Документ подписан простой электронной подписью
Информация о владельце:
ФИО: Выборнова Любовь Алексеевна
Должность: Ректор
Дата подписания: 30.10.2026 13:49:29
Уникальный программный ключ:
c3b3b9c625f6c113afa2a2c42baff9e05a58b76e

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
федеральное государственное бюджетное образовательное учреждение высшего образования
«Поволжский государственный университет сервиса» (ФГБОУ ВО «ПВГУС»)

Высшая школа интеллектуальных систем и кибертехнологий

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

«Управление антивирусной защитой»

Направление подготовки:

10.03.01 «Информационная безопасность»

Направленность (профиль):

«Организация и технологии защиты информации (по отрасли или в сфере профессиональной деятельности)»

Квалификация выпускника: **бакалавр**

Тольятти 2025

Рабочая программа дисциплины «Управление антивирусной защитой» разработана в соответствии с Федеральным государственным образовательным стандартом высшего образования – бакалавриат по направлению подготовки 10.03.01 «Информационная безопасность», утвержденным приказом Министерства науки и высшего образования Российской Федерации от 17.11.2020 г. № 1427.

Составители:

старший преподаватель	Ю.С. Мунирова
(ученая степень, ученое звание)	(ФИО)

РПД обсуждена на заседании ученого совета Высшей школы интеллектуальных систем и кибертехнологий

23.05.2025 г., протокол № _10__

Директор	к.э.н., доцент	О.А. Филиппова
	(уч.степень, уч.звание)	(ФИО)

1. ПЕРЕЧЕНЬ ПЛАНИРУЕМЫХ РЕЗУЛЬТАТОВ ОБУЧЕНИЯ ПО ДИСЦИПЛИНЕ, СООТНЕСЕННЫХ С ПЛАНИРУЕМЫМИ РЕЗУЛЬТАТАМИ ОСВОЕНИЯ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

1.1. Цель освоения дисциплины

Целями освоения дисциплины являются:

– формирование у обучающихся системных теоретических знаний о принципах организации и функционирования антивирусной защиты информационных систем;

– формирование умения организовывать защиту информации ограниченного доступа от воздействия вредоносного программного обеспечения в соответствии с нормативными правовыми актами и методическими документами;

– формирование навыков применения программных, программно-аппаратных и технических средств антивирусной защиты автоматизированных систем.

- формирование у обучающихся общепрофессиональных компетенций *в области использования информационно-коммуникационных технологий и т.п.*

- *формирование у обучающихся* профессиональных компетенций, необходимых для решения задач профессиональной деятельности.

1.2. Перечень планируемых результатов обучения по дисциплине

Код и наименование компетенции	Код и наименование индикатора достижения компетенции	Планируемые результаты обучения по дисциплине	Основание (ПС) *для профессиональных компетенций
ОПК-6. Способен при решении профессиональных задач организовывать защиту информации ограниченного доступа в соответствии с нормативными правовыми актами, нормативными и методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю	ИОПК-6.1. Применяет технологии, методы и средства защиты информации ограниченного доступа	Знает: – технологии, методы и средства антивирусной защиты информации ограниченного доступа; требования нормативных и методических документов ФСТЭК России в области антивирусной защиты Умеет: – применять технологии, методы и средства антивирусной защиты информации ограниченного доступа в автоматизированных системах Владеет: – навыками организации антивирусной защиты информации ограниченного доступа в соответствии с действующими нормативными требованиями	
ПК-4. Способен	ИПК-4.1. Применяет	Знает:	06.033 Специалист

выполнять работы по установке, настройке и обслуживанию программных, программно-аппаратных и технических средств защиты информации автоматизированных системах	программные, программно-аппаратные и технические средства защиты информации автоматизированных систем, в том числе криптографические методы, алгоритмы и протоколы ИПК-4.2. Осуществляет конфигурирование параметров программных, программно-аппаратных и технических средств защиты информации автоматизированных систем	– принципы работы и архитектуру программных средств антивирусной защиты автоматизированных систем Умеет: – осуществлять конфигурирование параметров средств антивирусной защиты автоматизированных систем Владеет: – навыками установки, настройки и обслуживания средств антивирусной защиты автоматизированных систем	по защите информации в автоматизированных системах

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

Дисциплина относится к факультативным дисциплинам образовательной программы бакалавриата Блока Ф. Дисциплины (модули) образовательной программы (Факультативные дисциплины).

3. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

3.1. Объем и структура дисциплины

Общая трудоёмкость дисциплины составляет **2 з.е. (72 час.)**, их распределение по видам работ представлено в таблице.

Виды учебных занятий и работы обучающихся	Трудоемкость, час
Общая трудоемкость дисциплины, час	**72**
Контактная работа обучающихся с преподавателем по видам учебных занятий (всего), в т.ч.:	**30/8**
занятия лекционного типа (лекции)	12/4
занятия семинарского типа (семинары, практические занятия, практикумы, коллоквиумы и иные аналогичные занятия)	18/4
Самостоятельная работа всего, в т.ч.:	**42/60**
Контроль (часы на зачет)	–/4
Промежуточная аттестация	**Зачет**

Примечание: *-/- объем часов соответственно для очной, очно-заочной формы обучения*

Дисциплина реализуется посредством проведения контактной работы с обучающимися (включая проведение текущего контроля успеваемости), самостоятельной работы обучающихся и промежуточной аттестации.

В процессе освоения дисциплины может применяться электронное обучение и дистанционные образовательные технологии.

В процессе освоения дисциплины обучающиеся обеспечены доступом к электронной информационно-образовательной среде и электронно-библиотечным системам.

3.2. Содержание дисциплины, структурированное по темам

Планируемые результаты освоения: код формируемой компетенции и индикаторы достижения компетенций	Наименование разделов, тем	Виды учебной работы			Формы текущего контроля (наименование оценочного средства)
		Контактная работа		Самостоятельная работа, час	
		Лекции, час	Практические занятия, час		
ОПК-6 ИОПК-6.1	**ТЕМА 1. ВРЕДОНОСНОЕ ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ КАК ОБЪЕКТ УПРАВЛЕНИЯ АНТИВИРУСНОЙ ЗАЩИТОЙ** Основное содержание: 1. Понятие и классификация вредоносного программного обеспечения. 2. Способы распространения и заражения вредоносным программным обеспечением. 3. Нормативные и методические документы, регламентирующие антивирусную защиту.	2/0,5			Устный опрос
	Практическое занятие № 1. Классификация вредоносного программного обеспечения по типовым признакам		3/0,5		Практическое задание
	Самостоятельная работа			7/10	Самостоятельное изучение методических материалов
ОПК-6 ИОПК-6.1	**ТЕМА 2. ПРИНЦИПЫ ПОСТРОЕНИЯ СИСТЕМЫ АНТИВИРУСНОЙ ЗАЩИТЫ** Основное содержание: 1. Принципы построения системы антивирусной защиты автоматизированной системы. 2. Уровни антивирусной защиты: рабочие места, серверы, сетевой периметр. 3. Требования к антивирусной защите информации ограниченного доступа.	2/0,5			

	Практическое занятие № 2. Разработка схемы многоуровневой антивирусной защиты типовой автоматизированной системы		3/0,5		Практическое задание
	Самостоятельная работа			7/10	Самостоятельное изучение методических материалов
ПК-4 ИПК-4.1	**ТЕМА 3. АРХИТЕКТУРА И МЕТОДЫ ОБНАРУЖЕНИЯ АНТИВИРУСНЫХ СРЕДСТВ** Основное содержание: 1. Архитектура и компоненты современного антивирусного средства защиты. 2. Методы обнаружения вредоносного программного обеспечения: сигнатурный, эвристический, поведенческий анализ. 3. Сравнительная характеристика отечественных антивирусных средств защиты.	2/0,5			Устный опрос / тестирование
	Практическое занятие № 3. Сравнительный анализ методов обнаружения вредоносного ПО		3/0,5		Практическое задание
	Самостоятельная работа			7/10	Самостоятельное изучение методических материалов

