

Министерство образования и науки Российской Федерации
Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Казанский национальный исследовательский технологический университет»
(ФГБОУ ВО «КНИТУ»)

УТВЕРЖДАЮ
Проректор по УР

А.В. Бурмистров
« 2 »  2017 г.

РАБОЧАЯ ПРОГРАММА

По дисциплине Б1.В.ДВ.8.2 «Защита информации в компьютерных системах»
Направление подготовки 18.03.02 «Энерго- и ресурсосберегающие процессы в химической технологии, нефтехимии и биотехнологии»
Профиль подготовки «Рациональное использование материальных и энергетических ресурсов»
Квалификация выпускника Бакалавр
Форма обучения очная
Институт, факультет Институт пищевых производств и биотехнологии, Факультет пищевых технологий
Кафедра-разработчик рабочей программы Химической кибернетики
Курс, семестр 2, 3

	Часы	Зачетные единицы
Лекции	18	0,5
Практические занятия	—	—
Семинарские занятия	—	—
Лабораторные занятия	36	1
Самостоятельная работа	54	1,5
Форма аттестации	зачет	зачет
Всего	108	3

Казань, 2017 г.

Рабочая программа составлена с учетом требований Федерального государственного образовательного стандарта высшего образования (№ 227 от 12.03.2015г.)

по направлению 18.03.02 «Энерго- и ресурсосберегающие процессы в химической технологии, нефтехимии и биотехнологии»

для профиля «Рациональное использование материальных и энергетических ресурсов», на основании учебного плана (2015г.), год начала подготовки: 2015г., 2016г., 2017г.

Разработчик программы:

старший преподаватель



Понкратов А.С.

Рабочая программа рассмотрена и одобрена на заседании кафедры ХК, протокол от 19.10. 2017г. № 3

И.о. зав. кафедрой



Понкратова С.А.

СОГЛАСОВАНО

Протокол заседания методической комиссии факультета пищевых технологий, реализующего подготовку образовательной программы

от 23.10. 2017г. № 3

Председатель комиссии, профессор



Сироткин А.С.

УТВЕРЖДЕНО

Протокол заседания методической комиссии факультета пищевых технологий, к которому относится кафедра-разработчик РП

от 23.10. 2017г. № 3

Председатель комиссии, профессор



Сироткин А.С.

Начальник УМЦ



Китаева Л.А.

1. Цели освоения дисциплины

Целями освоения дисциплины «Защита информации в компьютерных системах» являются:

- а) формирование компетенций, позволяющих работать с различными источниками информации, информационными ресурсами и технологиями;
- б) приобретение необходимых теоретических знаний по обеспечению защиты информации в компьютерных системах и сетях;
- в) обучение разным методам и средствам обеспечения защиты информации;
- г) формирование у бакалавров знаний и умений, необходимых для управления информационными системами организации.

2. Место дисциплины (модуля) в структуре образовательной программы

Дисциплина «Защита информации в компьютерных системах» относится к вариативной части ООП и формирует у бакалавров по направлению подготовки 18.03.02 «Энерго- и ресурсосберегающие процессы в химической технологии, нефтехимии и биотехнологии» набор знаний, умений, навыков и компетенций.

Для успешного освоения дисциплины бакалавр по направлению подготовки 18.03.02 должен освоить материал предшествующих дисциплин:

- а) «Информатика».

Дисциплина «Защита информации в компьютерных системах» является предшествующей и необходима для успешного усвоения последующих дисциплин:

- а) «Информационные ресурсы и системы»;
- б) «Промышленные сети и системы».

Знания, полученные при изучении дисциплины «Защита информации в компьютерных системах» могут быть использованы при прохождении всех видов практик и выполнении выпускных квалификационных работ по направлению подготовки 18.03.02 «Энерго- и ресурсосберегающие процессы в химической технологии, нефтехимии и биотехнологии».

3. Компетенции обучающегося, формируемые в результате освоения дисциплины

1. ОПК-1 способностью решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности.
2. ОПК-2 способностью использовать основные законы естественнонаучных дисциплин в профессиональной деятельности, применять методы математического анализа и моделирования, теоретического и экспериментального исследования.
3. ПК-3 способностью использовать современные информационные

технологии, проводить обработку информации с использованием прикладных программ и баз данных для расчета технологических параметров оборудования и мониторинга природных сред.

