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»

«Утверждаю»
Директор БИТУ (филиал)
ФГБОУ ВО «МГУТУ
им. К.Г. Разумовского (ПКУ)»
_____Е.В. Кузнецова
«29» июня 2023 г.

Рабочая программа дисциплины

Б1.В.ДВ.06.02 – ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

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 **«Информационная безопасность»** 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. Одинокова 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., ст. преподаватель Перевозчикова Е.Г.

Руководитель основной профессиональной образовательной программы
кандидат педагогических наук, доцент _____ Е.В. Одинокова
(подпись)

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 _____ Е.В.Одинокова
(подпись)

Оглавление

1. Цели и задачи дисциплины: 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:

- развертывать 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 «Информационная безопасность» 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.

Код и описание компетенции	**Планируемые результаты обучения по дисциплине**
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	**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
	Умеет: развертывать 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
	Владеет: 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 (разделяется по формам обучения)

Заочная форма обучения

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

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. Информационная безопасность и уровни ее обеспечения (ПК-23)

Тема 1. Понятие "информационная безопасность".

Информационная безопасность. Защита информации. Основные составляющие информационной безопасности.

Доступность, целостность и конфиденциальность информационных ресурсов. Важность и сложность проблемы информационной безопасности. Доктрина информационной безопасности Российской Федерации.

Тема 2. Составляющие информационной безопасности.

Основные составляющие. Важность проблемы. Понятие информационной безопасности. Защита информации. Основные составляющие информационной безопасности. Основные определения и критерии классификации угроз. Основные угрозы конфиденциальности.

Раздел 2. Стандарты информационной безопасности. (ПК-23)

Тема 2.1. Стандарты информационной безопасности: "Общие критерии".

Понятие безопасности информации. Международный стандарт информационной безопасности. Особенности процесса стандартизации в Интернете. Стандарты безопасности в Интернете: SSL (TLS), SET, IPSec. Особенности российского рынка. Государственные стандарты

Тема 2.2. Стандарты информационной безопасности распределенных систем.

Информационная безопасность распределенных систем. Рекомендации X.800. Сетевые сервисы безопасности. Аутентификация партнеров по общению. Управление доступом. Конфиденциальность данных. Аутентификация источника данных. Семиуровневая модель OSI. Сетевые механизмы безопасности. Шифрование. Электронная цифровая подпись. Администрирование средств безопасности.

Раздел 3. Административный уровень обеспечения информационной безопасности (ПК-23)

Тема 3.1. Цели, задачи и содержание административного уровня

Содержание административного уровня. Дайте определение политики безопасности. Направления разработки политики безопасности. Перечислите составные элементы автоматизированных систем. Субъекты информационных отношений и их роли при обеспечении информационной безопасности.

Тема 3.2. Разработка политики информационной безопасности.

Основная цель разработки политики безопасности на предприятии. Субъекты и объекты информационных систем и их классификация. Цели и задачи административного уровня обеспечения информационной безопасности. Место политики безопасности в структуре ВНД (внутренней нормативной документации) предприятия.

Субъекты информационных отношений и их роли при обеспечении информационной безопасности.

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	2	3	4					
2.	Преддипломная практика	1	2	3	4	5	6			
3.	Выпускная квалификационная работа	1	2	3	4	5	6			

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.	Информационная безопасность и уровни ее	Понятие "информационная безопасность".				20	20

	обеспечения						
2.	Информационная безопасность и уровни ее обеспечения	Составляющие информационной безопасности	1	1		22	24
3.	Стандарты информационной безопасности	Стандарты информационной безопасности: "Общие критерии".	1	1		22	24
4.	Стандарты информационной безопасности	Стандарты информационной безопасности распределенных систем		2		22	24
5.	Административный уровень обеспечения информационной безопасности	Цели, задачи и содержание административного уровня			2	22	24
6.	Административный уровень обеспечения информационной безопасности	Разработка политики информационной безопасности			2	22	24

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.	Информационная безопасность и уровни ее обеспечения	Обсуждение материала. Доклады Лабораторные и практические работы
2.	Стандарты информационной безопасности	Обсуждение материала. Доклады Лабораторные и практические работы
3.	Административный уровень обеспечения информационной безопасности	Обсуждение материала. Доклады Лабораторные и практические работы
4.	Классификация угроз "информационной безопасности"	Обсуждение материала. Доклады Лабораторные и практические работы

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	Информационная безопасность и уровни ее обеспечения	1	Собеседование по практическим занятиям	ПК-23
2.	2	Стандарты информационной	3	Собеседование	ПК-23

		безопасности		по практическим занятиям	
3.	3	Административный уровень обеспечения информационной безопасности	4	Собеседование по лабораторным работам	ПК-23

6.1. План самостоятельной работы студентов
Заочная форма обучения

№ п/п	Тема	Вид самостоятельной работы	Задание	Рекомендуемая литература	Количество часов
1	Информационная безопасность и уровни ее обеспечения	Проработка лекционного материала	Изучение литературы	Основная 1	42
2	Стандарты информационной безопасности	Подготовка к практическим занятиям, семинарам	Изучение литературы	Дополнительная 1, 2, 3	44
3	Административный уровень обеспечения информационной безопасности	Подготовка к практическим занятиям, семинарам	Изучение литературы	Дополнительная 1	44

6.2. Методические указания по организации самостоятельной работы студентов

При изучении курса необходимо добиться полного и сознательного усвоения теоретических основ физики, научится применять теорию к решению задач.

