

Министерство науки и высшего образования Российской Федерации  
Нижекамский химико-технологический институт (филиал)  
федерального государственного бюджетного образовательного учреждения  
высшего образования  
«Казанский национальный исследовательский технологический университет»  
(НХТИ ФГБОУ ВО «КНИТУ»)



УТВЕРЖДАЮ

Заместитель директора по УР

Н.И. Никифорова

2022 г.

## РАБОЧАЯ ПРОГРАММА

По дисциплине Б1.О.23 Защита информации  
Направление подготовки 09.03.01 «Информатика и вычислительная техника»  
Профиль/программа Автоматизированные системы обработки информации и управления  
Квалификация (степень) выпускника бакалавр  
Форма обучения очная, очно-заочная  
Факультет Информационных технологий  
Кафедра-разработчик рабочей программы информационных систем и технологий  
Очная форма обучения: курс - 4, семестр – 7

	Часы	Зачетные единицы
Лекции	18	0,5
Практические занятия	-	-
Лабораторные занятия	36	1
Контроль самостоятельной работы	54	1,5
Самостоятельная работа	81	2,25
Форма аттестации (часы на контроль)	Экзамен (27)	0,75
Всего	216	6

Очно-заочная форма обучения: курс - 4, семестр – 8

	Часы	Зачетные единицы
Лекции	18	0,5
Практические занятия	-	-
Лабораторные занятия	18	0,5
Контроль самостоятельной работы	63	1,75
Самостоятельная работа	90	2,5
Форма аттестации (часы на контроль)	Экзамен (27)	0,75
Всего	216	6

Нижнекамск, 2022 г.

Рабочая программа составлена с учетом требований Федерального государственного образовательного стандарта высшего образования ( № 929 от 19.09.2017) по направлению 09.03.01 «Информатика и вычислительная техника» на основании учебного плана набора обучающихся 2022.

Разработчик программы:

Ст.преподаватель  
(должность)

  
(подпись)

Захарова И.Н.  
(Ф.И.О)

Рабочая программа рассмотрена и одобрена на заседании кафедры ИСТ, протокол от 20.04.2022 № 8

Зав. кафедрой

  
(подпись)

Матухина О.В.  
(Ф.И.О.)

### ***1. Цели освоения дисциплины***

Целями освоения дисциплины Б1.О.23 «Защита информации» являются

- а) формирование знаний о методах, средствах защиты программ и данных от различных типов угроз;
- б) обучение технологии получения анализа состояния защищенности информации, выбора, построения и анализа показателей защищенности программно-аппаратных средств защиты информации;
- в) обучение применению программных и аппаратных средств защиты информации;
- г) раскрытие сущности теории защиты информации.

### ***2. Место дисциплины (модуля) в структуре основной образовательной программы***

Дисциплина Б1.О.23 «Защита информации» относится к обязательной части ООП и формирует у бакалавров по направлению подготовки 09.03.01 «Информатика и вычислительная техника» набор знаний, умений, навыков и компетенций.

Для успешного освоения дисциплины Б1.О.23 «Защита информации» бакалавр по направлению подготовки 09.03.01 «Информатика и вычислительная техника» должен освоить материал предшествующих дисциплин:

- а) Б1.О.16 Информационные технологии (информатика);
- б) Б1.О.25 Сети и телекоммуникации;
- в) Б1.О.26 Программирование на языке высокого уровня;
- г) Б1.В.05 Системное программное обеспечение;
- д) Б1.В.17 Базы данных;
- е) Б1.В.ДВ.04.01 Автоматизация финансово-хозяйственной деятельности организаций и предприятий;
- ж) Б1.В.ДВ.04.02 Программирование 1С.

Знания, полученные при изучении дисциплины, Б1.О.23 «Защита информации» могут быть использованы при прохождении практик и выполнении выпускной квалификационной работы.

