Федеральное государственное бюджетное образовательное учреждение высшего образования

САНКТ-ПЕТЕРБУРГСКИЙ ГОСУДАРСТВЕННЫЙ АРХИТЕКТУРНО-СТРОИТЕЛЬНЫЙ УНИВЕРСИТЕТ

Кафедра Информационных технологий

УТВЕРЖДАЮ
Начальник учебно-методического управления
Михайлов Сергей Владимирович Подписано цифровой подписью: Михайлов Сергей Владимирович С.В. Михайлов
«29» июня 2021г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)

Компьютерная вирусология

направление подготовки/специальность 01.03.02 Прикладная математика и информатика

направленность (профиль)/специализация образовательной программы Прикладная математика и информатика

Форма обучения очная

Санкт-Петербург, 2021

1. Цели и задачи освоения дисциплины (модуля)

Целью дисциплины является освоение студентами методов, способов и средств защиты компьютерных систем и сетей от вирусов.

− изучение структуры и принципов функционирования компьютерных вирусов;

− освоение современных методов защиты информационных систем от вирусов, вредоносных программ и спама;

− изучение облачных антивирусных технологий;

− приобретение навыков построения систем защиты как для отдельных компьютеров, так и для корпоративных информационных сетей.

2. Перечень планируемых результатов обучения по дисциплине (модулю), соотнесенных с индикаторами достижения компетенций

Код и наименование компетенции	Код и наименование индикатора достижения компетенции	Планируемые результаты обучения по дисциплине, обеспечивающие достижение планируемых результатов освоения ОПОП
ПКС-1 Способность разрабатывать программное обеспечение (ПО), включая проектирование, отладку, проверку работоспособности и модификацию ПО	ПКС-1.1 знает основные языки и концепции программирования	**знает** способы, методы и алгоритмы антивирусной защиты **умеет** анализировать угрозы информационной безопасности **владеет навыками** программными средствами защиты от вирусов в виде стандартных пакетов

3. Указание места дисциплины (модуля) в структуре образовательной программы

Данная дисциплина (модуль) включена в Блок «Дисциплины, модули» Б1.В.ДВ.02.02 основной профессиональной образовательной программы 01.03.02 Прикладная математика и информатика и относится к части, формируемой участниками образовательных отношений учебного плана.

№ п/п	Предшествующие дисциплины	Код и наименование индикатора достижения компетенции
1	Архитектура ЭВМ и язык Ассемблера	ОПК-4.1, ОПК-4.3
2	Информационная безопасность и защита информации	ОПК-4.1, ОПК-4.3
3	Программные и аппаратные средства информатики	ОПК-4.1, ОПК-5.1, ОПК-5.2

Архитектура ЭВМ и язык Ассемблера
Знать архитектуру компьютера
Информационная безопасность и защита информации
Владеть основными методами защиты информации
Программные и аппаратные средства информатики
Уметь применять программные средства компьютера

№ п/п	Последующие дисциплины	Код и наименование индикатора достижения компетенции

1	Выполнение и защита выпускной квалификационной работы	УК-1.1, УК-1.2, УК-1.3, УК-2.1, УК-2.2, УК-2.3, УК-3.1, УК-3.2, УК-3.3, УК-4.1, УК-4.2, УК-4.3, УК-5.1, УК-5.2, УК-5.3, УК-6.1, УК-6.2, УК-6.3, УК-7.1, УК-7.2, УК-7.3, УК-8.1, УК-8.2, УК-8.3, ОПК-1.1, ОПК-1.2, ОПК-1.3, ОПК- 2.1, ОПК-2.2, ОПК-2.3, ОПК-3.1, ОПК-3.2, ОПК-3.3, ОПК-4.1, ОПК- 4.2, ОПК-4.3, ПКС-1.1, ПКС-1.2, ПКС-1.3, ПКС-2.1, ПКС-2.2, ПКС- 2.3, ПКС-3.1, ПКС-3.2, ПКС-3.3, ПКС-4.1, ПКС-4.2, ПКС-4.3, УК- 9.1, УК-9.2, УК-9.3, УК-9.4, УК- 9.5, УК-10.1, УК-10.2, УК-10.3, ОПК-5.1, ОПК-5.2, ПК(Ц)-1.1, ПК (Ц)-1.2, ПК(Ц)-1.3, ПК(Ц)-1.4, ПК (Ц)-1.5
2	Криптография	ОПК-4.2, ОПК-4.3