В результате освоения дисциплины обучающийся должен:

1) Знать:

- а) основные принципы защиты информации в компьютерных системах;
- б) состав и методы организационно-правовой защиты информации;
- в) основные методы нарушения секретности, целостности и доступности информации;
- г) современные методы криптографической защиты информации;
- д) комплексные системы защиты информации.

2) Уметь:

- а) применять методы разграничения полномочий пользователей и управления доступом к ресурсам в защищенных операционных системах;
- б) использовать методы и средства криптографической защиты информации;
- в) применять методы и средства защиты от вредоносных программ;
- г) на научной основе организовать свой труд, владеть компьютерными методами сбора, хранения и обработки (редактирования) информации, используемыми в сфере профессиональной деятельности.

3) Владеть:

- а) навыками работы с прикладным программным обеспечением;
- б) основными методами, способами и средствами получения, хранения, переработки информации;
- в) навыками разработки, внедрения, эксплуатации и развития систем и сетей, обеспечивающих деятельность предприятия (организации).

4. Структура и содержание дисциплины «Защита информации в компьютерных системах»

Общая трудоемкость дисциплины составляет 3 зачетные единицы, 108 часа.

[illegible]

5. Содержание лекционных занятий по темам с указанием формируемых компетенций

№ п/п	Раздел дисциплины	Часы	Тема лекционного занятия	Краткое содержание	Формируемые компетенции
1	Общие сведения о защите информации	2	Тема 1. Общие сведения о защите информации.	Понятие национальной безопасности. Виды безопасности: государственная, экономическая, общественная, военная, экологическая, информационная. Роль и место системы обеспечения информационной безопасности в системе национальной безопасности РФ. Угрозы информационной безопасности и их классификация. Основные источники и пути реализации угроз.	ОПК-1, ОПК-2, ПК-3
		2	Тема 2. Правовые основы обеспечения информационно й безопасности (ИБ). Стандарты ИБ.	Виды защищаемой информации. Законодательство в информационной сфере. Доктрина информационной безопасности РФ. Информационно-манипулятивные технологии. Преступления и наказания в сфере высоких технологий. Понятие компьютерных преступлений и их классификация. Стандарты ИБ.	

		2	Тема 3. Вредоносное программное обеспечение	Понятие вредоносной программы, классификация: вирусы, троянские программы, сетевые черви, шифровальщики данных. Антивирусные программы, сетевые экраны и фильтры	
2	Методы и средства обеспечения защищенности информации..	2	Тема 4. Технические и программные средства обеспечения безопасности и информационной защиты.	Понятие инженерно-технических средств ЗИ, свойства, классификация, примеры использования. Аппаратные средства ЗИ: понятия, классификация, примеры использования.	ОПК-1, ОПК-2, ПК-3
		4	Тема 5. Симметричные и ассиметричные криптографические системы	Симметричные системы с секретным ключом. Алгоритмы DES, AES. Ассиметричные системы шифрования с публичным и секретным ключами	
3	Проблемы обеспечения защиты информации в информационных системах	2	Тема 6. Управление безопасностью предприятия. Методология построения защищенных систем и корпоративных сетей.	Понятие канала утечки информации, классификация, примеры. Понятие активного и пассивного подключения к защищаемой КС. Понятие идентификации и аутентификации пользователя. Способы аутентификации пользователей:	ОПК-1, ОПК-2, ПК-3

				парольная, по биометрическим данным. Понятия, примеры применения, принципы построения	
		4	Тема 7. Программно-аппаратные методы защиты в сети.	Межсетевые экраны. Понятие межсетевых экранов. Определение типов межсетевых экранов. Практическая реализация межсетевого экрана FireWall/Plus. Защита на основе маршрутизаторов. Фильтрующий маршрутизатор. Внешние и внутренние маршрутизаторы. Защита электронного обмена данными в Интернете.	

6. Содержание семинарских, практических занятий (лабораторного практикума)

Семинарские, практические занятия учебным планом не предусмотрены.

