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_» _ноября_____2017 г.

РАБОЧАЯ ПРОГРАММА

По дисциплине Б1.В.ДВ.8.1 «Основы информационной безопасности»
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 «Основы информационной безопасности» являются:

а) формирование компетенций, позволяющих соблюдать в профессиональной деятельности требования правовых актов в области защиты государственной тайны и информационной безопасности;

б) обучение технологиям обеспечения информационной безопасности в области управления объектами различного уровня, которые связаны с информационными технологиями, используемыми на этих объектах;

в) обучение основным этапам решения задач информационной безопасности;

г) формирование компетенций, позволяющих проводить информационно-поисковую работу с последующим использованием данных при решении профессиональных задач.

2. Место дисциплины (модуля) в структуре образовательной программы

Дисциплина «Основы информационной безопасности» 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 «Основы информационной безопасности» является предшествующей и необходима для успешного усвоения последующих дисциплин:

а) «Информационные ресурсы и системы»;

б) «Промышленные сети и системы».

Знания, полученные при изучении дисциплины «Основы информационной безопасности» 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) политику безопасности, сущность информационной безопасности информационных систем;

б) состав и методы организационно-правовой защиты информации;

в) методы антивирусной защиты информации;

г) современные методы криптографической защиты информации;

д) процедуры аутентификации данных и постановки электронной цифровой подписи.

2) Уметь:

а) применять организационно-правовые методы защиты информации в информационных системах;

б) обеспечивать антивирусную защиту информации;

в) использовать методы и средства криптографической защиты информации;

г) применять методы разграничения полномочий пользователей и управления доступом к ресурсам в защищенных операционных системах.

3) Владеть:

а) приемами антивирусной защиты и информационной защиты;

б) основными методами, способами и средствами получения, хранения, переработки информации;

в) методами анализа и оценки состояния обеспечения информационной безопасности в учреждении.

4. *Структура и содержание дисциплины «Основы информационной безопасности»*

Общая трудоемкость дисциплины составляет 3 зачетные единицы, 108 часа.

№ п/п	Раздел дисциплины	Семестр	Виды учебной работы (в часах)				Оценочные средства для проведения промежуточной аттестации по разделам
			Лекции	Семинар (Практические занятия, лабораторные практикумы)	Лабораторные работы	СРС	
1	Основы информационной безопасности. Стандарты информационной безопасности.	3	4	–	8	10	Реферат
2	Проблемы защиты информации. Несакционированный доступ (НСД) к информации.	3	4	–	10	16	Коллоквиум
3	Построение систем защиты от угроз нарушения конфиденциальности информации	3	6	–	12	16	Разноуровневые задачи и задания
4	Программно-аппаратные методы защиты компьютерных систем и сетей	3	4	–	6	12	Творческое задание
Форма аттестации							Зачет

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

№ п/п	Раздел дисциплины	Часы	Тема лекционного занятия	Краткое содержание	Формируемые компетенции
1	Основы информационной безопасности. Стандарты информационной безопасности.	2	Тема 1. Основы информационной безопасности.	Понятие национальной безопасности. Виды безопасности: государственная, экономическая, общественная, военная,	ОПК-1, ОПК-2, ПК-3

				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. Задачи информационной безопасности.	
		2	Тема 2. Стандарты информационной безопасности.	Классификация стандартов. «Оранжевая книга» Министерства Обороны США. Европейские критерии безопасности информационных технологий. Руководящие документы ФСТЭК РФ. Федеральные критерии безопасности информационных технологий.	
2	Проблемы защиты информации. Несакционированный доступ (НСД) к информации.	2	Тема 3. Несакционированный доступ (НСД) к информации.	Несанкционированный доступ к информации и его цели. Способы НСД к информации через технические средства. Способы НСД к компьютерам, сетевым ресурсам и программному обеспечению.	ОПК-1, ОПК-2, ПК-3
		2	Тема 4. Вредоносное программное обеспечение.	Понятие вредоносного программного обеспечения.	

				Компьютерные вирусы. Классификация компьютерных вирусов. Признаки проявления и способы заражения вирусами. Классификация и сравнительный анализ систем антивирусной защиты.	
3	Построение систем защиты от угроз нарушения конфиденциальности информации	2	Тема 5. Основные положения и определения криптографии. Криптографические методы защиты информации.	Основные понятия: криптография, криптоанализ, криптология, шифр, вскрытие шифра, стойкость шифра, ключ. Классификация криптографических методов	ОПК-1, ОПК-2, ПК-3
		2	Тема 6. Симметричные и ассиметричные криптосистемы.	Шифры: Подстановки. Перестановки. Гаммирование. Блочные шифры. Алгоритмы DES, AES, ГОСТ 28147-89. Системы с открытым ключом. Алгоритм RSA. Криптосистема Эль-Гамаля.	
		2	Тема 7. Электронная цифровая подпись.	Электронная цифровая подпись. Криптографические методы обеспечения целостности информации (криптографические хэш-функции, коды проверки подлинности). Электронная подпись на основе алгоритма RSA. Цифровая сигнатура.	
4	Программно-аппаратные методы защиты	2	Тема 8. Защита информации	Межсетевые экраны. Понятие межсетевых экранов. Определение типов	ОПК-1, ОПК-2, ПК-3

	компьютерных систем и сетей		компьютерных систем и сетей.	межсетевых экранов. Практическая реализация межсетевого экрана FireWall/Plus. Защита на основе маршрутизаторов. Фильтрующий маршрутизатор. Внешние и внутренние маршрутизаторы.	
		2	Тема 9. Обеспечение информационной безопасности в Интернет.	Правовая защита Интернет сайта. Способы защиты сетевых соединений SSL, TLS. Технические средства и методы защиты web-ресурсов.	