Приступая к изучению каждого нового раздела курса, прежде всего, следует ознакомиться с содержанием темы по программе дисциплины, уяснить объем темы и последовательность рассматриваемых в ней вопросов.

При изучении физики рекомендуется просматривать весь материал темы, чтобы составить о нем первоначальное представление.

Приступая впервые к работе над книгой, необходимо предварительно ознакомится с ним. Оглавление книги укажет на её содержание, предисловие и введение дадут представление о содержании книги, а беглый просмотр поможет узнать, какие в книге имеются таблицы, схемы, графики и другой иллюстративный материал.

При работе над книгой студенту необходимо выделять в тексте главное, разбираться в закономерностях, выводах формул. При чтении книги нужно внимательно рассматривать имеющийся в ней иллюстративный материал.

Закончив изучение темы, прежде чем переходить к следующей, следует ответить на вопросы по данной теме, помещенные в конце соответствующей главы и предназначенные для самопроверки приобретенных знаний. Изучение материала книги должно сопровождаться выполнением содержащихся в нем упражнений и решением задач, относящихся к рассматриваемой теме.

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

1. Информационная безопасность предприятия : учеб. пособие / Н.В. Гришина. — 2-е изд., доп. — М. : ФОРУМ : ИНФРА-М, 2017. http://znanium.com/catalog/product/612572

б) дополнительная литература

1. 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/catalog/product/495249
2. Информационная безопасность предприятия: Учебное пособие / Н.В. Гришина. - 2-е изд., доп. - М.: Форум: НИЦ ИНФРА-М, 2015. http://znanium.com/bookread2.php?book=491597
3. Башлы, П. Н. Информационная безопасность и защита информации [Электронный ресурс] : Учебник / П. Н. Башлы, А. В. Бабаш, Е. К. Баранова. - М.: РИОР, 2013. http://znanium.com/bookread2.php?book=405000

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

В образовательном процессе используются лекции, дискуссии лабораторные и практические работы.

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 дисциплинепроводятся:

- *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.

11. Оценочные средства (ОС)

Оценочные средства по дисциплине «Информационная безопасность» 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;
- ✓ подготовка доклада– от 1 до 5 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
- ✓ подготовка доклада– 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 – защита лабораторных работ, устный опрос по лекционному материалу (полный список контрольных вопросов приведен в фонде оценочных средств по дисциплине (в приложении к рабочей программе дисциплины)).

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, средств программного обеспечения, сертификационным испытаниям изделий	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	Этап формирования знаний
		Умеет: развертывать 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	Этап формирования умений
		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	**Текущий контроль** **Устный опрос** по материалам лекций – фронтальная форма контроля, представляющая собой ответы на вопросы преподавателя в устной форме.	1,2,3	ПК-23
2	**Текущий контроль.**	1,2,3	ПК-23

	Защита лабораторных работ – форма контроля, предусматривающая изложение и анализ знаниевых компонентов, методик исследования, этапов и результатов осуществления действий и операций по теме работе, представление и обоснование выводов по работе, факторный анализ результатов, формулирование предложений, ответы на вопросы преподавателя по теме работы.		
3	**Промежуточная аттестация Зачет с оценкой** – выставляется по итогам ответов на вопросы к зачету	1,2,3	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 и задания 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. Что является нормативно-правовой основой для введения дополнительных ограничений по контролю над деятельностью персонала?
14. Что такое «правовое обеспечение информационной безопасности», раскройте содержание правового обеспечения безопасности сведений.
15. Что такое «сертификат ключа электронной цифровой подписи» и зачем он нужен?
16. Перечислите службы образующие государственную систему защиты информации.
17. Правовая защита интересов личности, общества, государства от угроз воздействия недоброкачественной информации, от нарушения порядка распространения информации.
18. Основные положения конвенции Совета Европы «О защите физических лиц при автоматизированной обработке персональных данных».

19. Роль ЕС и международных организации в регулировании международного информационного обмена.
20. Национальные интересы РФ в информационной сфере и их обеспечения.
21. Административный уровень информационной безопасности
22. Администрирование средств безопасности
23. Вредоносное программное обеспечение
24. Действия, приводящие к неправомерному овладении конфиденциальной информацией: разглашение
25. Действия, приводящие к неправомерному овладении конфиденциальной информацией: утечка
26. Действия, приводящие к неправомерному овладении конфиденциальной информацией: несанкционированный доступ

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 оснащенности 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			