

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

« 30 » мая 2022 г.

РАБОЧАЯ ПРОГРАММА

По дисциплине Б1.В.06 Программно-аппаратные средства обеспечения информационной безопасности

Направление подготовки 09.03.02 «Информационные системы и технологии»

Профиль/программа Системы информационной безопасности

Квалификация (степень) выпускника бакалавр

Форма обучения очная

Факультет Информационных технологий

Кафедра-разработчик рабочей программы информационных систем и технологий

Очное: курс - 3, семестр – 5

	Часы	Зачетные единицы
Лекции	36	1
Практические занятия	-	-
Лабораторные занятия	54	1,5
Контроль самостоятельной работы	99	2,75
Самостоятельная работа	72	2
Форма аттестации (часы на контроль)	Экзамен (27)	0,75
Всего	288	8

Нижекамск, 2022 г.

Рабочая программа составлена с учетом требований Федерального государственного образовательного стандарта высшего образования
(№ 926 от 19.09.2017) по направлению 09.03.02

(номер, дата утверждения)

(шифр)

«Информационные системы и технологии»

(наименование направления)

на основании учебного плана набора обучающихся 2022 г.

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 г. № 8

Зав. кафедрой


(подпись)

О.В. Матухина

(Ф.И.О.)

1. Цели освоения дисциплины

Целями освоения дисциплины Б1.В.06 Программно-аппаратные средства обеспечения информационной безопасности 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.В.06 Программно-аппаратные средства обеспечения информационной безопасности относится к обязательной части ООП и формирует у бакалавров по направлению подготовки 09.03.02 «Информационные системы и технологии» набор знаний, умений, навыков и компетенций.

Для успешного освоения дисциплины Б1.В.06 Программно-аппаратные средства обеспечения информационной безопасности *бакалавр по* направлению подготовки 09.03.02 «Информационные системы и технологии» должен освоить материал предшествующих дисциплин:

- а) Б1.О.20 Основы информатики и кибернетики;
- б) Б1.О.23 Системы управления базами данных;
- в) Б1.О.25 Программирование на языке высокого уровня;
- г) Б1.В.05 Языки программирования общего назначения;
- д) Б1.В.04 Теория информации и кодирования;

Дисциплина является предшествующей и необходима для успешного усвоения последующих дисциплин:

- а) Б1.В.10 Криптографические методы защиты информации;
- б) Б1.В.16 Безопасность программного обеспечения;
- в) Б1.В.18 Управление информационным пространством;
- г) Б1.В.20 Проектирование и разработка защищённых автоматизированных систем;
- д) Б1.В.21 Киберфизические системы;
- е) Б1.В.23 Технологии проектирования программного обеспечения;
- ж) Б1.В.ДВ.01.01 Разработка приложений в среде 1С
- з) Б1.В.ДВ.03.01 Моделирование объектов, процессов и систем.

Знания, полученные при изучении дисциплины, Б1.В.06 Программно-аппаратные средства обеспечения информационной безопасности могут быть использованы при прохождении практик и выполнении выпускной квалификационной работы.

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

ПК-2 Способен обеспечить информационную безопасность на уровне баз данных

ПК-2.1 Знает угрозы безопасности баз данных, способы предотвращения

ПК-2.2 Умеет выявлять угрозы безопасности на уровне баз данных

ПК-2.3 Владеет навыками применения способов предотвращения угроз безопасности на уровне баз данных

ПК-3 Способен выполнять работы и управлять работами по созданию (модификации) и сопровождению ИС, автоматизирующих задачи организационного управления и бизнес-процессы

ПК-3.1 Знает инструменты и методы проектирования архитектуры ИС, устройство, функционирование вычислительных систем и современных ИС, автоматизирующих задачи организационного управления и бизнес-процессы

ПК-3.2 Умеет проектировать архитектуру ИС, анализировать входную информацию, разрабатывать структуру баз данных, автоматизирующих задачи организационного управления и бизнес-процессы

ПК-3.3 Владеет навыками проектирования архитектуры ИС, структуры баз данных, работы современных ИС, автоматизирующих задачи организационного управления и бизнес-процессы

В результате освоения дисциплины обучающийся должен:

1) Знать:

а) принципы работы современных информационных технологий и программных средств, 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) методики использования программных средств для решения практических задач защиты информации;

г) угрозы безопасности и способы предотвращения

д) инструменты и методы проектирования архитектуры ИС, устройство, функционирование вычислительных систем и современных ИС, автоматизирующих задачи организационного управления и бизнес-процессы с точки зрения информационной безопасности.

