МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«Национальный исследовательский ядерный университет «МИФИ»
Обнинский институт атомной энергетики –
филиал федерального государственного автономного образовательного учреждения высшего образования
«Национальный исследовательский ядерный университет «МИФИ»
(ИАТЭ НИЯУ МИФИ)

ОТДЕЛЕНИЕ ИНТЕЛЛЕКТУАЛЬНЫХ КИБЕРНЕТИЧЕСКИХ СИСТЕМ

Одобрено на заседании Ученого
совета ИАТЭ НИЯУ МИФИ,
протокол №25.8 от 25.08.2025

РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ И ЗАЩИТА ИНФОРМАЦИИ

название дисциплины

для студентов направления подготовки

Направление подготовки: 38.03.05 Бизнес-информатика

профиль:
Цифровая трансформация компании

Форма обучения: очная

г. Обнинск 2025 г.

1. Цели и задачи освоения дисциплины

Целью преподавания дисциплины «Информационная безопасность и защита информации» является ознакомление студентов с источниками, рисками и формами атак на информацию, автоматизированные и информационные системы, с организационными, техническими, программными и криптографическими методами и средствами защиты информации, циркулирующей в автоматизированных и информационных системах, с законодательством и стандартами в этой области, с современными методами идентификации и алгоритмами аутентификации пользователей, борьбы с вирусами, способами применения методов и средств защиты информации при проектировании и эксплуатации информационных систем для бизнеса, правилами построения политики информационной безопасности, программой информационной безопасности Российской Федерации и путях ее реализации.

2. Место дисциплины в структуре образовательной программы (далее – ОП) бакалавриата

Дисциплина реализуется в рамках обязательной части профессионального модуля.

Для освоения дисциплины необходимы компетенции, сформированные в рамках изучения следующих дисциплин: Операционные системы, Базы данных.

Дисциплины и/или практики, для которых освоение данной дисциплины необходимо как предшествующее: Производственная практика (преддипломная практика).

Дисциплина изучается на 4 курсе в 7 семестре.

3.Перечень планируемых результатов обучения по дисциплине, соотнесенных с планируемыми результатами освоения образовательной программы

В результате освоения ООП бакалавриата обучающийся должен овладеть следующими результатами обучения по дисциплине:

Коды компетенций	**Результаты освоения ООП** ***Содержание компетенций***	**Перечень планируемых результатов обучения по дисциплине**
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	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
ОПК-2	Способен проводить исследование и анализ рынка информационных систем и информационно-коммуникационных технологий, выбирать рациональные решения для управления бизнесом	З-ОПК-2 Знать: Инструменты и методы оценки качества и эффективности ИС Инструменты и методы оптимизации ИС Возможности ИС Предметная область автоматизации Архитектура, устройство и функционирование вычислительных систем Сетевые протоколы Основы современных операционных систем Основы современных систем управления базами данных Теория баз данных Системы хранения и анализа баз данных Современные стандарты информационного взаимодействия систем Программные средства и платформы инфраструктуры информационных технологий организаций Основы информационной безопасности организации Источники информации, необходимой для профессиональной деятельности Современный отечественный и зарубежный опыт в профессиональной деятельности. У-ОПК-2 Уметь: Разрабатывать метрики (количественные показатели) работы ИС Анализировать исходные данные. В-ОПК-2 Владеть навыками: Количественное определение существующих параметров работы ИС Определение параметров, которые должны быть улучшены Определение новых целевых показателей работы ИС Осуществление оптимизации ИС для достижения новых целевых показателей.