4. Объем дисциплины (модуля) в зачетных единицах с указанием количества академических часов, выделенных на контактную работу обучающихся с преподавателем (по видам учебных занятий) и на самостоятельную работу обучающихся

Вид учебной работы	Всего часов	Из них часы на практическую подготовку	Семестр
			5
Контактная работа	32		32
Лабораторные занятия (Лаб)	32	0	32
Иная контактная работа, в том числе:	0,4		0,4
консультации по курсовой работе (проекту), контрольным работам (РГР)	0,4		0,4
контактная работа на аттестацию (сдача зачета, зачета с оценкой; защита курсовой работы (проекта); сдача контрольных работ (РГР))	0,4		0,4
контактная работа на аттестацию в сессию (консультация перед экзаменом и сдача			
Часы на контроль	4		4
Самостоятельная работа (СР)	35,2		35,2
Общая трудоемкость дисциплины (модуля)			
часы:	72		72
зачетные единицы:	2		2

5. Содержание дисциплины (модуля), структурированное по разделам (темам) с указанием отведенного на них количества академических часов и видов учебных занятий

5.1. Тематический план дисциплины (модуля)

№	Разделы дисциплины	Семестр	Контактная работа (по учебным занятиям), час.						СР	Всего, час.	Код индикатора достижения компетенции
			лекции		ПЗ		ЛР				
			всего	из них на практическую подготовку	всего	из них на практическую подготовку	всего	из них на практическую подготовку			
1.	1 раздел. Основы компьютерной вирусологии										
1.1.	Определение и классификация компьютерных вирусов	5					2		4	6	ПКС-1.1
1.2.	Программная и аппаратная защита информационных систем	5					4		4	8	ПКС-1.1
1.3.	Классификация методов защиты от компьютерных вирусов	5					4		4	8	ПКС-1.1
2.	2 раздел. Защита персональных компьютеров и корпоративных систем от воздействия вирусов, вредоносных программ и спама										
2.1.	Защита отдельных персональных компьютеров	5					4		4	8	ПКС-1.1
2.2.	Системы защиты корпоративных систем и сетей	5					4		4	8	ПКС-1.1
2.3.	Программные продукты для защиты корпоративных сетей от современных интернет-угроз	5					2		4	6	ПКС-1.1
3.	3 раздел. Антивирусная защита информационных систем										
3.1.	Основы работы антивирусных программ	5					4		4	8	ПКС-1.1
3.2.	Разработка схемы антивирусной защиты	5					4		4	8	ПКС-1.1
3.3.	Российский рынок антивирусных программ	5					4		3,2	7,2	ПКС-1.1
4.	4 раздел. Иная контактная работа										
4.1.	Иная контактная работа	5								0,8	ПКС-1.1
5.	5 раздел. Контроль										
5.1.	Зачет	5								4	ПКС-1.1