### ***3. Компетенции и индикаторы достижения компетенции обучающегося, формируемые в результате освоения дисциплины***

ОПК-2 Способен понимать принципы работы современных информационных технологий и программных средств, в том числе отечественного производства, и использовать их при решении задач профессиональной деятельности;

ОПК-2.1 Знает принципы работы современных информационных технологий и программных средств, в том числе отечественного производства, при решении задач профессиональной деятельности

ОПК-2.2 Умеет выбирать современные информационные технологии и программные средства, в том числе отечественного производства, при решении задач профессиональной деятельности

ОПК-2.3 Владеет навыками применения современных информационных

технологий и программных средств, в том числе отечественного производства, при решении задач профессиональной деятельности

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;

ОПК-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

ОПК-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

ОПК-3.3 Владеет навыками подготовки обзоров, аннотаций, составления рефератов, научных докладов, публикаций, и библиографии по научноисследовательской работе с учетом требований информационной безопасности

ОПК-6 Способен разрабатывать бизнес-планы и технические задания на оснащение отделов, лабораторий, офисов компьютерным и сетевым оборудованием;

ОПК-6.1 Знает принципы формирования и структуру бизнес-планов и технических заданий на оснащение отделов, лабораторий, офисов компьютерным и сетевым оборудованием

ОПК-6.2 Умеет разрабатывать бизнес-планы и технические задания на оснащение отделов, лабораторий, офисов компьютерным и сетевым оборудованием

ОПК-6.3 Владеет навыками разработки бизнес-планов и технических заданий на оснащение отделов, лабораторий, офисов компьютерным и сетевым оборудованием

ОПК-9 Способен осваивать методики использования программных средств для решения практических задач.

ОПК-9.1 Знает методики использования программных средств для решения практических задач

ОПК-9.2 Умеет использовать программные средства для решения практических задач

ОПК-9.3 Владеет навыками использования программных средств для решения практических задач

***В результате освоения дисциплины обучающийся должен:***

***1) Знать:***

- а) принципы работы современных информационных технологий и программных средств, в том числе отечественного производства, при решении задач защиты информации;***

- б) 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.
- в) принципы формирования и структуру бизнес-планов и технических заданий на оснащение отделов, лабораторий, офисов компьютерным и сетевым оборудованием
- г) методики использования программных средств для решения практических задач защиты информации

2) *Уметь:*

- а) выбирать современные информационные технологии и программные средства, в том числе отечественного производства, при решении задач защиты информации
- б) решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности
- в) разрабатывать бизнес-планы и технические задания на оснащение отделов, лабораторий, офисов компьютерным и сетевым оборудованием
- г) использовать программные средства для решения практических задач

3) *Владеть:*

- а) навыками применения современных информационных технологий и программных средств, в том числе отечественного производства, при решении задач связанных с защитой информацией
- б) навыками подготовки обзоров, аннотаций, составления рефератов, научных докладов, публикаций, и библиографии по научно-исследовательской работе с учетом требований информационной безопасности
- в) навыками разработки бизнес-планов и технических заданий на оснащение отделов, лабораторий, офисов компьютерным и сетевым оборудованием
- г) навыками использования программных средств для решения практических задач защиты информации.

#### 4. Структура и содержание дисциплины Б1.О.23 «Защита информации»

Общая трудоемкость дисциплины составляет 6 зачетных единиц, 216 часов.

№ п/п	Раздел дисциплины	Семестр	Виды учебной работы (в часах)					Оценочные средства для проведения промежуточной аттестации по разделам
			Лекции	Практические занятия	Лабораторные работы	КСР	СРС	
1	Основы защиты информации.	7	2	-	-			Экзамен
2	Модели политик безопасности	7	4	-	4			Экзамен, подготовка реферата
3	Технологии защиты информации	7	6	-				Экзамен, выполнение расчетно-графической работы
4	Программно-аппаратная защита информации	7	4	-				Экзамен
5	Защита информации в компьютерных сетях.	7	2	-				Экзамен
ИТОГО			18		36	54	81	
Форма аттестации					Экзамен(27)			

