

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ  
**БАШКИРСКИЙ ИНСТИТУТ ТЕХНОЛОГИЙ И УПРАВЛЕНИЯ (ФИЛИАЛ)**  
ФЕДЕРАЛЬНОГО ГОСУДАРСТВЕННОГО БЮДЖЕТНОГО ОБРАЗОВАТЕЛЬНОГО  
УЧРЕЖДЕНИЯ ВЫСШЕГО ОБРАЗОВАНИЯ  
**«МОСКОВСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ  
ТЕХНОЛОГИЙ И УПРАВЛЕНИЯ ИМЕНИ К.Г. РАЗУМОВСКОГО  
(ПЕРВЫЙ КАЗАЧИЙ УНИВЕРСИТЕТ)»**  
(БИТУ (филиал) ФГБОУ ВО «МГУТУ им. К.Г. Разумовского (ПКУ)»)

**Кафедра «Информационные технологии и системы управления»**



**Рабочая программа дисциплины**

**Б1.В.ДВ.06.01 – АППАРАТНЫЕ СРЕДСТВА ЗАЩИТЫ ТЕХНИЧЕСКОЙ  
ИНФОРМАЦИИ НА ПРЕДПРИЯТИЯХ ПИЩЕВОЙ  
ПРОМЫШЛЕННОСТИ**

Направление подготовки 15.03.04 Автоматизация технологических процессов и производств

Тип образовательной программы прикладной бакалавриат

Направленность (профиль) подготовки Автоматизация технологических процессов и производств в пищевой промышленности и отраслях агропромышленного комплекса

Квалификация выпускника – бакалавр

Форма обучения заочная

Год набора 2020

Мелеуз 2023 г.

Рабочая программа дисциплины **«Аппаратные средства защиты технической информации на предприятиях пищевой промышленности»** разработана на основании федерального государственного образовательного стандарта высшего образования по направлению подготовки **15.03.04 Автоматизация технологических процессов и производств (бакалавриат)**, утвержденного приказом Министерства образования и науки Российской Федерации от 12.03.2015 № 200, учебного плана по основной профессиональной образовательной программе **высшего образования «Автоматизация технологических процессов и производств»**

Рабочая программа дисциплины разработана группой в составе:  
к.т.н. Колязов К.А., к.п.н. Одиноква Е.В., к.ф.-м.н. Смирнов Д.Ю., к.п.н. Тучкина Л.К., к.п.н. Яшин Д.Д., ст. преподаватель Остапенко А.Е.

Руководитель основной профессиональной образовательной программы  
кандидат педагогических наук, доцент

  
\_\_\_\_\_  
(подпись)

Е.В. Одиноква

Рабочая программа дисциплины обсуждена и утверждена на заседании кафедры  
«Информационные технологии и системы управления»

Протокол № 11 от «29» июня 2023 года

И.о. заведующего кафедрой  
к.п.н., доцент

  
\_\_\_\_\_  
(подпись)

Е.В. Одиноква

## Оглавление

1. Цели и задачи дисциплины .....	4
2. Место дисциплины в структуре ОПОП .....	4
3. Требования к результатам освоения дисциплины .....	4
4. Объем дисциплины и виды учебной работы .....	6
5. Содержание дисциплины.....	6
5.1. Содержание разделов и тем дисциплины .....	6
5.2 Разделы дисциплины и междисциплинарные связи с обеспечиваемыми (последующими) дисциплинами .....	7
5.3. Разделы и темы дисциплины и виды занятий .....	8
6. Перечень семинарских, практических занятий и лабораторных работ .....	9
6.1. План самостоятельной работы студентов.....	9
6.2. Методические указания по организации самостоятельной работы студентов .....	11
7. Примерная тематика курсовых работ (проектов) .....	11
8. Учебно-методическое и информационное обеспечение дисциплины .....	11
9. Материально-техническое обеспечение дисциплины: .....	12
10. Образовательные технологии.....	13
11. Оценочные средства.....	13
12. Организация образовательного процесса для лиц с ограниченными возможностями ..	17
13. Лист регистрации изменений .....	18

**1. Цели и задачи дисциплины «Аппаратные средства защиты технической информации на предприятиях пищевой промышленности»:** формирование компетентности в области разработки и эксплуатации автоматизированных систем в защищенном исполнении. отдельных компонентов автоматизированных систем управления, с учетом требований нормативно - технической и методической документации по обеспечению безопасности информации.

***Задачи изучения дисциплины:***

- изучение основных угроз безопасности информации в автоматизированных системах и освоение аппаратных методов защиты от данных угроз;
- изучение методов, алгоритмов, аппаратных средств обеспечения информационной безопасности автоматизированных систем;
- изучение современных технологий защищенных сетей передачи данных в автоматизированных системах.

**2. Место дисциплины в структуре ОПОП:**

Дисциплина является предметом по выбору вариативной части, предусмотренной учебным планом.