5.1. Лабораторные работы

№ п/п	Наименование раздела и темы лабораторных работ	Наименование и содержание лабораторных работ
1	Определение и классификация компьютерных вирусов	Определение и классификация компьютерных вирусов Определение и классификация компьютерных вирусов. Загрузочные вирусы. Алгоритм работы загрузочного вируса. Анализ кода загрузочного вируса. Файловые вирусы в Windows. Анализ кода файлового вируса
2	Программная и аппаратная защита информационных систем	Программная и аппаратная защита информационных систем Определение и классификация компьютерных вирусов. Загрузочные вирусы. Алгоритм работы загрузочного вируса. Анализ кода загрузочного вируса. Файловые вирусы в Windows. Анализ кода файлового вируса
3	Классификация методов защиты от компьютерных вирусов	Классификация методов защиты от компьютерных вирусов Определение и классификация компьютерных вирусов. Загрузочные вирусы. Алгоритм работы загрузочного вируса. Анализ кода загрузочного вируса. Файловые вирусы в Windows. Анализ кода файлового вируса
4	Защита отдельных персональных компьютеров	Защита отдельных персональных компьютеров Защита отдельных персональных компьютеров. Подсистемы защиты корпоративных систем и сетей. Программные продукты для защиты корпоративных сетей от современных интернет - угроз
5	Системы защиты корпоративных систем и сетей	Системы защиты корпоративных систем и сетей Защита отдельных персональных компьютеров. Подсистемы защиты корпоративных систем и сетей. Программные продукты для защиты корпоративных сетей от современных интернет - угроз
6	Программные продукты для защиты корпоративных сетей от современных интернет-угроз	Программные продукты для защиты корпоративных сетей от современных интернет-угроз Защита отдельных персональных компьютеров. Подсистемы защиты корпоративных систем и сетей. Программные продукты для защиты корпоративных сетей от современных интернет - угроз
7	Основы работы антивирусных программ	Основы работы антивирусных программ Программная и аппаратная защита информационных систем. Классификация методов защиты от компьютерных вирусов. Сигнатурный анализ. Проактивные методы обнаружения. Режимы работы антивирусов. Разработка схемы антивирусной защиты
8	Разработка схемы антивирусной защиты	Разработка схемы антивирусной защиты Программная и аппаратная защита информационных систем. Классификация методов защиты от компьютерных вирусов. Сигнатурный анализ. Проактивные методы обнаружения. Режимы работы антивирусов. Разработка схемы антивирусной защиты
9	Российский рынок антивирусных программ	Российский рынок антивирусных программ Программная и аппаратная защита информационных систем. Классификация методов защиты от компьютерных вирусов. Сигнатурный анализ. Проактивные методы обнаружения. Режимы работы антивирусов. Разработка схемы антивирусной защиты

5.2. Самостоятельная работа обучающихся

№ п/п	Наименование раздела дисциплины и темы	Содержание самостоятельной работы
1	Определение и классификация компьютерных вирусов	Определение и классификация компьютерных вирусов Анализ кода вирусов, выполнение заданий.
2	Программная и аппаратная защита информационных систем	Программная и аппаратная защита информационных систем Изучение материалов по программной и аппаратной защите ИС
3	Классификация методов защиты от компьютерных вирусов	Классификация методов защиты от компьютерных вирусов Изучение материалов по программной и аппаратной защите ИС
4	Защита отдельных персональных компьютеров	Защита отдельных персональных компьютеров Работа с программными продуктами для защиты персональных компьютеров. Выполнение заданий
5	Системы защиты корпоративных систем и сетей	Системы защиты корпоративных систем и сетей Работа с программными продуктами для защиты корпоративных сетей. Выполнение заданий
6	Программные продукты для защиты корпоративных сетей от современных интернет-угроз	Программные продукты для защиты корпоративных сетей от современных интернет-угроз Работа с программными продуктами для защиты корпоративных сетей. Выполнение заданий
7	Основы работы антивирусных программ	Основы работы антивирусных программ Изучение схем антивирусной защиты.
8	Разработка схемы антивирусной защиты	Разработка схемы антивирусной защиты Разработка схемы антивирусной защиты. Выполнение заданий
9	Российский рынок антивирусных программ	Российский рынок антивирусных программ Анализ отечественных программных решений для антивирусной защиты.