ПК-4 ИПК-4.1, ИПК-4.2	**ТЕМА 4. УСТАНОВКА И НАСТРОЙКА АНТИВИРУСНОГО СРЕДСТВА ЗАЩИТЫ** Основное содержание: 1. Порядок установки антивирусного средства защиты на автоматизированное рабочее место. 2. Конфигурирование параметров работы антивирусного средства защиты. 3. Настройка расписания проверок и обновлений.	2/0,5			Практическое задание
	Практическое занятие № 4. Установка и настройка антивирусного средства защиты на рабочей станции		3/0,5		Практическое задание
	Самостоятельная работа			7/10	Самостоятельное изучение методических материалов
ПК-4 ИПК-4.2	**ТЕМА 5. ЦЕНТРАЛИЗОВАННОЕ УПРАВЛЕНИЕ АНТИВИРУСНОЙ ЗАЩИТОЙ** Основное содержание: 1. Централизованные системы управления антивирусной защитой в организации. 2. Настройка политик антивирусной защиты для групп рабочих станций. 3. Мониторинг состояния антивирусной защиты в масштабе организации.	2/0,5			
	Практическое занятие № 5. Настройка централизованной политики антивирусной защиты		3/0,5		Практическое задание
	Самостоятельная работа			7/10	Самостоятельное изучение методических материалов

ОПК-6 ИОПК-6.1	**ТЕМА 6. РЕАГИРОВАНИЕ НА ИНЦИДЕНТЫ, СВЯЗАННЫЕ С ВРЕДОНОСНЫМ ПРОГРАММНЫМ ОБЕСПЕЧЕНИЕМ** Основное содержание: 1. Порядок реагирования на инциденты, связанные с обнаружением вредоносного программного обеспечения. 2. Мониторинг событий антивирусной защиты и анализ журналов. 3. Отчетность и документирование мероприятий по антивирусной защите.	2/0,5			Практическое задание / тестирование
	Практическое занятие № 6. Разбор типового инцидента, связанного с вредоносным программным обеспечением		3/0,5		Практическое задание
	Самостоятельная работа			7/10	Самостоятельное изучение методических материалов
	ИТОГО	**12/4**	**18/4**	**42/60**	

Примечание: *-/- объем часов соответственно для очной, очно-заочной формы обучения*

4. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ

4.1. Общие методические рекомендации по освоению дисциплины, образовательные технологии

Дисциплина реализуется посредством проведения контактной работы с обучающимися (включая проведение текущего контроля успеваемости), самостоятельной работы обучающихся и промежуточной аттестации.

При проведении учебных занятий по дисциплине обеспечивается развитие у обучающихся навыков системного и критического мышления, практических умений и владений, необходимых для решения профессиональных задач в области информационной безопасности (включая проведение интерактивных лекций, лабораторных и практических занятий, разбора практических ситуаций).

Преподавание дисциплины ведется с применением следующих видов образовательных технологий:

- балльно-рейтинговая технология оценивания;
- электронное обучение;
- проблемное обучение;
- разбор конкретных ситуаций (кейс-метод);
- информационные технологии, применяемые в электронной информационно-образовательной среде университета.

Для оценки знаний, умений, навыков и уровня сформированности компетенций по дисциплине применяется балльно-рейтинговая система контроля и оценки успеваемости студентов. Максимальное количество баллов в семестре – 100.

4.2. Методические указания для обучающихся по освоению дисциплины на занятиях лекционного типа

Лекционный курс предполагает систематизированное изложение основных вопросов тематического плана. В ходе лекционных занятий раскрываются базовые вопросы в рамках каждой темы дисциплины, обозначаются ключевые аспекты тем, а также делаются акценты на наиболее сложные и важные положения изучаемого материала.

Лекционные занятия проводятся в аудитории с применением мультимедийного проектора в виде учебной презентации или в ЭИОС университета.

Отдельные вопросы предлагаются для самостоятельного изучения (конспектируются).

Материалы лекций являются опорной основой для подготовки обучающихся к практическим (лабораторным) занятиям, выполнения заданий самостоятельной работы, а также к мероприятиям текущего контроля успеваемости и промежуточной аттестации по дисциплине.

4.3. Методические указания для обучающихся по освоению дисциплины на занятиях семинарского типа / на практических занятиях

Практические (лабораторные) занятия представляют собой детализацию лекционного теоретического материала, проводятся в целях закрепления курса и охватывают все основные разделы дисциплины. Основной формой проведения занятий является обсуждение наиболее проблемных и сложных вопросов по отдельным темам, а также решение практических задач и выполнение заданий на персональном компьютере.

Практические (лабораторные) занятия обучающихся обеспечивают:

- проверку и уточнение знаний, полученных на лекциях;
- получение умений и практических навыков по учебному материалу дисциплины;
- подведение итогов занятий по рейтинговой системе, согласно технологической карте дисциплины.