*Предварительные компетенции*, сформированные у обучающегося до начала изучения дисциплины:

- способностью к абстрактному мышлению, анализу, синтезу (ПК -23);
- готовностью к саморазвитию, самореализации, использованию творческого потенциала (ПК - 23);
- готовностью к коммуникации в устной и письменной формах на русском и иностранном языках для решения задач профессиональной деятельности (ПК -23);
- способностью разрабатывать (на основе действующих стандартов) методические и нормативные документы, техническую документацию в области автоматизации технологических процессов и производств, в том числе жизненному циклу продукции и ее качеству, руководить их созданием (ПК -23).
- Освоение дисциплины является основой для последующего изучения дисциплин:
- Эргономика и надежность автоматизированных систем;
- Преддипломная практика;
- Выпускная квалификационная работа.

**3. Требования к результатам освоения дисциплины:**

Процесс изучения дисциплины направлен на формирование следующих компетенций:

способностью выполнять работы по наладке, настройке, регулировке, опытной проверке, регламентному техническому, эксплуатационному обслуживанию оборудования, средств и систем автоматизации, контроля, диагностики, испытаний и управления, средств программного обеспечения, сертификационным испытаниям изделий (ПК-23).

В результате изучения дисциплины студент должен:

***Знать:***

- виды, функции и требования к современным средствам аппаратной аутентификации пользователей в клиент-серверных приложениях;
- методы и аппаратные средства защиты программного обеспечения от несанкционированного изучения, копирования и модификации;
- методы и алгоритмы управления и генерации ключей и их аппаратно-программная реализация и применение в автоматизированных системах;
- принципы построения безопасных автоматизированных рабочих мест и вычислительных сетей с использованием аппаратных комплексов.

**Уметь:**

- разворачивать и настраивать аппаратные средства для защиты локальных и распределенных вычислительных систем;
- обеспечивать надежную аутентификацию и управление доступом к информационным ресурсам с учетом требований нормативно-технической документации;
- настраивать каналы безопасного обмена информацией в локальных и распределенных автоматизированных системах.

**Владеть:**

- инструментарием, обеспечивающим аппаратную защиту информационных ресурсов от изучения, модификации и копирования;
- аппаратными комплексами управления ключами, сертификатами и правами пользователей в защищенных автоматизированных системах.

**Перечень планируемых результатов обучения по дисциплине, соотнесенных с планируемыми результатами освоения образовательной программы**

Процесс изучения дисциплины «Аппаратные средства защиты технической информации на предприятиях пищевой промышленности» направлен на формирование у обучающихся по программе высшего образования – программе бакалавриата – по направлению подготовки 15.03.04 Автоматизация технологических процессов и производств, направленность (профиль) «Автоматизация технологических процессов и производств в пищевой промышленности и отраслях агропромышленного комплекса» профессиональных компетенций ПК-23.

<b>Код и описание компетенции</b>	<b>Планируемые результаты обучения по дисциплине</b>
ПК-23 - способностью выполнять работы по наладке, настройке, регулировке, опытной проверке, регламентному техническому, эксплуатационному обслуживанию оборудования, средств и систем автоматизации, контроля, диагностики, испытаний и управления, средств программного обеспечения, сертификационным испытаниям изделий	<b>Знает:</b> методы и аппаратные средства защиты программного обеспечения от несанкционированного изучения, копирования и модификации; методы и алгоритмы управления и генерации ключей и их аппаратно-программная реализация и применение в автоматизированных системах; принципы построения безопасных автоматизированных рабочих мест и вычислительных сетей с использованием аппаратных комплексов
	<b>Умеет:</b> разворачивать и настраивать аппаратные средства для защиты локальных и распределенных вычислительных систем; обеспечивать надежную аутентификацию и управление доступом к информационным ресурсам с учетом требований нормативно-технической документации; настраивать каналы безопасного обмена информацией в локальных и распределенных автоматизированных системах
	<b>Владеет:</b> инструментарием, обеспечивающим аппаратную защиту информационных ресурсов от изучения, модификации и копирования; аппаратными комплексами управления ключами, сертификатами и правами пользователей в защищенных автоматизированных системах

#### 4. Объем дисциплины и виды учебной работы

##### Заочная форма обучения

Вид учебной работы	Всего часов / зачетных единиц	Семестры			
		8			
<b>Аудиторные занятия* (контактная работа)</b>	10	10			
В том числе:					
Лекции	2	2			
Практические занятия (ПЗ)	4	4			
Семинары (С)					
Лабораторные работы (ЛР)	4	4			
<b>Самостоятельная работа* (всего)</b>	130	130			
В том числе:					
Курсовой проект (работа)					
Расчетно-графические работы					
Реферат (при наличии)					
<i>Другие виды самостоятельной работы</i>					
Вид промежуточной аттестации (зачет с оценкой)	4	4			
Общая трудоемкость	часы	144	144		
	зачетные единицы	4	4		

\* для обучающихся по индивидуальному учебному плану количество часов контактной и самостоятельной работы устанавливается индивидуальным учебным планом<sup>1</sup>.