6. Методические материалы для самостоятельной работы обучающихся по дисциплине (модулю)

Программой дисциплины предусмотрено проведение лабораторных занятий, предполагающих формирование у обучающихся необходимых знаний, умений и навыков. Кроме того, важнейшим этапом изучения дисциплины является самостоятельная работа обучающихся с использованием всех средств и возможностей современных образовательных технологий.

В объем самостоятельной работы по дисциплине включается следующее:

- изучение теоретических вопросов по всем темам дисциплины;
- подготовка к лабораторным занятиям;
- подготовка к текущему контролю успеваемости студентов;
- подготовка к зачету.

Залогом успешного освоения дисциплины является обязательное посещение лекционных и лабораторных занятий, так как пропуск одного (тем более, нескольких) занятий может осложнить освоение разделов курса. На лабораторных занятиях материал, изложенный на лекциях, закрепляется при выполнении заданий.

Приступая к изучению дисциплины, обучающемуся необходимо в первую очередь ознакомиться с содержанием РПД, а также методическими указаниями по организации самостоятельной работы и подготовки к практическим занятиям.

При подготовке к лабораторным занятиям и в рамках самостоятельной работы по изучению дисциплины обучающимся необходимо:

- повторить законспектированный на лекционном занятии материал и дополнить его с учетом рекомендованной по данной теме литературы;
- при самостоятельном изучении теоретической темы сделать конспект, используя рекомендованные в РПД источники;
- выполнить лабораторные задания в рамках изучаемой темы;
- ответить на контрольные вопросы по теме, используя материалы ФОС, либо групповые индивидуальные задания, подготовленные преподавателем;
- подготовиться к проверочной работе, предусмотренной в контрольных точках;
- подготовиться к промежуточной аттестации.

Итогом изучения дисциплины является зачет. Зачет проводится по расписанию. Форма проведения занятия может быть устная, письменная и в электронном виде. Студенты, не прошедшие

7. Оценочные материалы для проведения текущего контроля успеваемости и промежуточной аттестации обучающихся по дисциплине (модулю)

7.1. Перечень компетенций с указанием этапов их формирования в процессе освоения дисциплины

№ п/п	Контролируемые разделы дисциплины (модуля)	Код и наименование индикатора контролируемой компетенции	Вид оценочного средства
1	Определение и классификация компьютерных вирусов	ПКС-1.1	Коллоквиум, отчет по заданию
2	Программная и аппаратная защита информационных систем	ПКС-1.1	Коллоквиум, отчет по заданию
3	Классификация методов защиты от компьютерных вирусов	ПКС-1.1	Коллоквиум, отчет по заданию
4	Защита отдельных персональных компьютеров	ПКС-1.1	Коллоквиум, отчет по заданию
5	Системы защиты корпоративных систем и сетей	ПКС-1.1	Коллоквиум, отчет по заданию
6	Программные продукты для защиты корпоративных сетей от современных интернет-угроз	ПКС-1.1	Коллоквиум, отчет по заданию
7	Основы работы антивирусных программ	ПКС-1.1	Коллоквиум, отчет по заданию

8	Разработка схемы антивирусной защиты	ПКС-1.1	Коллоквиум, отчет по заданию
9	Российский рынок антивирусных программ	ПКС-1.1	Коллоквиум, отчет по заданию
10	Иная контактная работа	ПКС-1.1	Консультация по контрольной работе
11	Зачет	ПКС-1.1	

7.2. Типовые контрольные задания или иные материалы текущего контроля успеваемости, необходимые для оценки знаний, умений и навыков и (или) опыта профессиональной деятельности, характеризующих этапы формирования компетенций в процессе освоения дисциплины

Примерные типовые задания для проверки сформированности индикатора достижения компетенций ПКС-1.1

1. Основная особенность компьютерных вирусов заключается:

а) в возможности их самопроизвольного внедрения в различные объекты операционной системы и способность создавать свои дубликаты;