2) Уметь:

а) решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности

б) выявлять угрозы информационной безопасности

в) проектировать архитектуру ИС, анализировать входную информацию, разрабатывать структуру баз данных, автоматизирующих задачи организационного управления и бизнес-процессы с точки зрения информационной безопасности.

3) Владеть:

- а) навыками подготовки обзоров, аннотаций, составления рефератов, научных докладов, публикаций, и библиографии по научно-исследовательской работе с учетом требований информационной безопасности;
- б) навыками применения способов предотвращения угроз информационной безопасности;
- в) навыками использования программных средств для решения практических задач защиты информации
- г) навыками проектирования архитектуры ИС, структуры баз данных, работы современных ИС, автоматизирующих задачи организационного управления и бизнес-процессы с точки зрения информационной безопасности.

4. Структура и содержание дисциплины Б1.В.06 Программно-аппаратные средства обеспечения информационной безопасности

Общая трудоемкость дисциплины составляет 8_зачетных единиц, 288 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	Основные принципы программной и программно-аппаратной защиты информации	7	10	-	12	33	20	Тестирование, подготовка реферата
2	Защита автономных автоматизированных систем	7	18	-	16	48	32	Тестирование, подготовка реферата
3	Защита информации в локальных сетях	7	8	-	4	18	20	Тестирование, подготовка реферата
ИТОГО			36		54	99	72	
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	Основные принципы программной и программно-аппаратной защиты информации	10	Предмет и задачи программно-аппаратной защиты информации	Предмет и задачи программно-аппаратной защиты информации. Основные понятия программно-аппаратной защиты информации. Классификация методов и средств программно-аппаратной защиты информации	ПК – 2.1, 3.1

			Стандарты безопасности	Нормативные правовые акты, нормативные методические документы, в состав которых входят требования и рекомендации по защите информации программными и программно-аппаратными средствами. Профили защиты программных и программно-аппаратных средств (межсетевых экранов, средств контроля съемных машинных носителей информации, средств доверенной загрузки, средств антивирусной защиты). Стандарты по защите информации, в состав которых входят требования и рекомендации по защите информации программными и программно-аппаратными средствами.	
			Защищенная автоматизированная система	Автоматизация процесса обработки информации. Понятие автоматизированной системы. Особенности автоматизированных систем в защищенном исполнении. Основные виды АС в защищенном исполнении. Методы создания безопасных систем	
			Дестабилизирующее воздействие на объекты защиты	Источники дестабилизирующего воздействия на объекты защиты. Способы воздействия на информацию. Причины и условия дестабилизирующего воздействия на информацию	
			Принципы программно-аппаратной защиты информации от несанкци-	Основные подходы к защите информации от НСД Организация доступа к файлам, контроль доступа и разграничение доступа, иерархический доступ к файлам. Фиксация доступа к файлам До-	

			онирован- ного до- ступа	ступ к данным со стороны про- цесса Особенности защиты дан- ных от изменения. Шифрование.	
2	Защита ав- тономных автоматизи- рованных систем	18	Основы за- щиты авто- номных ав- томатизиров анных си- стем	Работа автономной АС в защи- щенном режиме 10 Алгоритм за- грузки ОС. Штатные средства замыкания среды Расширение BIOS как средство замыкания программной среды Системы типа Электронный замок. ЭЗ с проверкой целостности про- граммной среды. Понятие АМДЗ (доверенная загрузка) Применение закладок, направ- ленных на снижение эффектив- ности средств, замыкающих среду.	ПК – 2.1, 3.1
			Защита про- грамм от изучения	Изучение и обратное проектиро- вание ПО 10 Способы изучения ПО: статическое и динамиче- ское изучение Задачи защиты от изучения и способы их решения Защита от отладки. Защита от дизассемблирования Защита от трассировки по прерываниям.	
			Вредонос- ное про- граммное обеспечение	Вредоносное программное обес- печение как особый вид разру- шающих воздействий Класси- фикация вредоносного программного обеспечения. Схема заражения. Средства нейтрализации вредоносного ПО. Профилактика заражения Поиск следов активности вредо- носного ПО. Реестр ОС. Основ- ные ветки, содержащие инфор- мацию о вредоносном ПО. Другие объекты, содержащие информацию о вредоносном ПО, файлы prefetch. Бот-неты.	