#### Очно-заочная форма обучения

№ п/п	Раздел дисциплины	Семестр	Виды учебной работы (в часах)					Оценочные средства для проведения промежуточной аттестации по разделам
			Лекции	Практические занятия	Лабораторные работы	КСР	СРС	
1	Основы защиты информации.	8	2	-	-	12	18	Экзамен
2	Модели политик безопасности	8	4	-	4	12	18	Экзамен, подготовка реферата
3	Технологии защиты информации	8	6	-	18	16	24	Экзамен, выполнение расчетно-графической работы
4	Программно-аппаратная защита информации	8	4	-	12	4	6	Экзамен
5	Защита информации в компьютерных сетях.	8	2	-	2	4	6	Экзамен
ИТОГО			18		18	54	81	
Форма аттестации					Экзамен(27)			



**5. Содержание лекционных занятий по темам с указанием формируемых компетенций**

№	Раздел дисциплины	Часы	Тема лекционного занятия	Краткое содержание	Индикаторы достижения компетенции
1	Основы защиты информации.	2	Тема 1. Основные понятия и определения защиты информации Тема 2. Системы защиты информации Тема 3. Стандартизация и сертификация в области защиты информации.	Защита информации. Объект защиты. Цель защиты информации. Система защиты информации. Свойства информации. Субъект, объект доступа. Угрозы безопасности информации и их классификация. Каналы утечки информации. Атаки на информацию Принципы проектирования СЗИ. Управление СЗИ. Обзор современных СЗИ. Закон Керхгоффа. Методы защиты информации Международные стандарты безопасности информационных технологий. Органы лицензирования и сертификации в области защиты информации в РФ. Процедуры лицензирования и сертификации	ОПК 2.1,3.1,6.1,9.1
2	Модели политик безопасности	4	Тема 4. Основные понятия политики безопасности Тема 5. Политики безопасности для защиты от несанкционированного доступа. Тема 6. Политики безопасности для защиты от нарушения целостности информации	Понятие политики безопасности. Виды политик. Политики безопасности для защиты от несанкционированного доступа. Дискреционная и мандатная политики безопасности. Политика безопасности Белла-ЛаПадулла Политики безопасности для защиты от нарушения целостности информации. Политика безопасности Биба	ОПК 2.1,3.1,6.1,9.1
	Технологии защиты информации	6	Тема 7. Идентификация и аутентификация субъектов Тема 8. Симметричная криптография Тема 9. Асимметричная крип-	Понятие, методы идентификации и аутентификации. Парольные подсистемы Симметричная криптография. Шифры замены и перестановки Публичный и закрытый ключи. Концепции Электронная подпись. Цифровые сертификаты.	ОПК 2.1,3.1,6.1,9.1

			тография (криптография с открытым ключом). Тема 10. Электронная цифровая подпись		
	Программно-аппаратная защита информации	4	Тема 11. Защита информации в операционных системах.	Угрозы безопасности операционной системе. Построение системы безопасности в системах с дискреционным доступом.	ОПК 2.1,3.1,6.1,9.1
	Защита информации в компьютерных сетях.	2	Тема 12. Защита информации в компьютерных сетях.	Классификация удаленных атак. Методы защиты от них. Использование технологий криптографии для передачи конфиденциального трафика.	ОПК 2.1,3.1,6.1,9.1

## **6. Содержание практических занятий**

*Не предусмотрено*

## **7. Содержание лабораторных занятий**

*Цель: получить навыки работы с компьютером по защите информации, овладеть методами информационных технологий по информационной безопасности информационных систем.*

