий и прикладной математики» К.В. Кревский.