4. Воспитательный потенциал дисциплины

Направления / цели воспитания	Задачи воспитания (код)	Воспитательный потенциал дисциплин
Профессиональное воспитание	Формирование культуры информационной безопасности (В-23)	Использование воспитательного потенциала дисциплины «Информационная безопасность и защита информации» для формирования 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.
Профессиональное воспитание	- формирование ориентации на неукоснительное соблюдение нравственных и правовых норм в соответствии с корпоративной этикой (В37)	Использование воспитательного потенциала дисциплины «Информационная безопасность и защита информации» для формирования профессиональных установок системного анализа через содержание дисциплин и практик, акцентирование учебных заданий, групповое решение модельных и практических задач, кейсов, подготовку учебных проектов, эссе и рефератов, прохождение практик на конкретных рабочих местах.

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

1. Организация научно-практических конференций, круглых столов, встреч с выдающимися учеными и ведущими специалистами отраслей.

2. Организация и проведение предметных олимпиад и конкурсов профессионального мастерства.

5. Объем дисциплины в зачетных единицах с указанием количества академических часов, выделенных на контактную работу обучающихся с преподавателем (по видам занятий) и на самостоятельную работу обучающихся

Общая трудоемкость (объем) дисциплины составляет 2 зачетных единиц (з.е.), 72 академических часа.

5.1. Объём дисциплины по видам учебных занятий (в часах)

Объем дисциплины	Всего часов
	Очная форма обучения
Общая трудоемкость дисциплины	72
Контактная работа обучающихся с преподавателем (по видам учебных занятий) (всего)	48
Аудиторная работа (всего):	48
Лекции	*16*
семинары, практические занятия	*16*
лабораторные работы	*16*
Внеаудиторная работа (всего):	24

индивидуальная работа обучающихся с преподавателем:	
курсовое проектирование	
групповая, индивидуальная консультация и иные виды учебной деятельности, предусматривающие групповую или индивидуальную работу обучающихся с преподавателем*)*	
творческая работа (эссе)	
Самостоятельная работа обучающихся(всего)	24
Вид промежуточной аттестации обучающегося (зачет/экзамен(часы))	Зачет

6. Содержание дисциплины, структурированное по темам (разделам) с указанием отведенного на них количества академических часов и видов учебных занятий

6.1. Разделы дисциплины и трудоемкость по видам учебных занятий (в акад.часах)

№ п/п	**Наименование раздела /темы дисциплины**	**Общая трудоёмкость всего** *(в часах)*	**Виды учебных занятий, включая самостоятельную работу обучающихся и трудоемкость** *(в часах)*			
			Аудиторные учебные занятия*			**СРО**
			Лек	**Сем/Пр**	**Лаб**	
1.1.	Введение в информационную безопасность	1	1			
1.2.	Законодательный уровень защиты информации.	4	2			2
1.3.	Административный уровень информационной безопасности.	4	2			2
1.4.	Криптографические методы защиты информации	14	2	4	4	4
1.5.	Идентификация, аутентификация, управление доступом.	14	2	4	4	4
1.2.	Безопасность вычислительных сетей	14	2	4	4	4
1.6	Безопасность баз данных.	6	2			4
1.7	Безопасность операционных систем	15	3	4	4	4

*Прим.: Лек – лекции, Сем/Пр – семинары, практические занятия, Лаб – лабораторные занятия, СРО – самостоятельная работа обучающихся

6.2. Содержание дисциплины, структурированное по разделам (темам)

6.2.1. Лекционный курс

№	**Наименование раздела /темы дисциплины**	**Содержание**
1.1.	**Введение в информационную безопасность**	Основные понятия и определения. Понятие информационной безопасности. Свойства информации как объекта защиты: доступность, целостность, конфиденциальность. Угроза информационной безопасности, виды угроз, классификация угроз. Мероприятия по обеспечению информационной безопасности.
1.2.	**Законодательный уровень защиты**	Основные законодательные акты РФ по защите информации. Законы «О государственной тайне», «Об информатике,