Занятия организуются, в том числе, в форме практической подготовки, которая предусматривает участие обучающихся в выполнении отдельных элементов работ, связанных с будущей профессиональной деятельностью.

Практическая подготовка предусматривает: выполнение всех практических заданий.

4.4. Методические указания по самостоятельной работе обучающихся

Самостоятельная работа обеспечивает подготовку обучающегося к аудиторным занятиям и мероприятиям текущего контроля и промежуточной аттестации по изучаемой дисциплине.

Самостоятельная работа студентов включает:

- изучение учебной литературы и нормативных документов по курсу;
- подготовку к практическим (лабораторным) занятиям;
- решение практических ситуаций и задач;
- работу с ресурсами информационно-телекоммуникационной сети «Интернет»;
- подготовку к тестированию по темам курса;
- подготовку к промежуточной аттестации по курсу.

Для обеспечения самостоятельной работы обучающихся используется электронный учебный курс, созданный в ЭИОС университета http://sdo.tolgas.ru/.

5. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

5.1. Перечень основной и дополнительной учебной литературы, необходимой для освоения дисциплины

Вся литература, включенная в данный перечень, представлена в виде электронных ресурсов в электронной библиотеке университета (ЭБС). Литература, используемая в печатном виде, представлена в научной библиотеке университета в объеме не менее 0,25 экземпляров на одного обучающегося.

Основная литература:

1. Мельников, В. П. Информационная безопасность и защита информации : учебное пособие / В. П. Мельников, С. А. Клейменов, А. М. Петраков. – Москва : Академия. – Текст : электронный.

2. Шаньгин, В. Ф. Информационная безопасность и защита информации / В. Ф. Шаньгин. – Москва : ДМК Пресс. – Текст : электронный.

Дополнительная литература:

3. Бирюков, А. А. Информационная безопасность: защита и нападение / А. А. Бирюков. – Москва : ДМК Пресс. – Текст : электронный.

4. Учебно-методическое пособие по дисциплине «Управление антивирусной защитой» : для студентов направления подготовки 10.03.01 «Информационная безопасность» / Поволж. гос. ун-т сервиса (ФГБОУ ВО «ПВГУС») ; сост.: Ю. С. Мунирова. – Тольятти : ПВГУС. – Текст : электронный.

5.2. Профессиональные базы данных, информационно-справочные системы, интернет-ресурсы

1. Официальный сайт Федеральной службы по техническому и экспортному контролю (ФСТЭК России) : сайт. – URL: https://fstec.ru – Текст : электронный.

2. Банк данных угроз безопасности информации ФСТЭК России (БДУ) : сайт. – URL: https://bdu.fstec.ru – Текст : электронный.

3. Реестр российского программного обеспечения : сайт. – URL: https://reestr.digital.gov.ru – Текст : электронный.

4. Электронная библиотечная система Поволжского государственного университета сервиса : сайт / ФГБОУ ВО «ПВГУС». – Тольятти. – URL: http://elib.tolgas.ru – Режим доступа: для авториз. пользователей. – Текст : электронный.

5.3. Программное обеспечение

Информационное обеспечение учебного процесса по дисциплине осуществляется с использованием следующего программного обеспечения (лицензионного и свободно распространяемого), в том числе отечественного производства:

№ п/п	Наименование	Условия доступа
1	Антивирусное программное обеспечение отечественного производства	из внутренней сети университета (лицензионный договор)
2	Средство централизованного управления антивирусной защитой	из компьютерных классов университета (лицензионный договор)
3	Microsoft Windows	из внутренней сети университета (лицензионный договор)
4	СДО MOODLE	из любой точки, в которой имеется доступ к сети Интернет (лицензионный договор)

6. ОПИСАНИЕ МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЙ БАЗЫ, НЕОБХОДИМОЙ ДЛЯ ОСУЩЕСТВЛЕНИЯ ОБРАЗОВАТЕЛЬНОГО ПРОЦЕССА ПО ДИСЦИПЛИНЕ

Помещения представляют собой учебные аудитории для проведения учебных занятий, предусмотренных учебным планом и рабочей программой дисциплины, оснащенные оборудованием и техническими средствами обучения.