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	Основы информационной безопасности. Стандарты информационной безопасности.	4	Доктрина информационной безопасности РФ. Иформационно-манипулятивные технологии.	ОПК-1, ОПК-2, ПК-3
		4	Правовое обеспечение информационной безопасности. Разбор нормативно-правовых актов.	
2	Проблемы защиты информации. Несакционированный доступ (НСД) к информации.	4	Изучение программных средств защиты от несанкционированного доступа и разграничения прав пользователей.	ОПК-1, ОПК-2, ПК-3
		4	Классификация вредоносного программного обеспечения: TrojWare, VirWare, MalWare. Компьютерные вирусы. Жизненный цикл компьютерных вирусов. Примеры конкретных видов вирусов и вирусных атак.	
		2	Применение и настройка антивирусных программ.	

3	Построение систем защиты от угроз нарушения конфиденциальности информации	4	Разработка алгоритмов и программирование симметричных шифров	ОПК-1, ОПК-2, ПК-3
		4	Разработка алгоритмов и программирование асимметричных шифров	
		4	Применение ЭЦП. Подпись и верификация электронных документов.	
4	Программно-аппаратные методы защиты компьютерных систем и сетей	2	Защита на основе маршрутизаторов. Фильтрация трафика. Виртуальные частные сети.	ОПК-1, ОПК-2, ПК-3
		4	Методы защиты авторской продукции в сети. Способы защиты сетевого контента – правовой и технический подходы. Цифровая стеганография.	

8. Самостоятельная работа бакалавра

№ п/п	Темы, выносимые на самостоятельную работу	Часы	Форма СРС	Формируемые компетенции
1	Основы информационной безопасности. Стандарты информационной безопасности.	10	Работа с дополнительными источниками информации. Подготовка к лабораторным занятиям.	ОПК-1, ОПК-2, ПК-3
2	Проблемы защиты информации. Несакционированный доступ (НСД) к информации.	16	Работа с дополнительными источниками информации. Подготовка к лабораторным занятиям.	ОПК-1, ОПК-2, ПК-3
3	Построение систем защиты от угроз нарушения конфиденциальности информации	16	Работа с дополнительными источниками информации. Подготовка к лабораторным занятиям.	ОПК-1, ОПК-2, ПК-3
4	Программно-аппаратные методы защиты компьютерных систем и сетей	12	Работа с дополнительными источниками информации. Подготовка к лабораторным занятиям.	ОПК-1, ОПК-2, ПК-3

9. Использование рейтинговой системы оценки знаний

При оценке результатов деятельности бакалавров в рамках дисциплины «Основы 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.

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

По дисциплине «Основы информационной безопасности» предусмотрены следующие оценочные средства текущей и промежуточной аттестации:

1. Реферат.
2. Коллоквиум.
3. Разноуровневые задачи и задания.
4. 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.

Коллоквиум – форма проверки знаний в письменной форме по теоретическому разделу. Оценивается углубление знаний при помощи использования дополнительных материалов при подготовке к коллоквиуму.

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 (зачете) оценивается полнота сформированных компетенций студента (см. таблицу).

Оценочные средства	**Кол-во**	**Min, баллов**	**Max, баллов**
Реферат	1	12	20
Коллоквиум	1	12	20
Разноуровневые задачи и задания	4	18	30
Творческое задание	1	18	30
Итоговая работа		60	100

10. Информационно-методическое обеспечение дисциплины

10.1. Основная литература

При изучении дисциплины «Основы информационной безопасности» в качестве основных источников информации рекомендуется использовать следующую литературу.

Основные источники информации	Количество экземпляров
1. Шаньгин В.Ф. Основы информационной безопасности 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. Основы информационной безопасности 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. Основы информационной безопасности и защита информации: Учебник / П. Н. Башлы, А. В. Бабаш, 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. Бабаш А.В. Основы информационной безопасности. Практикум (+CD) (для бакалавров) / А.В. Бабаш, 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. Основы информационной безопасности: 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: / 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 «Основы информационной безопасности» 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 «Основы информационной безопасности» разработаны фонды оценочных средств (ФОС), которые являются составной частью рабочей программы по дисциплине «Основы информационной безопасности» 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.ОД.18 «Основы информационной безопасности»	18	6	12	–	Творческие задания. Компьютерная симуляция. Работа в малых группах.

Приложение 4

Лист переутверждения рабочей программы

Рабочая программа по дисциплине
«Б1.В.ДВ.8.1 Основы информационной безопасности »
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.*