	информации.	информатизации и защите информации», «О лицензировании отдельных видов деятельности», «О персональных данных». Стандарты информационной безопасности. Руководящие документы Гостехкомиссии РФ.
1.3.	**Административный уровень информационной безопасности.**	Политика безопасности. Оценка и управление рискам в области ИБ. Физическая защита. Управление персоналом. Поддержание работоспособности. Планирование восстановительных работ.
1.4.	**Криптографические методы защиты информации**	Введение в криптографию. Основные понятия криптографии. Виды систем шифрования и области применения криптографических алгоритмов. Свойства шифров, примеры простых систем шифрования. Симметричные алгоритмы шифрования, сети Фейстеля, алгоритмы Blowfish, IDEA, ГОСТ 28147-89. Система AES. Ассиметричное шифрование. Система Диффи-Хеллмана, шифр Эль Гамаля, шифр RSA. Криптографические хеш-функции. Цифровая подпись. Стандарты цифровой подписи. Открытое распределение колючей.
1.5.	**Идентификация, аутентификация, управление доступом.**	Основные понятия. Методы аутентификации. Многоразовые пароли, атаки на пароли, требования к паролям и парольным системам. Одноразовые пароли, алгоритмы формирования одноразовых паролей. Строгая аутентификация. Система аутентификации Cerberos. Аутентификация с использованием технических средств: магнитные карты, смарт-карты, USB-ключи. Биометрическая аутентификация. Задача управления доступом. Дискреционное управление доступом. Изолированная программная среда. Полномочное управление доступом. Управление доступом в Java среде..
1.2.	**Безопасность вычислительных сетей**	Безопасность ресурсов сети: средства идентификации и аутентификации, методы разделения ресурсов и технологии разграничения доступа. Интеграция локальных вычислительных сетей в глобальные. Основные механизмы обеспечения безопасности и управления распределенными ресурсами. Протоколы аутентификации Kerberos, SSL, TLS. Технология PKI (Public Key Infrastructure) – интегрированный набор служб и средств администрирования для создания и развертывания приложений, применяющих шифрование с открытым ключом, а также для управления ими. Многоуровневая защита корпоративных сетей. Виртуальные частные сети, варианты построения и продукты реализации. Режим функционирования межсетевых экранов и их основные компоненты. Основные схемы сетевой защиты на базе межсетевых экранов. Системы адаптивного анализа защищенности. Задачи и программно-аппаратные средства администратора безопасности сети..
1.6	**Безопасность баз данных.**	Особенности БД как объектов защиты информации. Обеспечение конфиденциальности. Избирательная защита. Пользователи, привилегии, роли. Мандатная защита. Метки безопасности. Избирательные механизмы защиты в СУБД Oracle. Обеспечение доступности. Резервное копирование и восстановление. Аудит. SQL инъекции
1.7	**Безопасность операционных систем**	Общая характеристика операционных систем. Назначение, возможности, модели безопасности операционных систем

		группы Windows, UNIX. Организация управления доступом и защиты ресурсов ОС. Основные механизмы безопасности: средства и методы аутентификации в ОС, модели разграничения доступа, организация и использование средств аудита. Администрирование ОС: задачи и принципы сопровождения системного программного обеспечения, генерация, настройка, измерение производительности и модификация систем, управление безопасностью ОС

6.2.3. Лабораторные занятия

№	Наименование раздела /темы дисциплины	Название лабораторной работы
1.1.	Введение в информационную безопасность	Обеспечение доступности информации средствами ОС Windows
1.4.	Криптографические методы защиты информации	Шифрующие файловые системы
1.4.	Криптографические методы защиты информации	Использование пакета PGP
1.5.	Идентификация, аутентификация, управление доступом.	Развертывание инфраструктуры Windows.
1.5.	Идентификация, аутентификация, управление доступом.	Управление доступом в ОС Windows
1.7	Безопасность операционных систем	
1.2.	Безопасность вычислительных сетей	Использование межсетевых экранов

7. Перечень учебно-методического обеспечения для самостоятельной работы обучающихся по дисциплине

Студентами самостоятельно в рамках подготовки к лабораторным работам изучаются следующие вопросы:

