

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.13 Информационная безопасность систем управления
Направление подготовки 27.03.04 «Управление в технических системах»
Профиль/программа Системы и средства автоматизации технологических процессов
Квалификация выпускника бакалавр
Форма обучения очная-заочная
Факультет Информационных технологий
Кафедра-разработчик рабочей программы Информационных систем и технологий

Заочная форма обучения Курс 4, семестр 7

	Часы	Зачетные единицы
Лекции	9	0,25
Практические занятия	-	
Лабораторные занятия	18	0,5
КСР	18	0,5
Самостоятельная работа	27	0,75
Форма аттестации (часы на контроль)	Зачёт	
Всего	72	2

Нижекамск, 2022 г.

Рабочая программа составлена с учетом требований Федерального государственного образовательного стандарта высшего образования (№871 от 31.07.2020) по направлению 27.03.04 «Управление в технических системах» на основании учебного плана набора обучающихся 2022.

Разработчики 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)

Матухина О.В.

1. Цели освоения дисциплины

Целями освоения дисциплины Б1.В.09 Информационная безопасность систем управления 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 информационной безопасности.*

2. Место дисциплины (модуля) в структуре образовательной программы

Дисциплина Информационная безопасность систем управления относится к *вариативной* части ОП и формирует у бакалавров по направлению подготовки 27.03.04 «Управление в технических системах» набор знаний, умений, навыков и компетенций.

Для успешного освоения дисциплины *бакалавр* по направлению подготовки 27.03.04 «Управление в технических системах» должен освоить материал предшествующих дисциплин:

- а) Б1.Б.16 Информационные технологии (информатика);*
- б) Б1.В.12 Полевые, промышленные и информационные сети;*
- в) Б1.О.20 Прикладное программирование;*
- г) Б1.В.19 Программирование и основы алгоритмизации.*

Знания, полученные при изучении дисциплины, Б1.В.13 Информационная безопасность систем управления могут быть использованы при прохождении практик (указать виды практик из учебного плана) и выполнении *выпускных квалификационных работ* 27.03.04 «Управление в технических системах».

3. Компетенции обучающегося, формируемые в результате освоения дисциплины

ПК-2 Способен к определению целесообразности автоматизации процессов управления, к разработке информационного обеспечения автоматизированной системы управления производством и заданий на проектирование оригинальных компонентов АСУП, к контролю ввода ее в действие и эксплуатации

ПК - 2.1 Знает методы проектирования отдельных блоков и устройств систем автоматизации и выбирать стандартные средства вычислительной техники для проектирования систем автоматизации в соответствии с техническим заданием

ПК - 2.2 Умеет производить проектирование отдельных блоков и устройств систем автоматизации и выбирать стандартные средства вычислительной техники для проектирования систем автоматизации и управления в соответствии с техническим заданием

ПК – 2.3 Владеет методиками проектирования отдельных блоков и

устройств систем автоматизации выбирать стандартные средства вычислительной техники для проектирования систем автоматизации и управления в соответствии с техническим заданием

В результате освоения дисциплины обучающийся должен:

- 1) Знать: а) правовые основы информационной безопасности;
 б) классификацию потенциальных угроз информационной безопасности систем управления технологическими процессами;
 в) современные криптографические алгоритмы
 г) методы проектирования отдельных блоков и устройств систем автоматизации и выбирать стандартные средства вычислительной техники для проектирования систем автоматизации в соответствии с техническим заданием
- 2) Уметь: а) применять методы защиты компьютерной информации при проектировании АСОИУ в различных предметных областях;
 б) классифицировать типовые сетевые атаки;
 в) конфигурировать межсетевые экраны для предотвращения различных типов сетевых атак;
 г) производить проектирование отдельных блоков и устройств систем автоматизации и выбирать стандартные средства вычислительной техники для проектирования систем автоматизации и управления в соответствии с техническим заданием
- 3) Владеть: а) стандартами, моделями и методами шифрования;
 б) методами идентификации пользователей;
 в) методами защиты программ от вирусов;
 г) принципами построения системы безопасности в операционных системах;
 д) основными алгоритмами симметричного и асимметричного шифрования
 е) способностью использовать правовые основы по защите информации в области информационной безопасности систем управления технологическим процессом.
 ж) методиками проектирования отдельных блоков и устройств систем автоматизации выбирать стандартные средства вычислительной техники для проектирования систем автоматизации и управления в соответствии с техническим заданием;

4. Структура и содержание дисциплины Б1.В.13 Информационная безопасность систем управления

Общая трудоемкость дисциплины составляет __2__ зачетных единиц, __108__ часов.