№ п/п	Раздел дисциплины	Часы	Наименование лабораторной работы	Индикаторы достижения компетенции
1.	Модели политик безопасности	4	Реализация политик информационной безопасности. Дискреционная модель политики безопасности.	ОПК 2.1-2.3, 3.1-3.2, 6.1-6.3, 9.1-9.3
2.	Технологии защиты информации	2	Подсистемы парольной аутентификации пользователей.	ОПК 2.1-2.3, 3.1-3.2, 6.1-6.3, 9.1-9.3
3.		4	Симметричные алгоритмы шифрования	ОПК 2.1-2.3, 3.1-3.2, 6.1-6.3, 9.1-9.3
4.		4	Асимметричные криптосистемы.	ОПК 2.1-2.3, 3.1-3.2, 6.1-6.3, 9.1-9.3
5.		4	Электронно-цифровая подпись	ОПК 2.1-2.3, 3.1-3.2, 6.1-6.3, 9.1-9.3
6.	Программно-аппаратная защита информации	6	Защита файлов	ОПК 2.1-2.3, 3.1-3.2, 6.1-6.3, 9.1-9.3
7.		4	Оценка уязвимостей информационных технологий	ОПК 2.1-2.3, 3.1-3.2, 6.1-6.3, 9.1-9.3



8.	Технологии защиты информации	4	Определение категории значимости объекта управления к критической информационной инфраструктуре.	ОПК 2.1-2.3, 3.1-3.2, 6.1-6.3, 9.1-9.3
9.	Защита информации в компьютерных сетях.	2	Межсетевой экран	ОПК 2.1-2.3, 3.1-3.2, 6.1-6.3, 9.1-9.3
10.	Программно-аппаратная защита информации	2	Определение профиля защиты операционных систем	ОПК 2.1-2.3, 3.1-3.2, 6.1-6.3, 9.1-9.3

### **8. Самостоятельная работа**

<b>№ п/п</b>	<b>Темы, выносимые на самостоятельную работу</b>	<b>Часы</b>	<b>Форма СРС</b>	<b>Индикаторы достижения компетенции</b>
1.	Тема 1. Основные понятия и определения защиты информации	6		ОПК 2.1-2.3, 3.1-3.2, 6.1-6.3, 9.1-9.3
2.	Тема 2. Системы защиты информации	6		ОПК 2.1-2.3, 3.1-3.2, 6.1-6.3, 9.1-9.3
3.	Тема 3. Стандартизация и сертификация в области защиты информации.	6		ОПК 2.1-2.3, 3.1-3.2, 6.1-6.3, 9.1-9.3
4.	Тема 4. Основные понятия политики безопасности	6		ОПК 2.1-2.3, 3.1-3.2, 6.1-6.3, 9.1-9.3
5.	Тема 5. Политики безопасности для защиты от несанкционированного доступа.	6		ОПК 2.1-2.3, 3.1-3.2, 6.1-6.3, 9.1-9.3
6.	Тема 6. Политики безопасности для защиты от нарушения целостности информации	6		ОПК 2.1-2.3, 3.1-3.2, 6.1-6.3, 9.1-9.3
7.	Тема 7. Идентификация и аутентификация субъектов	6		ОПК 2.1-2.3, 3.1-3.2, 6.1-6.3, 9.1-9.3
8.	Тема 8. Симметричная криптография	6		ОПК 2.1-2.3, 3.1-3.2, 6.1-6.3, 9.1-9.3
9.	Тема 9. Асимметричная криптография (криптография с открытым ключом).	6		ОПК 2.1-2.3, 3.1-3.2, 6.1-6.3, 9.1-9.3
10.	Тема 10. Электронная цифровая подпись	6		ОПК 2.1-2.3, 3.1-3.2, 6.1-6.3, 9.1-9.3
11.	Тема 11. Защита информации в операционных системах.	6		ОПК 2.1-2.3, 3.1-3.2, 6.1-6.3, 9.1-9.3
12.	Тема 12. Защита информации в компьютерных сетях.	6		ОПК 2.1-2.3, 3.1-3.2, 6.1-6.3, 9.1-9.3