- обеспечение конфиденциальности, целостности и доступности информации в соответствии с требованиями международных и отечественных стандартов информационной безопасности;

- задачи и принципы сопровождения системного программного обеспечения, управление безопасностью ОС;

- средства языка SQL для организации разграничения доступа, концепция и реализация механизма ролей, использование представлений, организация аудита системных событий и действий пользователя в системах баз данных;

- реализация симметричных и асимметричных криптоалгоритмов в программно-аппаратных разработках российских производителей;

Контроль освоения материала осуществляется в ходе приема лабораторных работ. Используемая литература, приведенная в разделе 8. По умолчанию предполагается литература из п.п. 8.2 (дополнительная). В отдельных необходимых случаях после номера источника в круглых скобках указывается п.п. 8.1 (основная литература).

Содержание самостоятельной работы	Форма контроля
Обеспечение конфиденциальности, целостности и доступности информации в соответствии с требованиями международных и отечественных стандартов информационной безопасности	Собеседование перед сдачей соответствующей лабораторной работы
Задачи и принципы сопровождения системного программного обеспечения, управление безопасностью ОС	
Средства языка SQL для организации разграничения доступа, концепция и реализация механизма ролей, использование представлений, организация аудита системных событий и действий пользователя в системах баз данных	
Реализация симметричных и асимметричных криптоалгоритмов в программно-аппаратных разработках российских производителей	
Этапы проектирования комплексной системы информационной безопасности и требования к ним	

8. Фонд оценочных средств для проведения промежуточной аттестации обучающихся по дисциплине

8.1. Паспорт фонда оценочных средств по дисциплине

Вид контроля	Этап рейтинговой системы Оценочное средство	Балл	
		Минимум	Максимум
Текущий	**Контрольная точка № 1**		
	Контрольная № 1	5	15
	Контрольная точка № 2		
	Контрольная № 2	5	15
	Лабораторные работы	30	30
Промежуточный	**Зачет**		
	Вопросы на зачете	20	40
ИТОГО по дисциплине		60	100

8.2. Типовые контрольные задания или иные материалы

8.2.1. Зачет

Оценка "отлично" выставляется за полный ответ на все поставленные вопросы. Ответы должны иллюстрироваться примерами в виде схем и фрагментов программ на ассемблере или языке высокого уровня.:

Оценка "хорошо" выставляется за неполный или частичный ответ на большинство поставленных вопросов.

Оценка "удовлетворительно" ставится за владение понятиями и определениями в объеме курса.

Типовые вопросы на зачете

1. Дайте характеристику симметричных криптосистем. На каких принципах они основаны?
2. Перечислите основные уязвимости IP сетей.
3. Что дает злоумышленнику сборка мусора?
4. Каким образом можно использовать триггеры для обеспечения аудита БД?

5. Чем характеризуется избирательное управление доступом к информации.
6. Что такое «хеш-функция»? Зачем необходимо ее использовать? Приведите примеры хэш-функций.
7. Каким образом можно использовать представления для ограничения доступности информации в БД?
8. На каких принципах основано действие программ-архиваторов? Приведите пример.
9. Чем характеризуется полномочная (мандатная) политика безопасности.
10. Какие свойства сообщений используются в криптоанализе?
11. Для чего нужна и что представляет собой матрица доступа?
12. Поясните понятия «привилегия», «роль» в БД.
13. Что такое «объектная привилегия». Как они предоставляются?
14. Сформулируйте основные требования к паролям.
15. Что такое «системная привилегия». Для чего необходимы системные привилегии?
16. Для чего нужен и как организуется аудит?
17. Перечислите основные методы подбора паролей.
18. Перечислите и охарактеризуйте основные функции подсистемы защиты ОС.
19. Дайте характеристику асимметричных криптосистем. На каких принципах они основаны?
20. В чем различие фрагментарного и комплексного подхода к созданию защищенных систем?
21. Опишите свойства информации как объекта защиты.
22. Опишите алгоритм шифрования DES.
23. Перечислите основные причины возникновения угроз в сетях.
24. Сформулируйте основные функции ОС.
25. Основные свойства информации: целостность, конфиденциальность, доступность.
26. Перечислите типичные атаки на операционные системы.
27. Сформулируйте основные требования к шифрам. Какой шифр называется устойчивым?
28. Какими средствами реализуется целостность информации в базе данных?
29. Опишите основные группы методов защиты информации.
30. Что такое режим работы криптографического алгоритма? Перечислите основные режимы.
31. Перечислите угрозы, характерные для СУБД.
32. Понятие о политике безопасности. Как реализуется политика безопасности? Что предусматривает адекватная политика безопасности?
33. Что такое «потоковое шифрование»? Можно ли блочный шифр использовать как потоковый, если да, то в каком режиме?
34. Опишите следующие понятия: «идентификация», «авторизация», «аутентификация».
35. Что такое доступность базы данных?
36. Что такое цифровая подпись? Принципы построения цифровой подписи.