Занятия лекционного типа. Учебные аудитории для занятий лекционного типа укомплектованы мебелью и техническими средствами обучения, служащими для представления учебной информации (стационарные или переносные наборы демонстрационного оборудования – проектор, экран, компьютер/ноутбук), учебно-наглядные пособия (презентации по темам лекций), обеспечивающие тематические иллюстрации, соответствующие данной программе дисциплины.

Занятия семинарского типа. Учебные аудитории для занятий семинарского типа укомплектованы мебелью и техническими средствами обучения, служащими для представления учебной информации (стационарные или переносные наборы демонстрационного оборудования – проектор, экран, компьютер/ноутбук).

Промежуточная аттестация. Для проведения промежуточной аттестации по дисциплине используются компьютерные классы, оснащенные компьютерной техникой с возможностью подключения к сети «Интернет» и обеспечением доступа в электронную информационно-образовательную среду университета, и/или учебные аудитории, укомплектованные мебелью и техническими средствами обучения.

Самостоятельная работа. Помещения для самостоятельной работы оснащены компьютерной техникой с возможностью подключения к сети «Интернет» и доступом к электронной информационно-образовательной среде университета. Для организации самостоятельной работы обучающихся используются: компьютерные классы университета; библиотека (медиазал), имеющая места для обучающихся, оснащенные компьютерами с доступом к базам данных и сети «Интернет».

Электронная информационно-образовательная среда университета (ЭИОС). Каждый обучающийся в течение всего периода обучения обеспечен индивидуальным неограниченным доступом к электронной информационно-образовательной среде университета (ЭИОС) http://sdo.tolgas.ru/ из любой точки, в которой имеется доступ к информационно-телекоммуникационной сети «Интернет», как на территории университета, так и вне ее.

ЭИОС университета обеспечивает:

доступ к учебным планам, рабочим программам дисциплин (модулей), программам практик, электронным учебным изданиям и электронным образовательным ресурсам, указанным в рабочих программах дисциплин (модулей), программах практик;

формирование электронного портфолио обучающегося, в том числе сохранение его работ и оценок за эти работы.

В случае реализации образовательной программы с применением электронного обучения, дистанционных образовательных технологий ЭИОС дополнительно обеспечивает:

фиксацию хода образовательного процесса, результатов промежуточной аттестации и результатов освоения образовательной программы;

проведение учебных занятий, процедур оценки результатов обучения, реализация которых предусмотрена с применением электронного обучения, дистанционных образовательных технологий;

взаимодействие между участниками образовательного процесса, в том числе синхронное и (или) асинхронное взаимодействия посредством сети "Интернет".

7. ОСОБЕННОСТИ ОРГАНИЗАЦИИ ОБУЧЕНИЯ ДЛЯ ЛИЦ С ОГРАНИЧЕННЫМИ ВОЗМОЖНОСТЯМИ ЗДОРОВЬЯ И ИНВАЛИДОВ

При необходимости рабочая программа дисциплины может быть адаптирована для обеспечения образовательного процесса инвалидов и лиц с ограниченными возможностями здоровья, в том числе для дистанционного обучения. Для этого требуется заявление студента (его законного представителя) и заключение психолого-медико-педагогической комиссии (ПМПК).

В случае необходимости, обучающимся из числа лиц с ограниченными возможностями здоровья (по заявлению обучающегося), а для инвалидов также в соответствии с индивидуальной программой реабилитации инвалида, могут предлагаться следующие варианты восприятия учебной информации с учетом их индивидуальных психофизических особенностей, в том числе с применением электронного обучения и дистанционных технологий:

– для лиц с нарушениями зрения: в печатной форме увеличенным шрифтом; в форме электронного документа; в форме аудиофайла; в печатной форме на языке Брайля; индивидуальные консультации с привлечением тифлосурдопереводчика; индивидуальные задания и консультации;

– для лиц с нарушениями слуха: в печатной форме; в форме электронного документа; видеоматериалы с субтитрами; индивидуальные консультации с привлечением сурдопереводчика; индивидуальные задания и консультации;

– для лиц с нарушениями опорно-двигательного аппарата: в печатной форме; в форме электронного документа; в форме аудиофайла; индивидуальные задания и консультации.