Дисциплина реализуется посредством проведения учебных занятий (включая проведение текущего контроля успеваемости и промежуточной аттестации обучающихся). В соответствии с рабочей программой и тематическим планом изучение дисциплины проходит в форме контактной работы обучающихся с преподавателем и самостоятельной работы обучающихся. При реализации дисциплины предусмотрена аудиторная контактная работа и внеаудиторная контактная работа посредством электронной информационно-образовательной среды. Учебный процесс в аудитории осуществляется в форме лекций и практических занятий. В лекциях раскрываются основные темы изучаемого курса, которые входят в рабочую программу. На практических занятиях более подробно изучается программный материал в плоскости отработки практических умений и навыков и усвоения тем. Внеаудиторная контактная работа включает в себя проведение текущего контроля успеваемости в электронной информационно-образовательной среде.

#### 5. Содержание дисциплины

##### 5.1. Содержание разделов и тем дисциплины

##### Раздел 1. Безопасность локальных вычислительных систем (ПК-23).

**Тема 1. Предмет и задачи аппаратной защиты информации.** Цели. Задачи и содержание курса. Основные понятия. Предмет и задачи аппаратной защиты информации.

для обучающихся по индивидуальному учебному плану - учебному плану, обеспечивающему освоение соответствующей образовательной программы на основе индивидуализации ее содержания с учетом особенностей и образовательных потребностей конкретного обучающегося (в том числе при ускоренном обучении, для обучающихся с ограниченными возможностями здоровья и инвалидов, для лиц, зачисленных для продолжения обучения в соответствии с частью 5 статьи 5 Федерального закона от 05.05.2014 №84-ФЗ «Об особенностях правового регулирования отношений в сфере образования в связи с принятием в Российскую Федерацию Республики Крым и образованием в составе Российской Федерации новых субъектов - Республики Крым и города федерального значения Севастополя и о внесении изменений в Федеральный закон «Об образовании в Российской Федерации»).

Автоматизированная система (АС). Структура и компоненты АС. Сети ЭВМ. Электронный Документ (ЭД). Виды информации в КС. Информационные потоки в КС. Уязвимость компьютерных систем. Понятие доступа, субъект и объект доступа. Понятие несанкционированного Доступа (НСД). Классы и виды НСД. Несанкционированное копирование программ как особый ВИД НСД. Политика безопасности в компьютерных системах. Оценка защищенности. Способы защиты конфиденциальности целостности и доступности в КС. Стандарты и рекомендации по оценке защищенности от НСД.

**Тема 2. Аутентификация и идентификации пользователя.** Идентификация субъекта. Понятие протокола идентификации. Локальная и удаленная идентификация. Понятие идентифицирующей информации, Способы хранения идентифицирующей информации. Связь с ключевыми системами. Аппаратные средства аутентификации: биометрические, пассивные и активные устройства. Сетевая аутентификация в корпоративных системах. Управление сертификатами Kerberos. Протокол LDAP. Инфраструктура управления ключами PKI.

**Тема 3. Средства аппаратной защиты информации.** Принципы работы и функционал СЗИ. Обеспечение безопасной загрузки операционной системы и верификация модулей. Централизованное управление. Интеграция В существующую автоматизированную систему предприятия. Средства, сертифицированные ФСТЭК. Примеры СЗИ: БлокХост, Аккорд, Соболев.

**Тема 4. Системы обнаружения и предотвращения вторжений. IDS/IPS.** Алгоритмы интеллектуального анализа сетевой и локальной активности, выявляющие нестандартный обмен информацией. Пассивное и активное обнаружение атак. Прмеры систем предотвращения вторжений: Microsoft TMG. Snort. Интеграция IDS/IPS с антивирусами В распространенных программных пакетах обеспечения сетевой безопасности.

## **Раздел 2. Средства обеспечения информационной безопасности распределенных информационных систем (ПК-23).**

**Тема 1. Виртуализация и облачные технологии.** Виртуальные среды и машины: уровень интеграции виртуальной системы и совместное использование ресурсов хост—машины. Кластеры. Облачные технологии SaaS, PaaS, IaaS и прочие. Размещение вычислительных ресурсов организации в коммерческих и свободных облачных хостингах. Экономические и правовые вопросы использования облачных технологий. Вопросы безопасности данных в виртуальных и облачных средах. Виртуальные частные сети (VPN). Программные и аппаратные средства создания VPN и VLAN.

**Тема 2. Аппаратные криптошлюзы.** Аппаратные криптошлюзы. Доступ удаленного пользователя в локальную сеть организации. Связь разбросанных филиалов организации в единую сеть. Организация межкорпоративного сетевого портала для ведения совместного проекта. Защищенный серфинг. криптографическая защита данных, передаваемых по каналам связи сетей общего пользования между составными частями VPN. Настройка приоритетов трафика. Маршрутизация трафика. Протоколирование сетевой активности. Блокировка трафика.