Очно-заочная форма обучения

№ п/п	Раздел дисциплины	Семестр	Виды учебной работы (в часах)				Оценочные средства для проведения промежуточной аттестации по разделам
			Лекции	Лабораторные работы	КСР	СРС	

1	Основы информационной безопасности.	5	5	6	6	9	Контрольная работа
2	Модели политик безопасности	5	2	4	6	9	Контрольная работа
3	Информационная безопасность АСУТП	5	2	8	6	9	Контрольная работа
	ИТОГО		9	18	18	27	
Форма аттестации							Зачет(4)

5. Содержание лекционных занятий по темам с указанием формируемых компетенций

№ п/п	Раздел дисциплины	Часы	Тема лекционного занятия	Краткое содержание	Индикаторы достижения компетенции
1	Основы информационной безопасности.	6/5	Тема 1. Основные понятия и определения Информационной безопасности.	Информационная безопасность. Стандарт ГОСТ Р 50922-2006. Защита информации. Объект защиты. Цель защиты информации. Система защиты информации. Свойства информации. Субъект, объект доступа. Угрозы безопасности информации и их классификация. Каналы утечки информации.	ОПК-2, ПК-1, ПК-5
			Тема 2. СЗИ от угроз нарушения конфиденциальности	Модель системы защиты. Организационные меры информационной безопасности. Идентификация, авторизация, аутентификация. Методы аутентификации. Разграничение доступа (дискреционный, мандатный). Криптографические методы обеспечения конфиденциальности (симметричные, ассиметричные криптосистемы). Методы защиты внешнего периметра (Межсетевое экранирование, системы обнаружения вторжений). Протоколирование и аудит.	
			Тема 3. СЗИ от угроз нарушения целостности.	Принципы обеспечения целостности. Криптографиче-	

				ские методы обеспечения целостности информации (цифровая подпись, криптографические хэш-функции, коды проверки подлинности).	
			Тема 4. СЗИ от угроз нарушения доступности	Построение систем защиты от угроз нарушения доступности информации	
2	Модели политик безопасности	6/2	Тема 5. Основные понятия политики безопасности	Понятие политики безопасности. Виды политик.	ОПК-2, ПК-1, ПК-5
			Тема 6. Политики безопасности для защиты от несанкционированного доступа.	Политики безопасности для защиты от несанкционированного доступа. Дискреционная и мандатная политики безопасности. Политика безопасности Белла-ЛаПадулла.	
			Тема 7. Политики безопасности для защиты от нарушения целостности информации	Политики безопасности для защиты от нарушения целостности информации. Политика безопасности Биба.	
3	Информационная безопасность АСУТП	6/2	Тема 8. Безопасность периметра сети	Классификация удаленных атак. Методы защиты от них. Использования технологий криптографии для передачи конфиденциального трафика. Технологии VPN. Шифрование данных на сетевом уровне. Применение технологий шифрования данных совместно с межсетевыми экранами. Защищенные протоколы прикладных уровней. SSL, SHTTP. Пакет SSH. Методы защиты электронной почты. Пакет PGP.	ОПК-2, ПК-1, ПК-5
			Тема 9. Защита рабочих станций	Угрозы безопасности операционной системе. Построение системы безопасности в системах с дискреционным доступом.	