8. ОЦЕНОЧНЫЕ МАТЕРИАЛЫ (ФОНД ОЦЕНОЧНЫХ СРЕДСТВ) ДЛЯ ТЕКУЩЕГО КОНТРОЛЯ УСПЕВАЕМОСТИ И ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ

8.1. Описание показателей и критериев оценивания компетенций на различных этапах их формирования, описание шкал оценивания

Для оценки знаний, умений, навыков и уровня сформированности компетенции по дисциплине применяется балльно-рейтинговая система контроля и оценки успеваемости студентов. В основу балльно-рейтинговой системы положены принципы, в соответствии с которыми формирование рейтинга студента осуществляется в ходе текущего контроля успеваемости. Максимальное количество баллов в семестре – 100.

Шкала оценки результатов освоения дисциплины, сформированности результатов обучения

Форма проведения промежуточной аттестации	**Шкалы оценки уровня сформированности результатов обучения**		**Шкала оценки уровня освоения дисциплины**		
	Уровневая шкала оценки компетенций	100 бальная шкала, %	100 бальная шкала, %	5-балльная шкала, дифференцированная оценка/балл	недифференцированная оценка
зачет	допороговый	ниже 61	ниже 61	«неудовлетворительно» / 2	не зачтено
	пороговый	61-85,9	61-69,9	«удовлетворительно» / 3	зачтено
			70-85,9	«хорошо» / 4	зачтено
	повышенный	86-100	86-100	«отлично» / 5	зачтено

По итогам текущей успеваемости студенту может быть выставлена оценка по промежуточной аттестации в соответствии за набранными за семестр баллами (по накопительному рейтингу). Студентам, набравшим в ходе текущего контроля успеваемости по дисциплине от 61 до 100 баллов и выполнившим все обязательные виды запланированных учебных занятий, по решению преподавателя без прохождения промежуточной аттестации выставляется оценка в соответствии со шкалой оценки результатов освоения дисциплины.

***Результат обучения считается сформированным (повышенный уровень)**, если теоретическое содержание курса освоено полностью; при устных собеседованиях студент исчерпывающе, последовательно, четко и логически стройно излагает учебный материал; свободно справляется с задачами, вопросами и другими видами заданий, требующих применения знаний, использует в ответе дополнительный материал; все предусмотренные рабочей учебной программой задания выполнены в соответствии с установленными требованиями, студент способен анализировать полученные результаты; проявляет самостоятельность при выполнении заданий, качество их выполнения оценено числом баллов от 86 до 100, что соответствует повышенному уровню сформированности результатов обучения.*

***Результат обучения считается сформированным (пороговый уровень)**, если теоретическое содержание курса освоено полностью; при устных собеседованиях студент последовательно, четко и логически стройно излагает учебный материал; справляется с задачами, вопросами и другими видами заданий, требующих применения знаний; все предусмотренные рабочей учебной программой задания выполнены в соответствии с установленными требованиями, студент способен анализировать полученные результаты; проявляет самостоятельность при выполнении заданий, качество их выполнения оценено числом баллов от 61 до 85,9, что соответствует пороговому уровню сформированности результатов обучения.*

***Результат обучения считается несформированным**, если студент при выполнении заданий не демонстрирует знаний учебного материала, допускает ошибки, неуверенно, с большими затруднениями выполняет задания, не демонстрирует необходимых умений, качество выполненных заданий не соответствует установленным требованиям, качество их выполнения оценено числом баллов ниже 61, что соответствует допороговому уровню.*

Формы текущего контроля успеваемости

Формы текущего контроля	Количество контрольных точек	Баллов за 1 точку	Макс. балл
Устный опрос	3	8	24
Решение практических заданий	6	9	54
Тестирование по темам курса	2	11	22
Итого			**100 баллов**

Система оценивания представлена в электронном учебном курсе по дисциплине http://sdo.tolgas.ru/.

8.2. Типовые контрольные задания или иные материалы для ТЕКУЩЕГО КОНТРОЛЯ УСПЕВАЕМОСТИ

8.2.1. Типовые задания к практическим (лабораторным) занятиям

1. Классификация вредоносного программного обеспечения по типовым признакам.

2. Разработка схемы многоуровневой антивирусной защиты типовой автоматизированной системы.

3. Сравнительный анализ методов обнаружения вредоносного ПО.

4. Установка и настройка антивирусного средства защиты на рабочей станции.

5. Настройка централизованной политики антивирусной защиты.

6. Разбор типового инцидента, связанного с вредоносным программным обеспечением.

8.2.2. Типовые тестовые задания для текущего контроля

Правильные варианты ответов выделены жирным шрифтом.