			<p>Принцип функционирования. Методы обнаружения Классификация антивирусных средств. Сигнатурный и эвристический анализ Защита от вирусов в "ручном режиме" Основные концепции построения систем антивирусной защиты на предприятии</p>	
		Защита программ и данных от несанкционированного копирования	<p>Несанкционированное копирование программ как тип НСД Юридические аспекты несанкционированного копирования программ. Общее понятие защиты от копирования. Привязка ПО к аппаратному окружению и носителям. Защитные механизмы в современном программном обеспечении</p>	
		Защита информации на машинных носителях	<p>Проблема защиты отчуждаемых компонентов ПЭВМ. Методы защиты информации на отчуждаемых носителях. Шифрование. Средства восстановления остаточной информации. Создание посекторных образов НЖМД. Применение средств восстановления остаточной информации в судебных криминалистических экспертизах и при расследовании инцидентов. Нормативная база, документирование результатов Безвозвратное удаление данных. Принципы и алгоритмы.</p>	
		Аппаратные средства идентификации и аутентификации пользователей	<p>Требования к аппаратным средствам идентификации и аутентификации пользователей</p>	
		Системы обнаружения	<p>СОВ и СОА, отличия в функциях. Основные архитектуры</p>	

			атак и вторжений	СОВ 10 Использование сетевых снифферов в качестве СОВ Аппаратный компонент СОВ Программный компонент СОВ Модели системы обнаружения вторжений, Классификация систем обнаружения вторжений. Обнаружение сигнатур. Обнаружение аномалий. Другие методы обнаружения вторжений.	
			Защита информации в базах данных	Основные типы угроз. Модель нарушителя Средства идентификации и аутентификации. Управление доступом Средства контроля целостности информации в базах данных Средства аудита и контроля безопасности. Критерии защищенности баз данных Применение криптографических средств защиты информации в базах данных	
3	Защита информации в сетях	8	Основы построения защищенных локальных сетей	Сети, работающие по технологии коммутации пакетов Стек протоколов TCP/IP. Особенности маршрутизации. Штатные средства защиты информации стека протоколов TCP/IP. Средства идентификации и аутентификации на разных уровнях протокола TCP/IP, достоинства, недостатки, ограничения.	ПК – 2.1, 3.1
			Средства организации VPN	Виртуальная частная сеть. Функции, назначение, принцип построения Криптографические и некриптографические средства организации VPN Устройства, образующие VPN. Криптомаршрутизатор и криптофильтр. Криптороутер. Принципы, архитектура, модель нарушителя, достоинства и недостатки Криптофильтр. Принципы, архитектура, модель нарушителя, достоинства и недостатки	

			Обеспечение безопасности межсетевого взаимодействия (в сетях общего доступа)	Методы защиты информации при работе в сетях общего доступа. Межсетевые экраны типа firewall. Достоинства, недостатки, реализуемые политики безопасности Основные типы firewall. Симметричные и несимметричные firewall.	