б) в неизменной структуре программного кода;

в) в изменяющейся структуре программного кода;

г) в наличии отличительных признаков

2. Вирусы, находящиеся в памяти и являющиеся активными вплоть до выключения компьютера или перезагрузки операционной системы, являются:

а) стелс-вирусами;

б) резидентными;

в) полиморфик-вирусами;

г) оперативными

3. Для борьбы с вирусами используются:

а) программные средства;

б) аппаратные средства;

в) программные и аппаратно-программные средства;

г) технические средства

4. Обнаружение изменений, вакцинирование программ, использование резидентных сторожей, сканирование, эвристический анализ являются:

а) методами обнаружения вирусов;

б) методами удаления вирусов;

в) методами модификации вирусов;

г) методами систематизации вирусов

5. Вирус имеет следующие модули:

а) модуль маскирования, модуль модификации;

б) модуль размножения, модуль модификации;

в) модуль внедрения, модуль слежения, модуль выполнения вредительских действий;

г) модуль заражения, модуль маскирования, модуль выполнения вредительских действий

6. По среде "обитания" вирусы делятся на:

а) файловые, загрузочные, макровирусы, сетевые;

б) файловые, загрузочные, черви, сетевые;

в) файловые, системные, сетевые;

г) системные, загрузочные, сетевые

7. Вирусы, не содержащие ни одного постоянного участка кода, являются:

а) оперативными;

б) полиморфик-вирусами;
в) стелс-вирусами;
г) резидентными

8. Методы борьбы с вирусами подразделяются на:
а) методы слежения и обнаружения;
б) методы слежения и удаления;
в) методы обнаружения и удаления;
г) методы обнаружения и модификации

9. Метод сканирования применим для обнаружения:
а) известных вирусов;
б) любых вирусов;
в) полиморфных вирусов;
г) неизвестных вирусов

10. Аппаратно-программная защита от вирусов предполагает использование:
а) средств запрета подключения внешних носителей;
б) средств запрета подключения к компьютерным сетям;
в) специальных паролей и ключей;
г) специальных контроллеров и их программного обеспечения

7.3. Система оценивания результатов обучения по дисциплине (модулю) при проведении текущего контроля успеваемости

Оценка «отлично» (зачтено)	знания: - систематизированные, глубокие и полные знания по всем разделам дисциплины, а также по основным вопросам, выходящим за пределы учебной программы; - точное использование научной терминологии, систематически грамотное и логически правильное изложение ответа на вопросы; - полное и глубокое усвоение основной и дополнительной литературы, рекомендованной рабочей программой по дисциплине (модулю) умения: - умеет ориентироваться в теориях, концепциях и направлениях дисциплины и давать им критическую оценку, используя научные достижения других дисциплин навыки: - высокий уровень сформированности заявленных в рабочей программе компетенций; - владеет навыками самостоятельно и творчески решать сложные проблемы и нестандартные ситуации; - применяет теоретические знания для выбора методики выполнения заданий; - грамотно обосновывает ход решения задач; - безупречно владеет инструментарием учебной дисциплины, умение его эффективно использовать в постановке научных и практических задач; - творческая самостоятельная работа на практических/семинарских/лабораторных занятиях, активно участвует в групповых обсуждениях, высокий уровень культуры исполнения заданий