### ***8.1 Контроль самостоятельной работы***

<b>№ п/п</b>	<b>Темы, выносимые на самостоятельную работу</b>	<b>Часы</b>	<b>Форма КСР</b>	<b>Индикаторы достижения компетенции</b>
1.	Тема 1. Основные понятия и определения защиты информации	4	консультирование	ОПК 2.1-2.3, 3.1-3.2, 6.1-6.3, 9.1-9.3
2.	Тема 2. Системы защиты информации	4	консультирование	ОПК 2.1-2.3, 3.1-3.2, 6.1-6.3, 9.1-9.3
3.	Тема 3. Стандартизация и сертификация в области защиты информации.	4	консультирование	ОПК 2.1-2.3, 3.1-3.2, 6.1-6.3, 9.1-9.3
4.	Тема 4. Основные понятия политики безопасности	4	консультирование	ОПК 2.1-2.3, 3.1-3.2, 6.1-6.3, 9.1-9.3
5.	Тема 5. Политики безопасности для защиты от несанкционированного доступа.	4	консультирование	ОПК 2.1-2.3, 3.1-3.2, 6.1-6.3, 9.1-9.3
6.	Тема 6. Политики безопасности для защиты от нарушения целостности информации	4	консультирование	ОПК 2.1-2.3, 3.1-3.2, 6.1-6.3, 9.1-9.3
7.	Тема 7. Идентификация и аутентификация субъектов	4	консультирование	ОПК 2.1-2.3, 3.1-3.2, 6.1-6.3, 9.1-9.3
8.	Тема 8. Симметричная криптография	4	консультирование	ОПК 2.1-2.3, 3.1-3.2, 6.1-6.3, 9.1-9.3
9.	Тема 9. Асимметричная криптография (криптография с открытым ключом).	4	консультирование	ОПК 2.1-2.3, 3.1-3.2, 6.1-6.3, 9.1-9.3
10.	Тема 10. Электронная цифровая подпись	4	консультирование	ОПК 2.1-2.3, 3.1-3.2, 6.1-6.3, 9.1-9.3
11.	Тема 11. Защита информации в операционных системах.	4	консультирование	ОПК 2.1-2.3, 3.1-3.2, 6.1-6.3, 9.1-9.3
12.	Тема 12. Защита информации в компьютерных сетях.	4	консультирование	ОПК 2.1-2.3, 3.1-3.2, 6.1-6.3, 9.1-9.3

### ***9. Использование рейтинговой системы оценки знаний***

При оценке результатов деятельности обучающихся в рамках дисциплины «Защита информации» используется рейтинговая система. Рейтинговая оценка формируется на основании текущего и промежуточного контроля. Максимальное и минимальное количество баллов по различным видам учебной работы описано в «Положении о балльно-рейтинговой системе оценки знаний студентов и обеспечения качества учебного процесса» ФГБОУ ВО «КНИТУ».

При изучении дисциплины предусматривается экзамен, реферат, выполнение двух расчётно-графических работ. За эти контрольные точки студент может получить минимальное и максимальное количество баллов (см. таблицу).

За экзамен студент может получить минимум 24 балла и максимум – 40 баллов.

Оценочные средства	Кол-во	Min, баллов	Max, баллов
Расчётно-графических работа	2	26	40
Реферат	1	10	20
Экзамен	1	24	40
Итого:		60	100

### ***10. Оценочные средства для текущего контроля успеваемости, промежуточной аттестации по итогам освоения дисциплины***

Оценочные средства для проведения текущего контроля успеваемости, промежуточной аттестации обучающихся и итоговой (государственной итоговой) аттестации разрабатываются согласно положению о Фондах оценочных средств, рассматриваются как составная часть рабочей программы и оформляются отдельным документом.

### ***11. Информационно-методическое обеспечение дисциплины***

#### ***11.1. Основная литература***

При изучении дисциплины «Защита информации» в качестве основных источников информации рекомендуется использовать следующую литературу.