7. Содержание лабораторных занятий

№ п/п	Раздел дисциплины	Часы	Тема семинара, практического занятия, лабораторного практикума	Формируемые компетенции
1	Общие сведения о защите информации	2	Измерение информации. Классификация способов несанкционированного доступа. Модель нарушителя, уровни возможностей нарушителя	ОПК-1, ОПК-2, ПК-3
		2	Справочно-поисковые системы доступа к правовой информации в области информационной безопасности («Гарант», «Кодекс», «Консультант Плюс» и др.). Разбор примеров.	

		2	Компьютерные вирусы. Обнаружение и «лечение» компьютерных вирусов с помощью антивирусных программ.	
		4	Защита рефератов	
2	Методы и средства обеспечения защищенности информации.	4	Методы аутентификации, использующие пароли и PIN-коды. Аутентификация пользователей Web-систем.	ОПК-1, ОПК-2, ПК-3
		4	Использование программно-технических средств шифрования. Алгоритм AES – симметричного шифрования. Алгоритм RSA – ассиметричного шифрования	
		4	Криптографические методы защиты информации. Изучение принципов шифрования информации с открытым ключом. Проект «Шифровальщик».	
		2	Решение разноуровневых задач.	
3	Проблемы обеспечения защиты информации в информационных системах.	2	Классификация каналов утечки информации.. Понятие активного и пассивного подключения к защищаемой КС, примеры.	ОПК-1, ОПК-2, ПК-3
		2	Основные механизмы реализации удалённых атак. Межсетевые экраны (МЭ). Понятие, области применения, показатели защищенности МЭ. Требования к классам защищённости.	
		4	Защита баз данных на примере MS ACCESS.	
		4	Защита работ в соответствии с творческим заданием.	

8. Самостоятельная работа бакалавра

9.

№ п/п	Темы, выносимые на самостоятельную работу	Часы	Форма СРС	Формируемые компетенции
1	Общие сведения о защите информации	18	Работа с дополнительными источниками информации. Подготовка к лабораторным занятиям.	ОПК-1, ОПК-2, ПК-3

2	Методы и средства обеспечения защищенности информации.	20	Работа с дополнительными источниками информации. Подготовка к лабораторным занятиям. Выполнение индивидуальных заданий.	ОПК-1, ОПК-2, ПК-3
3	Проблемы обеспечения защиты информации в информационных системах.	16	Работа с дополнительными источниками информации. Подготовка к лабораторным занятиям. Выполнение индивидуальных заданий.	ОПК-1, ОПК-2, ПК-3

10. Использование рейтинговой системы оценки знаний

При оценке результатов деятельности бакалавров в рамках дисциплины «Защита информации в компьютерных системах» 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.

Рейтинговая система непрерывного контроля знаний бакалавров позволяет:

- реализовать индивидуальный подход в образовательном процессе;
- развить у бакалавров способность к самоорганизации и самообразованию;
- сформировать рейтинг бакалавров по степени освоения компетенций, включающих, как учебные результаты (знания, умения, навыки), так и личностные качества (дисциплина, ответственность, инициатива и др.).

Итоговая сумма баллов по дисциплине за семестр, где предусмотрен зачет

Оценка	Итоговая сумма баллов	Оценка (ECTS)
отлично	87-100	A (отлично)
хорошо	83-86	B (очень хорошо)
	78-82	C (хорошо)
	74-77	D (удовлетворительно)
удовлетворительно	68-73	
	60-67	E (посредственно)
неудовлетворительно	ниже 60 баллов	F (неудовлетворительно)

По дисциплине «Защита информации в компьютерных системах» предусмотрены следующие оценочные средства текущей и промежуточной аттестации:

1. Реферат.
2. Разноуровневые задачи и задания.
3. Творческое задание.

Подготовка и защита реферата на заданную тему. В течение семестра обучающийся должен подготовить один реферат, сопровождающийся докладом с презентацией. Оценивается оригинальность подобранного материала, объем, полнота и уровень выполненной работы, качество оформления, уровень защиты реферата.

Выполнение расчетных работ на лабораторных занятиях. Работа оценивается, если она выполнена обучающимся лично, самостоятельно и без помощи преподавателя. Оценивается качество выполненной работы и достигнутые результаты.

Творческое задание – частично регламентированное задание, имеющее нестандартное решение и позволяющее диагностировать умения, владения интегрировать знания различных областей, аргументировать собственную точку зрения. Может выполняться в индивидуальном порядке или группой обучающихся.