### **5.2 Разделы дисциплины и междисциплинарные связи с обеспечиваемыми (последующими) дисциплинами**

№ п/п	Наименование обеспечиваемых (последующих) дисциплин	№ разделов и тем данной дисциплины, необходимых для изучения обеспечиваемых (последующих) дисциплин (вписываются разработчиком)								
1.	Эргономика и надежность автоматизированных систем	1.1	1.2	1.3	1.4	2.1	2.2			

2.	Преддипломная практика	1.1	1.2	1.3	1.4	2.1	2.2			
3.	Выпускная квалификационная работа	1.1	1.2	1.3	1.4	2.1	2.2			

### 5.3. Разделы и темы дисциплины и виды занятий Заочная форма обучения

№ п/п	Наименование раздела	Наименование темы	Виды занятий в часах				
			Лекции	Практические занятия	Лабораторные занятия	СРС	Всего
1.	Безопасность локальных вычислительных систем	Предмет и задачи аппаратной защиты информации	1			23	24
2.	Безопасность локальных вычислительных систем	Аутентификация и идентификации пользователя		1		22	23
3.	Безопасность локальных вычислительных систем	Средства аппаратной защиты информации			2	21	23
4.	Безопасность локальных вычислительных систем	Системы обнаружения и предотвращения вторжений. IDS/IPS		2		21	23
5.	Средства обеспечения информационной безопасности распределенных информационных систем	Виртуализация и облачные технологии	1		2	21	24
6.	Средства обеспечения информационной безопасности распределенных информационных систем	Аппаратные криптошлюзы		1		22	23

### 5.4 Формы учебных занятий с использованием активных и интерактивных технологий обучения

№	Наименование разделов (тем), в которых используются активные и/или интерактивные образовательные технологии	Образовательные технологии
1.	Предмет и задачи аппаратной защиты информации	Лекция визуализация, Защита лабораторных работ
2.	Аутентификация и идентификации пользователя	Лекция визуализация, Защита лабораторных работ
3.	Средства аппаратной защиты информации	Лекция визуализация, Защита лабораторных работ
4.	Системы обнаружения и предотвращения вторжений. IDS/IPS	Лекция визуализация, Защита лабораторных работ
5.	Виртуализация и облачные технологии	Лекция визуализация,

		Защита лабораторных работ
6.	Аппаратные криптошлюзы	Лекция визуализация, Защита лабораторных работ

**6. Перечень семинарских, практических занятий и лабораторных работ**  
**Заочная форма обучения**

№ п/п	№ раздела и темы дисциплины (модуля)	Наименование семинарских, практических и лабораторных занятий (работ)	Трудоемкость (час.)	Оценочные средства	Формируемые компетенции
1.	1.2	Методы, алгоритмы и программно-аппаратные средства аутентификации и их интеграция в подсистему безопасности Windows	1	Собеседование по лабораторным работам и практическим занятиям	ПК-23
2.	1.3	Снифферы и сканеры портов как средства изучения системы для выполнения атак и получения конфиденциальной информации	2	Собеседование по лабораторным работам и практическим занятиям	ПК-23
3.	1.4	Изучение функций систем предотвращения и обнаружения вторжений и технологии EMT	2	Собеседование по лабораторным работам и практическим занятиям	ПК-23
4.	2.1	Изучение технологий виртуализации кластеризации и облачных технологий	2	Собеседование по лабораторным работам и практическим занятиям	ПК-23
5.	2.2	Программные и аппаратные комплексы криптошлюзов: сравнение эффективности	1	Собеседование по лабораторным работам и практическим занятиям	ПК-23

**6.1. План самостоятельной работы студентов**  
**Заочная форма обучения**

№ п/п	Тема	Вид самостоятельной работы	Задание	Рекомендуемая литература	Количество часов
1	Классификация угроз информационной безопасности и изучение законодательной базы	Проработка лекционного материала	Изучение доп. литературы	Аппаратно-программные средства защиты информации: Практикум / Душкин А.В., Дубровин А.С., Здольник В.В. - Воронеж: Научная книга, 2017. <a href="http://znanium.com/bookread2">http://znanium.com/bookread2</a> .	23

				<a href="http://znanium.com/bookread2.php?book=977192">http://znanium.com/bookread2.php?book=977192</a>	
2	Изучение архитектуры ЭВМ и принципов выполнения программ В Фон-Неймановской архитектуре компьютера.	Подготовка к практическим занятиям, семинарам	Изучение доп. литератур ы	Моделирование системы защиты информации: Практикум: Учебное пособие / Е.К.Баранова, А.В.Бабаш - М.: ИЦ РИОР: НИЦ ИНФРА-М, 2015. <a href="http://znanium.com/bookread2.php?book=476047">http://znanium.com/bookread2.php?book=476047</a>	22
3	Аппаратные средства аутентификации и с использованием биометрических данных и смарт-карт	Подготовка к практическим занятиям, семинарам	Изучение доп. литератур ы	Аппаратно-программные средства защиты информации: Практикум / Душкин А.В., Дубровин А.С., Здольник В.В. - Воронеж:Научная книга, 2017. <a href="http://znanium.com/bookread2.php?book=977192">http://znanium.com/bookread2.php?book=977192</a> Программно-аппаратная защита информации: Учебное пособие / Хорев П.Б., - 2-е изд., испр. и доп. - М.:Форум, НИЦ ИНФРА-М, 2015. <a href="http://znanium.com/bookread2.php?book=489084">http://znanium.com/bookread2.php?book=489084</a>	21
4	Изучение структуры типовой СЗИ Аккорд	Выполнение индивидуальных заданий	Изучение доп. литератур ы	Моделирование системы защиты информации: Практикум: Учебное пособие / Е.К.Баранова, А.В.Бабаш - М.: ИЦ РИОР: НИЦ ИНФРА-М, 2015. <a href="http://znanium.com/bookread2.php?book=476047">http://znanium.com/bookread2.php?book=476047</a> Аппаратно-программные средства защиты информации: Практикум / Душкин А.В., Дубровин А.С., Здольник В.В. - Воронеж:Научная книга, 2017. <a href="http://znanium.com/bookread2.php?book=977192">http://znanium.com/bookread2.php?book=977192</a>	21
5	Изучение способов реализации ключевой защиты	Выполнение индивидуальных заданий	Изучение доп. литератур ы	Шейдаков Н.Е., Серпенинов О.В., Тищенко Е.Н. Физические основы защиты информации: Учеб. пособие. — М.: РИОР: ИНФРА-М, 2016. <a href="http://znanium.com/bookread2.php?book=556661">http://znanium.com/bookread2.php?book=556661</a>	21