Основные источники информации	Кол-во экз.
1. Защита информации : учебное пособие / А.П. Жук, Е.П. Жук, О.М. Лепешкин, А.И. Тимошкин. — 3-е изд. — Москва : РИОР : ИНФРА-М, 2021. — 400 с. — (Высшее образование). — DOI: <a href="https://doi.org/10.12737/1759-3">https://doi.org/10.12737/1759-3</a> . - ISBN 978-5-369-01759-3. - Текст : электронный. - URL: <a href="https://znanium.com/catalog/product/1210523">https://znanium.com/catalog/product/1210523</a> . – Режим доступа: по подписке.	1 (безлимитный доступ к ЭБС «Znanium» после регистрации с IP-адреса НХТИ)
2 Сычев, Ю. Н. Защита информации и информационная безопасность : учебное пособие / Ю.Н. Сычев. — Москва : ИНФРА-М, 2021. — 201 с. — (Высшее образование: Бакалавриат). — DOI 10.12737/1013711. - ISBN 978-5-16-014976-9. - Текст : электронный. - URL: <a href="https://znanium.com/catalog/product/1013711">https://znanium.com/catalog/product/1013711</a> – Режим доступа: по подписке.	1 (безлимитный доступ к ЭБС «Znanium» после регистрации с IP-адреса НХТИ)

3 Баранова, Е. К. Информационная безопасность и защита информации : учебное пособие / Е.К. Баранова, А.В. Бабаш. — 4-е изд., перераб. и доп. — Москва : РИОР : ИНФРА-М, 2021. — 336 с. — (Высшее образование). — DOI: <a href="https://doi.org/10.29039/1761-6">https://doi.org/10.29039/1761-6</a> . - ISBN 978-5-369-01761-6. - Текст : электронный. - URL: <a href="https://znanium.com/catalog/product/1189326">https://znanium.com/catalog/product/1189326</a> — Режим доступа: по подписке., по паролю. — ЭБС «Znanium», УМО	1 (безлимитный доступ к ЭБС «Znanium» после регистрации с IP-адреса НХТИ)
4. Шаньгин, В. Ф. Комплексная защита информации в корпоративных системах : учебное пособие / В. Ф. Шаньгин. — Москва : ФОРУМ : ИНФРА-М, 2020. — 592 с. — (Высшее образование: Бакалавриат). - ISBN 978-5-8199-0730-6. - Текст : электронный. - URL: <a href="https://znanium.com/catalog/product/1093695">https://znanium.com/catalog/product/1093695</a> — Режим доступа: по подписке., по паролю. — ЭБС «Znanium» УМО	1 (безлимитный доступ к ЭБС «Znanium» после регистрации с IP-адреса НХТИ)
5. Гришина, Н. В. Основы информационной безопасности предприятия : учебное пособие / Н.В. Гришина. — Москва : ИНФРА-М, 2021. — 216 с. — (Высшее образование: Бакалавриат). — <a href="http://www.dx.doi.org/10.12737/textbook_5cf8ce075a0298.77906820">www.dx.doi.org/10.12737/textbook_5cf8ce075a0298.77906820</a> . - ISBN 978-5-16-015105-2. - Текст : электронный. - URL: <a href="https://znanium.com/catalog/product/1784437">https://znanium.com/catalog/product/1784437</a> — Режим доступа: по подписке. — ЭБС «Znanium» УМО	1 (безлимитный доступ к ЭБС «Znanium» после регистрации с IP-адреса НХТИ)

### ***11.2. Дополнительная литература***

В качестве дополнительных источников информации рекомендуется использовать следующую литературу:

<b>Дополнительные источники информации</b>	<b>Кол-во экз.</b>
1. Загинайлов, Ю. Н. Теория информационной безопасности и методология защиты информации [Электронный ресурс]: учебное пособие. - М.-Берлин: Директ-Медиа, 2015. - 253 с. Режим доступа, по паролю. — ЭБС «Книгафонд»	1 (безлимитный доступ к ЭБС «Книгафонд» после регистрации с IP-адреса НХТИ)