Оценка «хорошо» (зачтено)	знания: - достаточно полные и систематизированные знания по дисциплине; - усвоение основной и дополнительной литературы, рекомендованной рабочей программой по дисциплине (модулю) умения: - умеет ориентироваться в основных теориях, концепциях и направлениях дисциплины и давать им критическую оценку; - использует научную терминологию, лингвистически и логически правильно излагает ответы на вопросы, умеет делать обоснованные выводы; - владеет инструментарием по дисциплине, умение его использовать в постановке и решении научных и профессиональных задач навыки: - самостоятельная работа на практических занятиях, участие в групповых обсуждениях, высокий уровень культуры исполнения заданий; - средний уровень сформированности заявленных в рабочей программе компетенций; - без затруднений выбирает стандартную методику выполнения заданий; - обосновывает ход решения задач без затруднений
Оценка «удовлетворительно» (зачтено)	знания: - достаточный минимальный объем знаний по дисциплине; - усвоение основной литературы, рекомендованной рабочей программой; - использование научной терминологии, стилистическое и логическое изложение ответа на вопросы, умение делать выводы без существенных ошибок умения: - умеет ориентироваться в основных теориях, концепциях и направлениях по дисциплине и давать им оценку; - владеет инструментарием учебной дисциплины, умение его использовать в решении типовых задач; - умеет под руководством преподавателя решать стандартные задачи навыки: - работа под руководством преподавателя на практических занятиях, допустимый уровень культуры исполнения заданий; - достаточный минимальный уровень сформированности заявленных в рабочей программе компетенций; - испытывает затруднения при обосновании алгоритма выполнения заданий
Оценка «неудовлетворительно» (не зачтено)	знания: - фрагментарные знания по дисциплине; - отказ от ответа (выполнения письменной работы); - знание отдельных источников, рекомендованных рабочей программой по дисциплине; умения: - не умеет использовать научную терминологию; - наличие грубых ошибок навыки: - низкий уровень культуры исполнения заданий; - низкий уровень сформированности заявленных в рабочей программе компетенций; - отсутствие навыков самостоятельной работы; - не может обосновать алгоритм выполнения заданий

7.4. Теоретические вопросы и практические задания для проведения промежуточной аттестации обучающихся, необходимые для оценки знаний, умений и навыков и (или) опыта профессиональной деятельности, характеризующих этапы формирования компетенций в процессе освоения образовательной программы

7.4.1. Теоретические вопросы для проведения промежуточной аттестации обучающихся

Теоретические вопросы для проведения аттестации студентов

1. Введение в компьютерную вирусологию
2. История возникновения и развития
3. Правовые аспекты борьбы с вирусами
4. Классификация вирусов
5. Способы проникновения и симптомы заражения.
6. Места существования вирусов.
7. Методы борьбы с вирусами.
8. Стандартные средства операционной системы защиты от вирусов
9. Прикладное программное обеспечение по борьбе с вирусами
10. Программа Unloker – для разблокировки заблокированных файлов
11. Пакет Comodo Internet Securyte
12. Утилита DR Web Gurelt
13. Антивирус Зайцева AVZ
14. Метод сравнения с эталоном
15. Эвристический анализ
16. Антивирусный мониторинг
17. Метод обнаружения изменений
18. Встраивание антивирусов в BIOS компьютера

7.4.2. Практические задания для проведения промежуточной аттестации обучающихся

ПРОВЕРКА РАБОТЫ АНТИВИРУСА

Цель работы: проверить работоспособность установленного Антивируса

В процессе выполнения практического задания необходимо проверить навыки:
- работы с резервным хранилищем и карантином.

1. ОСНОВНЫЕ СВЕДЕНИЯ

Завершающий этап установки любой программы - это проверка корректности выполнения основных ее функций. Для антивирусных приложений основу функционала составляет способность находить и обезвреживать вредоносные программы.

Естественно, встает вопрос: как проверить действительно ли программа может это делать - ведь известно, что новые вирусы появляются каждый день, причем десятками, а иногда и сотнями. Не каждому пользователю под силу регулярно отслеживать хотя бы их часть. Этим занимаются антивирусные компании. Их филиалы, разбросанные по всему миру, непрерывно следят за вирусной активностью в Интернет, перехватывают и анализируют все подозрительные файлы. На основе полученных данных формируются вирусные сигнатуры, которые рядовой пользователь получает во время обновления своих антивирусных баз1).

Таким образом, проверить надежность антивирусной защиты от всех уже существующих вирусов и тех, которые только завтра или через год будут созданы, нереально.