6	Изучение методов и криптографических алгоритмов организации защищенных каналов	Выполнение индивидуальных заданий	Изучение доп. литературы	История защиты информации в зарубежных странах: Учебное пособие / Бабаш А. В., Ларин Д. А. - М.: ИЦ РИОР, НИЦ ИНФРА-М, 2016. <a href="http://znanium.com/bookread2.php?book=492549">http://znanium.com/bookread2.php?book=492549</a>	22
---	--	-----------------------------------	--------------------------	--	----

**6.2. Методические указания по организации самостоятельной работы студентов СРС**, направленная на углубление и закрепление знаний, а также развитие практических умений заключается в:

- работе студентов с лекционным материалом и раздаточными материалами, поиске и анализе литературы и электронных источников информации,
- выполнении домашних заданий,
- изучении теоретического материала к практическим занятиям и подготовке ответов на контрольные вопросы по практическим работам,
- изучении тем, вынесенных на самостоятельную проработку,
- подготовке к выполнению практических работ,
- подготовке к дифференцированному зачету.

Для формирования навыков самостоятельной познавательной деятельности необходимо использовать различные формы самостоятельной работы: работу с учебной литературой, выполнение самостоятельных работ, контрольных работ. Перед выполнением самостоятельных, контрольных работ необходимо тщательно изучить теоретический материал по данной теме. При работе с учебниками и книгами рекомендуется использовать различные приемы работы с текстом.

**1. Конспектирование** – краткая запись, краткое изложение содержания прочитанного. Различают сплошное, выборочное, полное, краткое конспектирование. Конспектировать можно от первого или от третьего лица. Предпочтительнее конспектировать от первого лица, т.к. в этом случае лучше развивается самостоятельность мышления.

**2. Тезирование** – краткое изложение основных идей в определенной последовательности.

**3. Реферирование** – обзор одного или ряда источников по теме с собственной оценкой их содержания, формы.

**4. Составление плана текста** – после прочтения текста необходимо разбить его на части и озаглавить каждую из них.

**5. Составление формально-логической модели** – словесно-схематическое изображение прочитанного.

При подготовке к аудиторным занятиям необходимо помнить особенности каждой формы его проведения.

**7. Примерная тематика курсовых работ (проектов) (при наличии)** По учебному плану курсовые работы не предусмотрены

**8. Учебно-методическое и информационное обеспечение дисциплины:**

**а) основная литература** (указывается литература, изданная за последние пять лет)

Информационная безопасность и защита информации: Учебное пособие / Баранова Е.К., Бабаш А.В., - 4-е изд., перераб. и доп. - М.:ИЦ РИОР, НИЦ ИНФРА-М, 2018. <http://znanium.com/bookread2.php?book=957144>

Моделирование системы защиты информации. Практикум : учеб. пособие / Е.К. Баранова, А.В. Бабаш. — 2-е изд., перераб. и доп. — М. : РИОР : ИНФРА-М, 2018. <http://znanium.com/bookread2.php?book=916068>

Комплексная защита информации в корпоративных системах : учеб. пособие / В.Ф. Шаньгин. — М. : ИД «ФОРУМ» : ИНФРА-М, 2017. <http://znanium.com/bookread2.php?book=546679>

Информационная безопасность и защита информации: Учебное пособие / Баранова Е. К., Бабаш А. В. - 3-е изд. - М.: ИЦ РИОР, НИЦ ИНФРА-М, 2016. <http://znanium.com/bookread2.php?book=495249>

Защита информации: Учебное пособие / А.П. Жук, Е.П. Жук, О.М. Лепешкин, А.И. Тимошкин. - 2-е изд. - М.: ИЦ РИОР: НИЦ ИНФРА-М, 2015. <http://znanium.com/bookread2.php?book=474838>

Программно-аппаратная защита информации: Учебное пособие / Хорев П.Б., - 2-е изд., испр. и доп. - М.:Форум, НИЦ ИНФРА-М, 2015. <http://znanium.com/bookread2.php?book=489084>

#### **б) дополнительная литература**

Аппаратно-программные средства защиты информации: Практикум / Душкин А.В., Дубровин А.С., Здольник В.В. - Воронеж:Научная книга, 2017. <http://znanium.com/bookread2.php?book=977192>