### ***11.3. Электронные источники информации***

При изучении дисциплины «Защита информации» использование электронных источников информации:

Федеральный портал «Российское образование» <a href="http://www.edu.ru/">http://www.edu.ru/</a>	Открытый Интернет-ресурс, свободный безлимитный доступ.
--	---

Федеральный центр информационно-образовательных ресурсов <a href="http://fcior.edu.ru/">http://fcior.edu.ru/</a>	Электронные образовательные ресурсы и сервисы для всех уровней и ступеней образования. Открытый Интернет-ресурс, свободный безлимитный доступ.
Информационная система «Единое окно доступа к образовательным ресурсам» <a href="http://window.edu.ru/">http://window.edu.ru/</a>	Российское образование: единое окно доступа к образовательным ресурсам, свободный безлимитный доступ.

#### ***11.4. Современные профессиональные базы данных и информационные справочные системы.***

1. Журнал «Информационные технологии». Сайт журнала. – Доступ свободный: <http://novtex.ru/IT/>.

2. Журнал «Информационные технологии и системы». Сайт журнала. – Доступ свободный: <https://itsys.tb.ru>.

**Согласовано:**

зав. отделом  
по библиотечному  
обслуживанию

Тарасова В.Я.

## **12. Материально-техническое обеспечение дисциплины (модуля).**

«Компьютерный класс 115В»

Учебная аудитория для проведения учебных занятий оснащена оборудованием:

1. Доступ к электронной информационно-образовательной среде вуза
2. Схемы и стенды для проведения лабораторных практикумов

Техническими средствами обучения:

1. Интерактивная доска;
2. Проектор

Помещения для самостоятельной работы оснащены компьютерной техникой в количестве 15 шт. с возможностью подключения к сети «Интернет» и обеспечены доступом в электронную информационную среду НХТИ. Допускается замена оборудования его виртуальными аналогами.

Лицензированное программное обеспечение и свободно распространяемое программное обеспечение, используемое в учебном процессе при освоении дисциплины:

Microsoft Office

## **13. Образовательные технологии**

Тема	Вид занятия	Интерактивная форма	часы
Тема 1. Основные понятия и определения Информационной безопасности.	Лекция	Вводная лекция, лекция визуализация	0,25
Тема 2. СЗИ от угроз нарушения конфиденциальности	Лекция	лекция визуализация	0,25
Тема 3. СЗИ от угроз нарушения целостности.	Лекция	лекция визуализация	0,25
Тема 4. СЗИ от угроз нарушения доступности	Лекция	лекция визуализация	0,25
Тема 5. Основные понятия политики безопасности	Лекция	лекция визуализация	0,25
Тема 6. Политики безопасности для защиты от несанкционированного доступа.	Лекция	лекция визуализация	0,25
Тема 7. Политики безопасности для защиты от нарушения целостности информации	Лекция	лекция визуализация	0,25
Тема 8. Безопасность периметра сети	Лекция	лекция визуализация	0,25
Тема 9. Защита рабочих станций	Лекция	лекция визуализация	0,25
Тема 10. Мероприятия по защите ключевых систем информационной инфраструктуры	Лекция	лекция визуализация	0,25
Симметричные алгоритмы шифрования	Лаб.зан	Метод проектов	0,25
Симметричные и асимметричные криптосистемы. Электронно-цифровая подпись	Лаб.зан	Метод проектов	0,25

Реализация политик информационной безопасности. Дискреционная модель политики безопасности.	Лаб.зан	Метод проектов	0,25
Анализ степени защищенности объекта информатизации	Лаб.зан	Работа в малых группах, метод проектов	0,25
Исследование средств защиты информации и идентификации пользователей в ОС	Лаб.зан	Работа в малых группах, метод проектов	0,5
Итого:			4