К тому же, использовать настоящие вирусы только для предварительного тестирования программы нельзя. Нельзя исключать вероятность, что программа установки где-то дала сбой и следовательно защита не установлена. Тогда во время проверки может произойти заражение вирусом, на котором производится тестирование, что недопустимо.

Но несмотря на все эти проблемы, метод диагностики антивирусных программ все же существует. Для этого используется специальный файл, "The Anti-Virus or Anti-Malware test file", созданный Европейским институтом компьютерных антивирусных исследований (European Institute for Computer Antivirus Research).

В задании 1 этой лабораторной работы предлагается познакомиться с тестовым вирусом, в заданиях 2, 3 и 4 - протестировать работу нескольких (2-3) установленных ранее Антивирусов, параллельно изучив структуру резервного хранилища и карантина, в задании 5 - провести сравнительный анализ возможностей различных Антивирусов.

Подготовка

Перед началом лабораторной работы убедитесь, что Ваш компьютер:

• Включен

• На нем загружена операционная система Microsoft Windows XP или Microsoft Windows 2000 Professional

• Выполнен вход в систему под учетной записью, обладающей правами администратора

Примечание: Скриншоты даны на примере Антивируса Касперского 7.0

2. ЗАДАНИЯ И МЕТОДИЧЕСКИЕ УКАЗАНИЯ ПО ВЫПОЛНЕНИЮ

Задание 1. Создание тестового вируса

Тестовый вирус, разработанный Европейским институтом компьютерных антивирусных исследований, называется EICAR - по аббревиатуре полного названия института (European Institute for Computer Antivirus Research).

EICAR представляет собой небольшой 68-байтный файл. Его расширение можно варьировать в зависимости от сценария тестирования. Если добавить .com, то запуск получившегося файла eicar.com на незащищенном компьютере вызовет только показ уведомления "EICAR-STANDARD- ANTIVIRUS-TEST-FILE!". Иных, свойственных вирусам проявлений он не несет. Однако если на компьютере стоит и исправно работает антивирус, EICAR будет заблокирован. Это происходит потому, что все ведущие производители антивирусных программ договорились между собой - считать EICAR вирусом и применять к нему все правила и действия, применяемые к настоящим вредоносным программам.

Для более подробного тестирования можно применять другие расширения. Например, если указать .txt, можно проверить проверяются ли текстовые файлы. Для проверки будут ли обнаруживаться вирусы в архивах, EICAR можно заархивировать.

Если открыть EICAR в каком-либо текстовом редакторе, например Блокнот (Notepad), то обнаружится, что он состоит из 68 символов:

X5O!P%@AP[4\PZX54(P^)7CC)7}$EICAR-STANDARD-ANTIVIRUS-TEST-FILE!$H+H*

Следовательно, тестовый вирус в любой момент можно создать самостоятельно. Для этого нужно только открыть любой текстовый редактор, набрать в нем эту строку и сохранить получившийся файл в формате текстового файла (обычный текст).

EICAR также всегда можно загрузить с сайта Европейского института компьютерных антивирусных исследований http://www.eicar.org .

Суть EICAR такова, что он оказывается неизлечимым. Это происходит потому, что антивирус идентифицирует EICAR как вирус по наличию в нем упомянутых 68 символов. Если их удалить - то от файла ничего не останется. Следовательно, с помощью EICAR можно тестировать только основную функцию антивируса - обнаружение.