На промежуточной аттестации оценивается полнота сформированных компетенций студента (см. таблицу).

Оценочные средства	Кол-во	Min, баллов	Max, баллов
Реферат	1	18	30
Разноуровневые задачи и задания	2	18	30
Творческое задание	1	24	40
Итоговая работа		60	100

10. Информационно-методическое обеспечение дисциплины

10.1. Основная литература

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

Основные источники информации	Количество экземпляров
1. Шаньгин В.Ф. Защита информации в компьютерных системах компьютерных систем и сетей: учебное пособие. – М.: ИД "ФОРУМ": ИНФРА-М ", 2017. – 416 с.	ЭБС «Znanium.com» http://znanium.com/go.php?id=775200 Доступ с любой точки интернет после регистрации с IP-адресов КНИТУ
2. Баранова Е.К. Защита информации в компьютерных системах и защита информации: учебное пособие. – 3-е изд. – М.: ИЦ «РИОР»: ИНФРА-М, 2017. – 322 с.	ЭБС «Znanium.com» http://znanium.com/go.php?id=763644 Доступ с любой точки интернет после регистрации с IP-адресов КНИТУ
3. Защита информации в компьютерных системах и защита информации: Учебник / П. Н. Башлы, А. В. Бабащ, Е. К. Баранова. – М.: РИОР, 2013. – 222 с.	ЭБС «Znanium.com» http://znanium.com/go.php?id=405000 Доступ с любой точки интернет после регистрации с IP-адресов КНИТУ
4. Бабащ А.В. Защита информации в компьютерных системах. Практикум (+CD) (для бакалавров) / А.В. Бабащ, Е.К. Баранова, Ю.Н. Мельников. – М.: КноРус, 2016. – 131 с.	ЭБС «Book.ru» http://www.book.ru/book/918700 Доступ с любой точки интернет после регистрации с IP-адресов КНИТУ
5. Кирпичников, А. П. Криптографические методы защиты компьютерной информации: учебное пособие / А. П. Кирпичников, З. М. Хайбуллина; Казан. нац. исслед. технол. ун-т. – Казань : Изд-во КНИТУ, 2016. – 100 с.	66 экз. в УНИЦ КНИТУ http://ft.kstu.ru/ft/Kirpichnikov-Kriptograficheskie_metody_zashchity.pdf Доступ с IP-адресов КНИТУ

10.2. Дополнительная литература

В качестве дополнительных источников информации рекомендуется использовать следующую литературу:

Дополнительные источники информации	Количество экземпляров
1. Бирюков, А.А. Защита информации в компьютерных системах: защита и нападение / Бирюков А.А. – М.: ДМК-пресс, 2012. – 474 с.	ЭБС «Консультант студента» http://www.studentlibrary.ru/book/ISBN9785940746478.html Доступ с любой точки интернет после регистрации с IP-адресов КНИТУ

2. Гришина Н.В. Информационная безопасность предприятия: учеб. пособие для студ. вузов. – 2-е изд., доп. – М.: Форум : Инфра-М, 2015. – 239 с.	5 экз. в УНИЦ КНИТУ
3. Девянин П.Н. Модели безопасности компьютерных систем. Управление доступом и информационными потоками: учеб. пособие для студ. вузов. – М.: Горячая линия – Телеком, 2011. – 319 с.	20 экз. в УНИЦ КНИТУ
4. Малюк А. А. Введение в информационную безопасность: учеб. пособие / под ред. В.С. Горбатова. – М.: Горячая линия - Телеком, 2011. – 288 с.	20 экз. в УНИЦ КНИТУ
5. Баранова Е.К. Моделирование системы защиты информации: Практикум : учебное пособие.– 2-е изд., перераб. и доп. – М.: ИЦ РИОР: ИНФРА-М, 2016. – 224 с.	ЭБС «Znanium.com» http://znanium.com/go.php?id=549914 Доступ с любой точки интернет после регистрации с IP-адресов КНИТУ
6. Михельсон, К.К. Информационное право. Конспект лекций: учебное пособие / Михельсон К.К. – М.: Проспект, 2016. – 144с.	ЭБС «Консультант студента» http://www.studentlibrary.ru/book/ISBN9785392195244.html Доступ с любой точки интернет после регистрации с IP-адресов КНИТУ
7. Климентьев, К.Е. Компьютерные вирусы и антивирусы: взгляд программиста / Климентьев К.Е. – М.: ДМК-пресс, 2013. – 656 с.	ЭБС «Консультант студента» http://www.studentlibrary.ru/book/ISBN9785940748854.html Доступ с любой точки интернет после регистрации с IP-адресов КНИТУ