				<p>Механизмы разграничения доступа в операционных системах. Идентификация, аутентификация и авторизация субъектов доступа. Аудит доступа.</p> <p>Реализация мандатного доступа в операционных системах. Алгоритмы аутентификации пользователей NTLM и Kerberos</p> <p>Подсистема защиты операционных систем семейства Windows, UNIX.</p> <p>Типовые сценарии атак на операционные системы.</p> <p>Перебор паролей. Атаки, основанные на переполнении буфера. Атаки на доверие. Использование разрушающих программных средств (РПС). Вирусы, сетевые черви, троянские кони. Антивирусная защита информации.</p>	
			Тема 10. Мероприятия по защите ключевых систем информационной инфраструктуры	<p>Последовательность мероприятий по защите КСИИ. Текущее состояние ИБ. Моделирование угроз. Разработка специальных технических требований. ФСТЭК РФ. Правовая защита информации, нормативные документы по безопасности критически важных объектов. Международные стандарты безопасности информационных технологий. Органы лицензирования и сертификации в области защиты информации в РФ. Процедуры лицензирования и сертификации Требования по защите информации.</p>	

6. Содержание практических занятий

Не предусмотрено учебным планом

7. Содержание лабораторных занятий

Цель: получить навыки работы с компьютером по защите информации, владеть методами информационных технологий по информационной безопасности систем управления технологическим процессом.

№ п/п	Раздел дисциплины	Часы	Наименование лабораторной работы	Краткое содержание	Индикаторы достижения компетенции
1	Основы информационной безопасности.	2	Симметричные алгоритмы шифрования	Изучение алгоритмов криптографической защиты информации и особенностей их практической реализации.	ПК – 2.1-2.3
2		2	Ассиметричные алгоритмы шифрования	Изучение алгоритмов криптографической защиты информации и особенностей их практической реализации.	
3		2	Симметричные и асимметричные криптосистемы. Электронно-цифровая подпись	Изучение работы симметричных и асимметричных криптосистем, а также систем установки электронно-цифровой подписи. Познакомиться с организацией защищенного документооборота.	
4	Модели политик безопасности	4	Реализация политик информационной безопасности. Дискреционная модель политики безопасности.	Изучение проблем реализации политик информационной безопасности в компьютерных системах на примере дискреционной модели.	ПК – 2.1-2.3
5	Информационная безопасность АСУТП	2	Работа с реестром	Получение практических навыков выявления вредоносных программ с помощью реестра ОС.	ПК – 2.1-2.3
6		2	Анализ степени защищенности объекта информатизации	Приобретение практических навыков в определении степени защищенности объекта информатизации.	

7		4	Исследование средств защиты информации и идентификации пользователей в ОС	Исследование средств защиты программного обеспечения от несанкционированного использования, исследование защитных механизмов операционной системы.	
---	--	---	---	--	--

Место проведения: учебные лаборатории кафедры без использования специального оборудования

8. Самостоятельная работа

№ п/п	Темы, выносимые на самостоятельную работу	Часы	Форма СРС	Индикаторы достижения компетенции
	Тема 1. Основные понятия и определения Информационной безопасности.	2/3	Проработка лекционного материала	ПК – 2.1-2.3
	Тема 2. СЗИ от угроз нарушения конфиденциальности	2/3	Проработка лекционного материала, расчетно-графическая работа №1	ПК – 2.1-2.3
	Тема 3. СЗИ от угроз нарушения целостности.	2/3	Проработка лекционного материала, расчетно-графическая работа №2	ПК – 2.1-2.3
	Тема 4. СЗИ от угроз нарушения доступности	2/3	Проработка лекционного материала	ПК – 2.1-2.3
	Тема 5. Основные понятия политики безопасности	2/3	Проработка лекционного материала, подготовка реферата	ПК – 2.1-2.3
	Тема 6. Политики безопасности для защиты от несанкционированного доступа.	2/3	Проработка лекционного материала	ПК – 2.1-2.3
	Тема 7. Политики безопасности для защиты от нарушения целостности информации	1	Проработка лекционного материала	ПК – 2.1-2.3
	Тема 8. Безопасность периметра сети	2/3	Проработка лекционного материала, групповая творческая работа №1	ПК – 2.1-2.3
	Тема 9. Защита рабочих станций	2/3	Проработка лекционного материала, групповая творческая работа №2	ПК – 2.1-2.3
	Тема 10. Мероприятия по защите ключевых систем информационной инфраструктуры	1/2	Проработка лекционного материала	ПК – 2.1-2.3