История защиты информации в зарубежных странах: Учебное пособие / Бабаш А. В., Ларин Д. А. - М.: ИЦ РИОР, НИЦ ИНФРА-М, 2016. <http://znanium.com/bookread2.php?book=492549>

Шейдаков Н.Е., Серпенинов О.В., Тищенко Е.Н. Физические основы защиты информации: Учеб. пособие. — М.: РИОР: ИНФРА-М, 2016. <http://znanium.com/bookread2.php?book=556661>

Моделирование системы защиты информации: Практикум: Учебное пособие / Е.К.Баранова, А.В.Бабаш - М.: ИЦ РИОР: НИЦ ИНФРА-М, 2015. <http://znanium.com/bookread2.php?book=476047>

Программно-аппаратная защита информации: Учебное пособие / Хорев П.Б., - 2-е изд., испр. и доп. - М.:Форум, НИЦ ИНФРА-М, 2015. <http://znanium.com/bookread2.php?book=489084>

#### **в) программное обеспечение**

1. Microsoft Windows
2. Microsoft Word
3. Microsoft Excel
4. Microsoft Power Point

#### **г) базы данных, информационно-справочные и поисковые системы**

1. <http://znanium.com/> ООО электронно-библиотечная система "ЗНАНИУМ"
2. <https://rucont.ru/> ООО "Национальный цифровой ресурс «РУКОНТ»
3. <http://biblioclub.ru/> ЭБС «Университетская библиотека онлайн»

#### **9. Материально-техническое обеспечение дисциплины:**

Учебная аудитория для проведения занятий лекционного типа; занятий семинарского типа; для курсового проектирования (выполнения курсовых работ); для проведения групповых и индивидуальных консультаций; для текущего контроля и промежуточной аттестации.

Рабочие места обучающихся; Рабочее место преподавателя; Классная доска; Проекторы; Ноутбук; Экран; Интерактивная доска; Звукоусиливающая аппаратура; Учебно-наглядные пособия.

Лаборатория Информационных технологий. Учебная аудитория для проведения занятий лекционного типа; занятий лабораторного и практического типа; для курсового проектирования (выполнения курсовых работ); для проведения групповых и индивидуальных консультаций; для текущего контроля и промежуточной аттестации.

Рабочие места обучающихся; Рабочее место преподавателя; Ноутбук; Проектор переносной; Экран переносной; Классная доска; 20 рабочих мест обучающихся оснащенные ПЭВМ с подключением к сети интернет и обеспечением доступа в электронную информационно-образовательную среду Университета. (ПО лицензии)

#### **10. Образовательные технологии:**

При реализации учебной дисциплины применяются различные образовательные технологии, в том числе технологии электронного обучения, используют в учебном процессе активные и интерактивные формы учебных занятий в сочетании с внеаудиторной работой с целью формирования и развития профессиональных навыков обучающихся.

Учебные часы дисциплины предусматривают классическую контактную работу преподавателя с обучающимся в аудитории и контактную работу посредством электронной информационно-образовательной среды в синхронном и асинхронном режиме (вне аудитории) посредством применения возможностей компьютерных технологий (электронная почта, электронный учебник, видеофильм, презентация и др.)

*Активные методы обучения* – методы, стимулирующие познавательную деятельность обучающихся, строятся в основном на диалоге, который предполагает свободный обмен мнениями о путях разрешения той или иной проблемы, они характеризуются высоким уровнем активности обучающихся. Именно такое обучение сейчас общепринято считать «наилучшей практикой обучения». Исследования показывают, что именно на активных занятиях – если они ориентированы на достижение конкретных целей и хорошо организованы – учащиеся часто усваивают материал наиболее полно и с пользой для себя. Фраза «наиболее полно и с пользой для себя» означает, что учащиеся думают о том, что они изучают, применяют это в ситуациях реальной жизни или для дальнейшего обучения и могут продолжать учиться самостоятельно.

По дисциплине проводятся:

- *лекция-визуализация* – передача информации посредством графического представления в образной форме (слайды, видео-слайды, плакаты и т.д.). Лекция считается визуализацией, если в течение полутора часов преподаватель использует не менее 12 наглядных изображений, максимум - 21. Роль преподавателя в лекции-визуализации – комментатор. Подготовка данной лекции преподавателем состоит в том, чтобы изменить, переконструировать учебную информацию по теме лекционного занятия в визуальную форму для представления через технические средства обучения (ноутбук, акустические системы, экран, мультимедийный проектор) или вручную (схемы, рисунки, чертежи и т.п.). Лекцию-визуализацию рекомендуется проводить по темам, ключевым для данного предмета, раздела. При подготовке наглядных материалов следует соблюдать требования и правила, предъявляемые к представлению информации.

- *собеседование* – специально организованная беседа, устраиваемая с целью выявления подготовленности лица к определенному виду деятельности.

#### **11. Оценочные средства (ОС)**

Оценочные средства по дисциплине «Аппаратные средства защиты технической информации на предприятиях пищевой промышленности» разработаны в соответствии с положением о балльно-рейтинговой системе оценки успеваемости студентов ФГБОУ ВО «МГУТУ им. К.Г. Разумовского (Первый казачий университет)».