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.	Основные принципы программной и программно-аппаратной защиты информации	2	Нормативно-правовые акты, стандарты по защите информации программно-аппаратными средствами	ПК – 2.1-2.3 ПК – 3.1-3.3
2.		2	Идентификация и аутентификация пользователей	
3.		2	Разграничение доступа.	
4.		2	Регистрация событий	
5.		4	Защита файлов	
6.	Защита автономных и автоматизированных систем	4	Ознакомление с современными программными и программно-аппаратными средствами защиты от НСД	ПК – 2.1-2.3 ПК – 3.1-3.3
7.		4	Применения средств исследования реестра ОС для нахождения следов активности вредоносного ПО	
8.		4	Защита информации от несанкционированного копирования	
9.		2	Защитные механизмы в приложениях Office	
10.		2	Применение средства восстановления остаточной информации на примере Foremost или аналога	
11.		2	Применение специализированного программного средства для восстановления удаленных файлов	
12.		2	Применение программ для безвозвратного удаления данных	
13.		2	Программы для шифрования данных на съемных носителях	
14.		4	Моделирование проведения атаки. Изучение инструментальных средств обнаружения вторжений	
15.		4	Изучение механизмов защиты СУБД	
16.		4	Изучение штатных средств защиты СУБД MSSQL Server	
17.		4	VPN	ПК – 2.1-2.3

18.	Защита информации в сетях	4	Изучение и сравнение архитектур Dual Homed Host, Bastion Host, Perimetr	ПК – 3.1-3.3
19.		4	Изучение различных способов закрытия "опасных" портов	

8. Самостоятельная работа

№ п/п	Темы, выносимые на самостоятельную работу	Часы	Форма СРС	Индикаторы достижения компетенции
1.	Предмет и задачи программно-аппаратной защиты информации	4	Работа с лекционным материалом, учебной литературой. Подготовка к тестированию.	ПК – 2.1-2.3 ПК – 3.1-3.3
2.	Стандарты безопасности	4	Работа с лекционным материалом, учебной литературой. Подготовка к тестированию.	ПК – 2.1-2.3 ПК – 3.1-3.3
3.	Защищенная автоматизированная система	4	Работа с лекционным материалом, учебной литературой. Подготовка к тестированию.	ПК – 2.1-2.3 ПК – 3.1-3.3
4.	Дестабилизирующее воздействие на объекты защиты	4	Работа с лекционным материалом, учебной литературой. Подготовка к тестированию.	ПК – 2.1-2.3 ПК – 3.1-3.3
5.	Принципы программно-аппаратной защиты информации от несанкционированного доступа	4	Работа с лекционным материалом, учебной литературой. Подготовка к тестированию.	ПК – 2.1-2.3 ПК – 3.1-3.3
6.	Основы защиты автономных автоматизированных систем	4	Работа с лекционным материалом, учебной литературой. Подготовка к тестированию.	ПК – 2.1-2.3 ПК – 3.1-3.3
7.	Защита программ от изучения	4	Работа с лекционным материалом, учебной литературой. Подготовка к тестированию.	ПК – 2.1-2.3 ПК – 3.1-3.3
8.	Вредоносное программное обеспечение	4	Работа с лекционным материалом, учебной литературой. Подготовка к тестированию.	ПК – 2.1-2.3 ПК – 3.1-3.3
9.	Защита программ и данных от несанкционированного копирования	4	Работа с лекционным материалом, учебной литературой. Подготовка к тестированию.	ПК – 2.1-2.3 ПК – 3.1-3.3
10.	Защита информации на машинных носителях	4	Работа с лекционным материалом, учебной литературой. Подготовка к тестированию.	ПК – 2.1-2.3 ПК – 3.1-3.3
11.	Аппаратные средства идентификации и аутентификации пользователей	4	Работа с лекционным материалом, учебной литературой. Подготовка к тестированию.	ПК – 2.1-2.3 ПК – 3.1-3.3
12.	Системы обнаружения атак и вторжений	4	Работа с лекционным материалом, учебной литературой. Подготовка к тестированию.	ПК – 2.1-2.3 ПК – 3.1-3.3
13.	Защита информации в базах данных	4	Работа с лекционным материалом, учебной литературой. Подготовка к тестированию.	ПК – 2.1-2.3 ПК – 3.1-3.3
14.	Основы построения защищенных локальных сетей	4	Работа с лекционным материалом, учебной литературой. Подготовка к тестированию.	ПК – 2.1-2.3 ПК – 3.1-3.3
15.	Средства организации VPN	8	Работа с лекционным материалом, учебной литературой. Подготовка к	ПК – 2.1-2.3 ПК – 3.1-3.3