8.2.2. Вопросы к контрольной работе по защите ОС и БД

Вариант 1

1. Для чего применяются и как организованы идентификация, аутентификация и авторизация СД?
2. Что такое триггер? Каким образом можно использовать триггеры для обеспечения аудита БД?
3. Что такое «системная привилегия». Для чего необходимы системные привилегии?
4. Какие виды атак можно реализовать с помощью SQL-инъекций?

Вариант 2

1. Для чего нужна и что представляет собой матрица доступа?

2. Поясните понятие «привилегия» в БД. Предоставление и отзыв привилегий.
3. Для чего нужен и как организуется аудит?
4. Способы противодействия SQL- инъекциям.

Вариант 3

1. Сформулируйте основные требования к паролям.
2. Перечислите недостатки средств защиты информации в SQL.
3. Какими средствами реализуется целостность информации в базе данных?
4. Каким образом осуществляется идентификация пользователей в СУБД Interbase?

Вариант 4

1. Перечислите основные методы подбора паролей.
2. Перечислите особенности БД и СУБД, как объекта защиты информации.
3. Поясните понятие «роль» в БД. В чем состоит гибкость ролей? Создание ролей.
4. Что такое доступность базы данных? Каким образом можно обеспечить доступность БД?

Вариант 5

1. Для чего применяются и как организованы идентификация, аутентификация и авторизация СД?
2. Перечислите угрозы, характерные для СУБД.
3. Что такое «объектная привилегия». Как они предоставляются?
4. В чем, по-вашему, недостатки систем, обеспечивающих защиту БД на уровне приложений?

Вариант 6

1. Для чего нужна и что представляет собой матрица доступа?
2. Что такое представление? Как их использовать для ограничения доступности информации в БД?
3. Основные группы пользователей БД.
4. Что такое SQL-инъекции, каковы условия для их реализации?

Вариант 7

1. В чем, по-вашему может состоять атака «сборка мусора?» в ИС. Что дает злоумышленнику такая атака?
2. Что такое триггер? Каким образом можно использовать триггеры для обеспечения аудита БД?
3. Что такое «системная привилегия». Для чего необходимы системные привилегии?
4. Какие виды атак можно реализовать с помощью SQL-инъекций?

Вариант 8

1. Охарактеризуйте избирательное и полномочное разграничение доступа.
2. Для чего нужен и как организуется аудит?
3. Поясните понятие «привилегия» в БД. Предоставление и отзыв привилегий.
4. Способы противодействия SQL- инъекциям.

Вариант 9

1. Для чего применяются и как организованы идентификация, аутентификация и авторизация СД?
2. Перечислите недостатки средств защиты информации в SQL.
3. Какими средствами реализуется целостность информации в базе данных?
4. Каким образом осуществляется идентификация пользователей в СУБД Interbase?