*Критерии оценки текущих занятий для очной формы обучения*

✓ посещение студентом одного занятия – 1 балл;

- ✓ выполнение заданий для самостоятельной работы – от 1 до 3 баллов за каждый пункт задания;
- ✓ активная работа на занятии – от 1 до 3 баллов;
- ✓ защита лабораторной работы – от 1 до 5 баллов.

*Критерии оценки текущих занятий для заочной формы обучения*

- ✓ посещение студентом одного занятия – 5 баллов;
- ✓ выполнение заданий для самостоятельной работы – от 10 до 15 баллов за каждый пункт задания;
- ✓ активная работа на занятии – от 1 до 10 баллов
- ✓ защита лабораторной работы – от 1 до 15 баллов.

### **БАЛЛЬНО-РЕЙТИНГОВАЯ СИСТЕМА**

Максимальная сумма рейтинговых баллов, которая может быть начислена студенту по учебной дисциплине, составляет 100 рейтинговых

Форма промежуточной аттестации	Количество баллов		
	Текущий контроль	Рубежный контроль	Сумма баллов
Зачет с оценкой	30-70	20-30	60-100

Рейтинг студента в семестре по дисциплине складывается из рейтинговых баллов, которыми преподаватель в течение семестра оценивает посещение учебных занятий, его текущую работу на занятиях и самостоятельную работу, результаты текущих контрольных работ, устных опросов, премиальных и штрафных баллов.

Преподаватель, осуществляющий проведение практических занятий, доводит до сведения студентов на первом занятии информацию о формировании рейтинга студента и рубежного рейтинга.

По окончании семестра каждому студенту выставляется его рейтинговая оценка текущей успеваемости, которая является оценкой посещаемости занятий, активности на занятиях, качества самостоятельной работы.

Студент допускается к мероприятиям промежуточной аттестации, если его рейтинговая оценка текущей успеваемости (без учета премиальных рейтинговых баллов) не менее по дисциплине, завершающейся зачетом с оценкой - 30 рейтинговых баллов;

Студенты, не набравшие минимальных рейтинговых баллов по учебной дисциплине проходят процедуру добора баллов.

Максимальная рейтинговая оценка текущей успеваемости студента за семестр по результатам текущей работы и текущего контроля знаний (без учета премиальных баллов) составляет: 70 рейтинговых баллов для дисциплин, заканчивающихся зачетом с оценкой.

Ответ студента может быть максимально оценен на зачете с оценкой в 30 рейтинговых баллов;

Студент, по желанию, может сдать зачет с оценкой в формате «автомат», если его рейтинг за семестр, с учетом премиальных баллов, составил не менее:

- 60 рейтинговых баллов с выставлением оценки «удовлетворительно»;
- 70 рейтинговых баллов с выставлением оценки «хорошо»;
- 90 рейтинговых баллов с выставлением оценки «отлично».

Рейтинговая оценка по дисциплине и соответствующая аттестационная оценка по шкале «удовлетворительно», «хорошо», «отлично» при использовании формата «автомат», проставляется экзаменатором в зачетную книжку и зачетно-экзаменационную ведомость только в день проведения экзамена согласно расписанию группы, в которой обучается студент.

Для приведения рейтинговой оценки к аттестационной (пятибалльный формат) используется следующая шкала:

Аттестационная оценка по дисциплине	Рейтинг студента по дисциплине (включая премиальные баллы)
«отлично»	90- 100 баллов
«хорошо»	70 - 89 баллов
«удовлетворительно»	60 - 69 баллов
«неудовлетворительно»	менее 60 баллов

Рубежный рейтинг по дисциплине у студента на зачете с оценкой не менее чем в 20 рейтинговых баллов считается неудовлетворительным (независимо от рейтинга студента в семестре). В этом случае в зачетно-экзаменационную ведомость в графе «Аттестационная оценка» проставляется «неудовлетворительно».

Преподавателю предоставляется право начислять студентам премиальные баллы за активность (участие в научных конференциях, конкурсах, олимпиадах, активная работа на аудиторных занятиях, публикации статей, работа со школьниками, выполнение заданий повышенной сложности, изготовление наглядных пособий и т.д.) в количестве, не превышающем 20 рейтинговых баллов за семестр. Премиальные баллы не входят в сумму рейтинга текущей успеваемости студента, а прибавляются к ним.

**Оценочные средства текущего контроля** формируются в соответствии с ЛНА (Локальными нормативными актами) университета.

Назначение оценочных средств текущего контроля – выявить сформированность компетенции ПК-23.