10.3. Электронные источники информации

При изучении дисциплины «Защита информации в компьютерных системах» в качестве электронных источников информации, рекомендуется использовать следующие источники:

Электронный каталог УНИЦ КНИТУ – Режим доступа:

<http://ruslan.kstu.ru>

Электронная библиотека УНИЦ КНИТУ – Режим доступа:

<http://ft.kstu.ru/ft/>

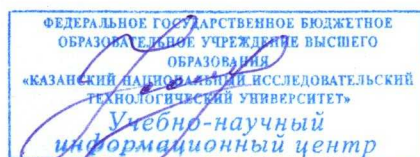
ЭБС «Znanium.com» – Режим доступа: <http://www.znanium.com>

ЭБС «Book.ru» » – Режим доступа: <http://www.book.ru>

ЭБС «Консультант студента» – Режим доступа: <http://www.studentlibrary.ru>

Согласовано:

Зав. сектором ОКУФ



11. Оценочные средства для текущего контроля успеваемости, промежуточной аттестации по итогам освоения дисциплины

Для проведения текущего контроля успеваемости и промежуточной аттестации студентов на соответствие их достижений планируемым результатам обучения по дисциплине «Защита информации в компьютерных системах» разработаны фонды оценочных средств (ФОС), которые являются составной частью рабочей программы по дисциплине «Защита информации в компьютерных системах» и оформлены отдельным документом в соответствии с положением о фонде оценочных средств по дисциплине (модулю).

12. Материально-техническое обеспечение дисциплины (модуля).

В качестве материально-технического обеспечения дисциплины используются:

- для проведения лекционных занятий – аудитория, оснащенная мультимедийным оборудованием (проектор, экран, колонки) для чтения лекций-презентаций;
- для проведения лабораторных занятий – компьютерные классы кафедры ХК, оснащенные современным оборудованием;
- для самостоятельной работы – компьютерные классы, подключенные к сети «Интернет» с обеспечением доступа в электронную информационно-образовательную среду ФГБОУ ВО «КНИТУ», представленную ресурсами сайта университета <http://www.kstu.ru>;
- методические пособия/указания для выполнения лабораторных заданий;
- лицензионный доступ к ЭБС, БД и отдельным электронным версиям изданий из любой точки Интернет после регистрации с компьютеров ФГБОУ ВО «КНИТУ»;
- лицензионное программное обеспечение: ПО Microsoft по программе DreamSpark, бывшая MSDN; Windows 7 Version 1511; MS Office 2010-2016 Standard.

13. Образовательные технологии

Основные интерактивные формы и удельный вес занятий, проводимых в интерактивных формах, приведены в таблице:

Дисциплина	Интерактивные часы				Образовательные технологии
	Всего	Лек.	Лаб.	Практ.	
Б1.В.ДВ.8.2 «Защита информации в компьютерных системах»	18	6	12	–	Творческие задания. Компьютерная симуляция. Работа в малых группах.

Лист переутверждения рабочей программы

Рабочая программа по дисциплине

«Б1.В.ДВ.8.2 Защита информации в компьютерных системах»

пересмотрена на заседании кафедры

химической кибернетики, ФПТ, ФГБОУ ВО «КНИТУ»

№ п/п	Дата переутверждения РП (протокол заседания кафедры № от 20)	Наличие изменений	Наличие изменений в списке литературы*	Подпись разработ- чика РП	Подпись заведующего кафедрой	Подпись начальника УМЦ/ОМг/ ОАиД
1	№1 от 29.08.2018	нет	нет			

*Если в списке литературы есть изменения, обновленный список необходимо утвердить у заведующей сектором комплектования УНИЦ и один экземпляр представить в УМЦ/ОМг/ОАиД.