Вариант 10

1. Для чего нужна и что представляет собой матрица доступа?
2. Перечислите особенности БД и СУБД, как объекта защиты информации.
3. Поясните понятие «роль» в БД. В чем состоит гибкость ролей? Создание ролей.
4. Что такое доступность базы данных? Каким образом можно обеспечить доступность БД?

Вариант 11

1. Сформулируйте основные требования к паролям.
2. Для чего и какими способами осуществляется разграничение доступа к объектам ОС?
3. Перечислите угрозы, характерные для СУБД.
4. Что такое «объектная привилегия». Как они предоставляются?

Вариант 12

1. Приведите пример классификации угроз безопасности информационным системам системам.
2. Для чего и какими способами осуществляется разграничение доступа к объектам ОС?
3. Что дает злоумышленнику сборка мусора?
4. В чем, по-вашему, недостатки систем, обеспечивающих защиту БД на уровне приложений?

Вариант 13

1. Какие факторы могут повлиять на доступность БД. Перечислите основные подходы к обеспечению доступности.
2. Каким образом реализуется хранение матрицы доступа в базах данных.
3. Приведите описание возможной схемы двухсторонней строгой аутентификации с участием третьей, доверенной стороны.
4. Какие возможны подходы к идентификации и аутентификации пользователей БД. В чем, по-вашему, состоят преимущества и недостатки этих подходов.

8.3. Методические материалы, определяющие процедуры оценивания знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций

Экзамен (100 баллов)	Лабораторные работы	30
	Контрольная работа № 1	15
	Контрольная работа № 2	15
	Ответы на экзаменационный билет	40

9. Перечень учебной литературы, необходимой для освоения дисциплины

1. Нестеров, С. А. Основы информационной безопасности / С. А. Нестеров. — 3-е изд., стер. — Санкт-Петербург : Лань, 2024. — 324 с. — ISBN 978-5-507-49077-6. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/370967
2. Организационное и правовое обеспечение информационной безопасности : учебник для вузов / Т. А. Полякова, А. А. Стрельцов, С. Г. Чубукова, В. А. Ниесов ; под редакцией Т. А. Поляковой, А. А. Стрельцова. — 2-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2025. — 357 с. — (Высшее образование). — ISBN 978-5-534-19108-0. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/560516

3. Щеглов, А. Ю. Защита информации: основы теории : учебник для вузов / А. Ю. Щеглов, К. А. Щеглов. — Москва : Издательство Юрайт, 2025. — 349 с. — (Высшее образование). — ISBN 978-5-534-19762-4. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/561077

10. Методические указания для обучающихся по освоению дисциплины

Вид учебного занятия	Организация деятельности студента
Лекция	Написание конспекта лекций: кратко, схематично, последовательно фиксировать основные положения, выводы, формулировки, обобщения; помечать важные мысли, выделять ключевые слова, термины. Проверка терминов, понятий с помощью энциклопедий, словарей, справочников с выписыванием толкований в тетрадь. Обозначить вопросы, термины, материал, который вызывает трудности, пометить и попытаться найти ответ в рекомендуемой литературе. Если самостоятельно не удается разобраться в материале, необходимо сформулировать вопрос и задать преподавателю на консультации, на практическом занятии и лабораторной работе. Уделить внимание следующим понятиям: данные, представление, атака, целостность, конфиденциальность, доступность
Практические занятия	Проработка рабочей программы, уделяя особое внимание целям и задачам, структуре и содержанию дисциплины. Работа с конспектом лекций, просмотр рекомендуемой литературы.
Контрольная работа	Ознакомиться с основной и дополнительной литературой, включая справочные издания, зарубежные источники, основополагающие термины. Попрактиковаться в решении задач
Лабораторная работа	При выполнении лабораторных работ необходимо ориентироваться на конспекты лекций, рекомендуемую литературу и др.

11. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине, включая перечень программного обеспечения и информационных справочных систем (при необходимости)

11.1. Перечень информационных технологий

Программные продукты: операционные системы Windows XP, Windows 2010 Pro, СУБД Oracle 9, система защиты информации от несанкционированного доступа «Secret Net», программный пакет PGP, почтовая программа The Bat!, межсетевой экран Outpost Firewall, сетевые сканеры: NMap, XSpider, GFI LANGuard Network Security Scanner, Microsoft Baseline Security Analyzer, сетевой монитор системы обнаружения атак Snort, антивирусный пакет Dr. Web – сканер для Windows.

11.2. Перечень программного обеспечения

- Microsoft Windows 10 Pro для образовательных учреждений, договор №1322эа от 27.10.2020.
- Microsoft Office 2010 Professional Plus для образовательных учреждений, договор №1322эа от 27.10.2020.
- Kaspersky Endpoint Security для образовательных учреждений, договор №1322эа от 27.10.2020.

11.3. Перечень информационных справочных систем

Доступ к электронным библиотечным ресурсам и электронной библиотечной системе (ЭБС) осуществляется посредством специальных разделов на официальном сайте ИАТЭ НИЯУ МИФИ. Обеспечен доступ к электронным каталогам библиотеки ИАТЭ НИЯУ МИФИ, а также

электронным образовательным ресурсам (ЭИОС), сформированным на основании прямых договоров с правообладателями учебной и учебно-методической литературы, методических пособий:

1. ЭБС «Айбукс», Договор № 05-25-910 от 2.06.2025 на оказание услуг по предоставлению доступа к электронно-библиотечной системе «Айбукс.ру/ibooks.ru». Срок действия: 1.09.2025г. по 31.08.2026г.
2. ЭБС «ЛАНЬ», Договор № 08-25-910 от 30.05.2025 на оказание услуг по предоставлению доступа к базе данных ЭБС «Лань». Срок действия: с 1.09.2025г. по 31.08.2026г.
3. ЭБС «ЮРАЙТ», Договор № 09-25-910 от 3.06.2025 на оказание услуг по предоставлению доступа к «Образовательной платформе ЮРАЙТ». Срок действия: с 1.09.2025г. по 31.08.2026г.
4. ЭБС «Консультант студента», Договор № 06-25-910 от 3.06.2025 на оказание услуг по предоставлению доступа к комплектам «Медицина, Здравоохранение», «Книги издательства «Феникс», «Издательский дом МЭИ», «Книги издательства «Проспект»: «Иностранные языки», «Естественные науки», «Экономика и управление», «Гуманитарные науки», «Юридические науки», входящим в базу данных «Электронная библиотека технического вуза». (ЭБС «Консультант студента»). Срок действия: 1.09.2025г. по 31.08.2026г.
5. Научная электронная библиотека E-library.ru, Договор № SU-353/2025 от 2.11.2024 на доступ к электронным изданиям в составе базы данных «НАУЧНАЯ ЭЛЕКТРОННАЯ БИБЛИОТЕКА eLIBRARY.RU». Срок действия: с 1.01.2025г. по 31.12.2025г.

12. Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине

Сетевой компьютерный класс. Для проведения лабораторных занятий используется система виртуальных машин Virtual PC компании Oracle. Использование виртуальных машин позволяет моделировать в рамках одного физического компьютера несколько лабораторных установок, оснащенных различными ОС и связанных в различные сетевые конфигурации

13. Перечень образовательных технологий, используемых при осуществлении образовательного процесса по дисциплине

Студенты самостоятельно изучают литературу и техническую документацию, для получения знаний, необходимых для выполнения лабораторных работ. Самостоятельно осваивают принципы использования применяемых программных средств. Самостоятельно выполняют тестирование и отладку программ. Самостоятельно осваивают ряд вопросов из раздела "Современные микропроцессоры"

Программу составил:

А.В. Пляскин, доцент ОИКС, к.т.н., -