**Оценочные средства для промежуточной аттестации (в форме зачета с оценкой).**

Код компетенции	Содержание компетенции (части компетенции)	Результаты обучения	Этапы формирования компетенций в процессе освоения образовательной программы
ПК-23	способностью выполнять работы по наладке, настройке, регулировке, опытной проверке, регламентному техническому, эксплуатационному обслуживанию оборудования, средств и систем автоматизации, контроля, диагностики, испытаний и управления,	<p>Знает: методы и аппаратные средства защиты программного обеспечения от несанкционированного изучения, копирования и модификации; методы и алгоритмы управления и генерации ключей и их аппаратно-программная реализация и применение в автоматизированных системах; принципы построения безопасных автоматизированных рабочих мест и вычислительных сетей с использованием аппаратных комплексов</p> <p>Умеет: разворачивать и настраивать аппаратные средства для защиты локальных и распределенных вычислительных систем; обеспечивать надежную аутентификацию и управление доступом к информационным ресурсам с учетом требований нормативно-технической документации; настраивать каналы безопасного обмена информацией в локальных и распределенных автоматизированных системах</p>	<p>Этап формирования знаний</p> <p>Этап формирования умений</p>

средств программного обеспечения, сертификационным испытаниям изделий	Владеет: инструментарием, обеспечивающим аппаратную защиту информационных ресурсов от изучения, модификации и копирования; аппаратными комплексами управления ключами, сертификатами и правами пользователей в защищенных автоматизированных системах	Этап формирования навыков и получения опыта
---	---	---

**Материалы для проведения текущего и промежуточного контроля знаний студентов:**

№ п/п	Вид контроля	Контролируемые темы (разделы)	Компетенции, компоненты которых контролируются
1	Устный опрос	1.1	ПК-23
2	Устный опрос	1.2	ПК-23
3	Устный опрос	1.3	ПК-23
4	Устный опрос	1.4	ПК-23
5	Устный опрос	2.1	ПК-23
6	Устный опрос	2.2	ПК-23

**Вопросы для собеседования №1 (№2, №3)**

**№1**

1. Использование протокола IPSec для защиты сетевого трафика
2. Назначение и использование редактора реестра

**№2**

1. Технология теневого копирования данных
2. Назначение, создание и использование профилей пользователей

**Вопросы к зачету**

1. Сущность понятия "защищаемая информация"
2. Разновидность защищаемой информации
3. Носители защищаемой информации
4. Понятие ИБ. Составляющие ИБ.
5. Понятие «государственная тайна», сведения, составляющие государственную тайну. Основные положения Закона РФ "О государственной тайне".
6. Коммерческая тайна и ее особенности. Основные положения Закона РФ «О коммерческой тайне»
7. Российское законодательство в области ИБ.
8. Государственная система защиты информации
9. Защищенные информационные системы. Основные понятия.
10. Понятие угроз ИБ. Критерии их классификации.
11. Административно-правовые методы защиты информации. Политика информационной безопасности: основные положения.
12. Физические (организационные) методы обеспечения информационной безопасности. Основные классы мер организационного уровня обеспечения информационной безопасности.
13. DLP-системы: назначение, принципы построения, функциональные возможности.
14. Назначение криптографических методов защиты информации. Классификация методов криптографического преобразования информации.
15. Классификация шифров замены. Примеры.
16. Классификация шифров перестановки. Примеры.
17. Аналитические методы шифрования. Пример.
18. Методы гаммирования. Стандарты шифрования.

19. Роль стандартов ИБ. Основные понятия и определения.
20. Критерии безопасности компьютерных систем «Оранжевая книга».
21. Гармонизированные критерии Европейских стран.
22. Стандарт ISO / IEC 15408.
23. Международный стандарт безопасности информационных систем ISO 17799.
24. Открытый стандарт СОВИТ
25. Аудит информационной безопасности: цель, виды, методики.
26. Основные этапы проведения аудита информационной безопасности.
27. Учетные записи и группы пользователей. Стратегия управления учетными записями в Active Directory
28. Дисковые квоты.
29. Профили пользователей.
30. Понятие и назначение реестра Windows. Назначение корневых разделов реестра Windows.
31. Команды работы с реестром.
32. Настройка политик безопасности в Windows: политика учетных записей, политика паролей, политика аудита.
33. Обеспечение хранения данных в Windows Server 2008: теневые копии, архивы.
34. Информационная безопасность распределенных систем. Рекомендации X.800.

## **12. Организация образовательного процесса для лиц с ограниченными возможностями**

Организация образовательного процесса для лиц с ограниченными возможностями осуществляется в соответствии с «Методическими рекомендациями по организации образовательного процесса для инвалидов и лиц с ограниченными возможностями здоровья в образовательных организациях высшего образования, в том числе оснащённости образовательного процесса» Министерства образования и науки РФ от 08.04.2014г. № АК-44/05вн.

В образовательном процессе используются социально-активные и рефлексивные методы обучения, технологии социокультурной реабилитации с целью оказания помощи в установлении полноценных межличностных отношений с другими студентами, создании комфортного психологического климата в студенческой группе.

Студенты с ограниченными возможностями здоровья, в отличие от остальных студентов, имеют свои специфические особенности восприятия, переработки материала. Подбор и разработка учебных материалов производится с учетом индивидуальных особенностей.

Предусмотрена возможность обучения по индивидуальному графику, при составлении которого возможны различные варианты проведения занятий: в академической группе и индивидуально, на дому с использованием дистанционных образовательных технологий.

### 13. Лист регистрации изменений

№ п/п	Содержание изменения	Реквизиты документа об утверждении изменения	Дата введения изменения
1			
2			
3			
4			
5			
6			