8.1 Контроль самостоятельной работы

№ п/п	Темы, выносимые на самостоятельную работу	Часы	Форма КСР	Индикаторы достижения компетенции
	Тема 1. Основные понятия и определения Информационной безопасности.	2	Проработка лекционного материала	ПК – 2.1-2.3

	Тема 2. СЗИ от угроз нарушения конфиденциальности	2	Проработка лекционного материала, расчетно-графическая работа №1	ПК – 2.1-2.3
	Тема 3. СЗИ от угроз нарушения целостности.	2	Проработка лекционного материала, расчетно-графическая работа №2	ПК – 2.1-2.3
	Тема 4. СЗИ от угроз нарушения доступности	2	Проработка лекционного материала	ПК – 2.1-2.3
	Тема 5. Основные понятия политики безопасности	2	Проработка лекционного материала, подготовка реферата	ПК – 2.1-2.3
	Тема 6. Политики безопасности для защиты от несанкционированного доступа.	2	Проработка лекционного материала	ПК – 2.1-2.3
	Тема 7. Политики безопасности для защиты от нарушения целостности информации	1	Проработка лекционного материала	ПК – 2.1-2.3
	Тема 8. Безопасность периметра сети	2	Проработка лекционного материала, групповая творческая работа №1	ПК – 2.1-2.3
	Тема 9. Защита рабочих станций	2	Проработка лекционного материала, групповая творческая работа №2	ПК – 2.1-2.3
	Тема 10. Мероприятия по защите ключевых систем информационной инфраструктуры	1	Проработка лекционного материала	ПК – 2.1-2.3

9. Использование рейтинговой системы оценки знаний.

При оценке результатов деятельности студентов в рамках дисциплины «Информационная безопасность систем управления» 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 рейтинговой системе.

При изучении дисциплины предусматривается выполнение трех расчетно-графических работ, реферата и двух групповых творческих заданий, за эти контрольные точки студент может получить максимальное кол-во баллов – 100(17б. – 1-я расчетно-графическая работа, 20б – 2-я расчетно-графическая работа, 20б – реферат, 15б - групповая творческая работа№1, 28б – групповая творческая работа №2).

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 «Информационная безопасность систем управления» 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 «Информационная безопасность систем управления» 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>.

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	0,2
Тема 2. СЗИ от угроз нарушения конфиденциальности	Лекция	лекция визуализация	0,2
Тема 3. СЗИ от угроз нарушения целостности.	Лекция	лекция визуализация	0,2
Тема 4. СЗИ от угроз нарушения доступности	Лекция	лекция визуализация	0,2
Тема 5. Основные понятия политики безопасности	Лекция	лекция визуализация	0,2
Тема 6. Политики безопасности для защиты от несанкционированного доступа.	Лекция	лекция визуализация	0,2
Тема 7. Политики безопасности для защиты от нарушения целостности информации	Лекция	лекция визуализация	0,2
Тема 8. Безопасность периметра сети	Лекция	лекция визуализация	0,2
Тема 9. Защита рабочих станций	Лекция	лекция визуализация	0,2
Тема 10. Мероприятия по защите ключевых систем информационной инфраструктуры	Лекция	лекция визуализация	0,2
Симметричные алгоритмы шифрования	Лаб.зан	Метод проектов	0,75
Симметричные и асимметричные криптосистемы. Электронно-цифровая подпись	Лаб.зан	Метод проектов	0,75
Реализация политик информационной безопасности. Дискреционная модель политики безопасности.	Лаб.зан	Метод проектов	0,75
Анализ степени защищенности объекта информатизации	Лаб.зан	Работа в малых группах, метод проектов	0,75
Исследование средств защиты информации и идентификации пользователей в ОС	Лаб.зан	Работа в малых группах, метод проектов	1
Итого:			4