			тестированию.	
16.	Обеспечение безопасности межсетевого взаимодействия (в сетях общего доступа)	8	Работа с лекционным материалом, учебной литературой. Подготовка к тестированию.	ПК – 2.1-2.3 ПК – 3.1-3.3

8.1 Контроль самостоятельной работы

№ п/п	Темы, выносимые на самостоятельную работу	Часы	Форма КСР	Индикаторы достижения компетенции
1.	Предмет и задачи программно-аппаратной защиты информации	9	консультирование	ПК – 2.1-2.3 ПК – 3.1-3.3
2.	Стандарты безопасности	6	консультирование	ПК – 2.1-2.3 ПК – 3.1-3.3
3.	Защищенная автоматизированная система	6	консультирование	ПК – 2.1-2.3 ПК – 3.1-3.3
4.	Дестабилизирующее воздействие на объекты защиты	6	консультирование	ПК – 2.1-2.3 ПК – 3.1-3.3
5.	Принципы программно-аппаратной защиты информации от несанкционированного доступа	6	консультирование	ПК – 2.1-2.3 ПК – 3.1-3.3
6.	Основы защиты автономных автоматизированных систем	6	консультирование	ПК – 2.1-2.3 ПК – 3.1-3.3
7.	Защита программ от изучения	6	консультирование	ПК – 2.1-2.3 ПК – 3.1-3.3
8.	Вредоносное программное обеспечение	6	консультирование	ПК – 2.1-2.3 ПК – 3.1-3.3
9.	Защита программ и данных от несанкционированного копирования	6	консультирование	ПК – 2.1-2.3 ПК – 3.1-3.3
10.	Защита информации на машинных носителях	6	консультирование	ПК – 2.1-2.3 ПК – 3.1-3.3
11.	Аппаратные средства идентификации и аутентификации пользователей	6	консультирование	ПК – 2.1-2.3 ПК – 3.1-3.3
12.	Системы обнаружения атак и вторжений	6	консультирование	ПК – 2.1-2.3 ПК – 3.1-3.3
13.	Защита информации в базах данных	6	консультирование	ПК – 2.1-2.3 ПК – 3.1-3.3
14.	Основы построения защищенных локальных сетей	6	консультирование	ПК – 2.1-2.3 ПК – 3.1-3.3
15.	Средства организации VPN	6	консультирование	ПК – 2.1-2.3 ПК – 3.1-3.3

16.	Обеспечение безопасности межсетевого взаимодействия (в сетях общего доступа)	6	консультирование	ПК – 2.1-2.3 ПК – 3.1-3.3
-----	--	---	------------------	------------------------------

9. Использование рейтинговой системы оценки знаний

При оценке результатов деятельности обучающихся в рамках дисциплины Б1.В.06 Программно-аппаратные средства обеспечения информационной безопасности 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 реферат, тестирование. 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
Реферат	1	20	40
Тестирование	1	40	60
Итого:		60	100

При изучении дисциплины предусматривается выполнение курсовой работы. Студент может получить минимальное и максимальное количество баллов (см. таблицу).

Оценочные средства	Кол-во	Min, баллов	Max, баллов
Курсовой работа	1	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 Б1.В.06 Программно-аппаратные средства обеспечения информационной безопасности 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: https://doi.org/10.12737/1759-3 . - ISBN 978-5-369-01759-3. - Текст : электронный. - URL: https://znanium.com/catalog/product/1210523). — Режим доступа: по подписке.	1 (безлимитный доступ к ЭБС «Znanium» после регистрации с IP-адреса НХТИ)
1. 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: https://znanium.com/catalog/product/1013711 . — 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: https://doi.org/10.29039/1761-6 . - ISBN 978-5-369-01761-6. - Текст : электронный. - URL: https://znanium.com/catalog/product/1189326 . — 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: https://znanium.com/catalog/product/1093695 . — 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). — www.dx.doi.org/10.12737/textbook_5cf8ce075a0298.77906820 . - ISBN 978-5-16-015105-2. - Текст : электронный. - URL: https://znanium.com/catalog/product/1784437 . — 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:

Дополнительные источники информации	Кол-во экз.
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 Б1.В.06 Программно-аппаратные средства обеспечения информационной безопасности использование электронных источников информации:

Федеральный портал «Российское образование» http://www.edu.ru/	Открытый Интернет-ресурс, свободный безлимитный доступ.
Федеральный центр информационно-образовательных ресурсов http://fcior.edu.ru/	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» http://window.edu.ru/	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>.