1. Программа, способная к самостоятельному распространению по сети без участия пользователя, называется:

А) сетевым червем

Б) файловым вирусом

В) макровирусом

Г) архиватором

2. Метод обнаружения вредоносного ПО, основанный на анализе действий программы во время её выполнения, называется:

А) сигнатурным анализом

Б) поведенческим анализом

В) статическим анализом кода

Г) резервным копированием

3. Централизованная система, позволяющая управлять антивирусной защитой на всех рабочих станциях организации из единой консоли, называется:

А) системой централизованного управления антивирусной защитой

Б) системой резервного копирования

В) системой электронного документооборота

Г) системой видеонаблюдения

4. Регулярное пополнение базы данных известных вредоносных программ антивирусного средства называется:

А) обновлением сигнатурных баз

Б) дефрагментацией

В) архивированием

Г) форматированием

5. Действия, предпринимаемые организацией в случае обнаружения вредоносного программного обеспечения, регламентируются:

А) порядком реагирования на инциденты

Б) штатным расписанием

В) сметой расходов

Г) графиком отпусков

6. Файл, содержащий сведения о событиях, зафиксированных антивирусным средством защиты, называется:

А) журналом событий (логом)

Б) дистрибутивом

В) конфигурационным файлом

Г) архивом

Темы докладов/сообщений

1. Понятие и классификация вредоносного программного обеспечения.
2. Нормативные и методические документы ФСТЭК России, регламентирующие антивирусную защиту.
3. Принципы построения системы антивирусной защиты автоматизированной системы.
4. Требования к антивирусной защите информации ограниченного доступа.
5. Централизованное управление антивирусной защитой в организации.
6. Организация антивирусной защиты автоматизированных рабочих мест.

Вопросы для устного опроса

1. Архитектура и компоненты современного антивирусного средства защиты.
2. Методы обнаружения вредоносного программного обеспечения (сигнатурный, эвристический, поведенческий анализ).
3. Порядок установки антивирусного средства защиты на автоматизированное рабочее место.
4. Конфигурирование параметров работы антивирусного средства защиты.
5. Настройка расписания проверок и обновлений антивирусного средства защиты.
6. Настройка политик антивирусной защиты в централизованной системе управления.

8.3. Типовые контрольные задания или иные материалы для проведения ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ

Форма проведения промежуточной аттестации по дисциплине: зачет (по результатам накопительного рейтинга или в форме компьютерного тестирования).

Устно-письменная форма по вопросам к зачету предполагается, как правило, для сдачи академической задолженности.

Перечень вопросов для подготовки к зачету

ОПК-6. Способен при решении профессиональных задач организовывать защиту информации ограниченного доступа в соответствии с нормативными правовыми актами, нормативными и методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю

1. Понятие и классификация вредоносного программного обеспечения.
2. Нормативные и методические документы ФСТЭК России, регламентирующие антивирусную защиту.
3. Принципы построения системы антивирусной защиты автоматизированной системы.
4. Требования к антивирусной защите информации ограниченного доступа.
5. Централизованное управление антивирусной защитой в организации.
6. Организация антивирусной защиты автоматизированных рабочих мест.
7. Организация антивирусной защиты серверного оборудования.
8. Порядок реагирования на инциденты, связанные с вредоносным программным обеспечением.
9. Взаимодействие антивирусной защиты с иными подсистемами защиты информации.
10. Отчетность и документирование мероприятий по антивирусной защите.

ПК-4. Способен выполнять работы по установке, настройке и обслуживанию программных, программно-аппаратных и технических средств защиты информации автоматизированных систем

1. Архитектура и компоненты современного антивирусного средства защиты.
2. Методы обнаружения вредоносного программного обеспечения (сигнатурный, эвристический, поведенческий анализ).
3. Порядок установки антивирусного средства защиты на автоматизированное рабочее место.
4. Конфигурирование параметров работы антивирусного средства защиты.
5. Настройка расписания проверок и обновлений антивирусного средства защиты.
6. Настройка политик антивирусной защиты в централизованной системе управления.
7. Мониторинг событий антивирусной защиты и реагирование на обнаруженные угрозы.
8. Устранение неисправностей и сбоев в работе антивирусного средства защиты.
9. Обновление баз сигнатур антивирусного средства защиты.
10. Оценка эффективности функционирования системы антивирусной защиты.