3. Базы данных правовой информации, информационно-справочные и поисковые системы - «Гарант» - www.garant.ru; - Информационно-справочная система «Консультант Плюс».

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
Предмет и задачи программно-аппаратной защиты информации	Лекция	Вводная лекция, лекция визуализация	0.5
Стандарты безопасности	Лекция	лекция визуализация	0.5
Защищенная автоматизированная система	Лекция	лекция визуализация	0.5
Дестабилизирующее воздействие на объекты защиты	Лекция	лекция визуализация	0.5
Принципы программно-аппаратной защиты информации от несанкционированного доступа	Лекция	лекция визуализация	0.5
Основы защиты автономных автоматизированных систем	Лекция	лекция визуализация	0.5
Защита программ от излучения	Лекция	лекция визуализация	0.5
Вредоносное программное обеспечение	Лекция	лекция визуализация	0.5
Защита программ и данных от несанкционированного копирования	Лекция	лекция визуализация	0.5
Защита информации на машинных носителях	Лекция	лекция визуализация	0.5
Аппаратные средства идентификации и аутентификации пользователей	Лекция	лекция визуализация	0.5
Системы обнаружения атак и вторжений	Лекция	лекция визуализация	0.5
Защита информации в базах данных	Лекция	лекция визуализация	0.5
Основы построения защищенных локальных сетей	Лекция	лекция визуализация	0.5
Средства организации VPN	Лекция	лекция визуализация	0.5
Обеспечение безопасности межсетевого взаимодействия (в сетях общего доступа)	Лекция	лекция визуализация	0.5
Нормативно-правовые акты, стандарты по защите информации программно-аппаратными средствами	Лаб.зан	Работа в малых группах, метод проектов	0,3
Идентификация и аутентификация пользователей	Лаб.зан	Работа в малых группах, метод проектов	0,3
Разграничение доступа.	Лаб.зан	Работа в малых группах, метод проектов	0,3

Регистрация событий	Лаб.зан	Работа в малых группах, метод проектов	0,3
Защита файлов	Лаб.зан	Работа в малых группах, метод проектов	0,3
Ознакомление с современными программными и программно-аппаратными средствами защиты от НСД	Лаб.зан	Работа в малых группах, метод проектов	0,3
Применения средств исследования реестра ОС для нахождения следов активности вредоносного ПО	Лаб.зан	Работа в малых группах, метод проектов	0,3
Защита информации от несанкционированного копирования	Лаб.зан	Работа в малых группах, метод проектов	0,3
Защитные механизмы в приложениях Office	Лаб.зан	Работа в малых группах, метод проектов	0,3
Применение средства восстановления остаточной информации на примере Foremost или аналога	Лаб.зан	Работа в малых группах, метод проектов	0,3
Применение специализированного программного средства для восстановления удаленных файлов	Лаб.зан	Работа в малых группах, метод проектов	0,3
Применение программ для безвозвратного удаления данных	Лаб.зан	Работа в малых группах, метод проектов	0,3
Программы для шифрования данных на съемных носителях	Лаб.зан	Работа в малых группах, метод проектов	0,3
Моделирование проведения атаки. Изучение инструментальных средств обнаружения вторжений	Лаб.зан	Работа в малых группах, метод проектов	0,3
Изучение механизмов защиты СУБД	Лаб.зан	Работа в малых группах, метод проектов	0,3
Изучение штатных средств защиты СУБД MSSQL Server	Лаб.зан	Работа в малых группах, метод проектов	0,3
VPN	Лаб.зан	Работа в малых группах, метод проектов	0,3
Изучение и сравнение архитектур Dual Homed Host, Bastion Host, Perimetr	Лаб.зан	Работа в малых группах, метод проектов	0,3
Изучение различных способов закрытия "опасных" портов	Лаб.зан	Работа в малых группах, метод проектов	0,3
Итого:			14