Поэтому для тестирования своих продуктов Лаборатория Касперского предлагает использовать модифицированный тестовый вирус, а именно:

№ Файл Описание

1 CURE-EICAR Обнаружив такой файл, антивирус должен его "вылечить", сократив его размер до 4 байт (символы "CURE")

2 DELE-EICAR Этот файл Антивирус определяет как неизлечимый вирус или троянскую программу и удаляет. Следовательно, по результатам проверки DELE-EICAR должен быть обнаружен только в резервном хранилище

3 CORR-EICAR Предназначен для диагностики работы Антивируса в случае обнаружения файла с поврежденной структурой, вследствие чего проверить его на наличие вирусов невозможно. Такой файл признается условно чистым

4 ERRO-EICAR При сканировании такого файла Антивирус должен вести себя так, как будто произошла ошибка при анализе его содержимого (например, из-за нарушения целостности при проверке многотомного архива или при обрыве связи во время проверки по сети). ERRO-EICAR также признается условно чистым

5 SUSP-EICAR Этот файл корректно работающий Антивирус признает подозрительным, а именно зараженным неизвестным вирусом. Следовательно, он должен быть помещен на карантин или удален (в зависимости от настроек, по умолчанию действие при обнаружении подозрительного объекта запрашивается у пользователя)

6 WARN-EICAR WARN-EICAR также признается подозрительным, но не неизвестным вирусом, а модификацией известного. Это также приводит к предложению поместить его на карантин или удалить (в зависимости от настроек)

Создаются эти файлы по следующему принципу. 68-символьная строка с начала дополняется пятью символами, в зависимости от модификации - приставкой CURE, DELE, CORR, ERRO, SUSP или WARN и дефисом. Например, содержимое CURE-EICAR выглядит так:

CURE-X5O!P%@AP[4\PZX54(P^)7CC)7}$EICAR-STANDARD-ANTIVIRUS-TEST-FILE! $H+H*

В этом задании нужно создать тестовые вирусы EICAR, CURE-EICAR и SUSP-EICAR.

1. В этом задании нужно будет создать три файла с тестовыми вирусами: eicar.com, cure- eicar.com и susp-eicar.com. Для того, чтобы антивирус не заблокировал тестовые вирусы еще на подготовительном этапе, нужно временно отключить постоянную защиту.

Для этого вызовите контекстное меню иконки Антивируса в системной панели и выберите пункт Приостановка защиты1)

2. В открывшемся окне Приостановка защиты оставьте предложенный по умолчанию вариант После перезапуска приложения и нажмите ОК

3. После этого появится сообщение о том, что защита не работает, а иконка Антивируса обесцветится. Постоянная защита отключена

4. Запустите текстовый редактор Блокнот, воспользовавшись системным меню Пуск / Программы / Стандартные / Блокнот

5. В открывшемся окне наберите строку2)

X5O!P%@AP[4\PZX54(P^)7CC)7}$EICAR-STANDARD-ANTIVIRUS-TEST-FILE!$H+H*

6. Сохраните получившийся файл в папку C:\Test3) под именем eicar.com. Для этого воспользуйтесь меню Файл / Сохранить как…

7. В открывшемся окне перейдите к полю Имя файла и наберите в нем "C:\Test\eicar.com"

8. Вернитесь к окну Блокнота, нажав Сохранить

9. Модифицируйте EICAR, добавив к нему приставку "CURE-"

10. Сохраните получившийся файл под именем "C:\Test\cure-eicar.com", воспользовавшись командой Файл / Сохранить как…

11. Аналогично создайте SUSP-EICAR, повторив пункты 9-10, но для приставки "SUSP-"

12. Закройте окно текстового редактора Блокнот

13. В результате этих действий в папке C:\Test должно появиться три файла: eicar.com, cure - eicar.com и susp-eicar.com. Убедитесь в этом.

Откройте папку C:\Test,

14. Проверьте размер каждого из файлов. Для этого по очереди наведите курсор мыши на каждый из файлов и ознакомьтесь с информацией, представленной во всплывающем окне.

Файл eicar.com должен иметь размер 68 байт, а cure-eicar.com и susp-eicar.com - по 73 байта

15. Убедитесь, что при запуске тестовый вирус выводит предупреждающее окно. Для этого запустите eicar.com, дважды щелкнув по нему курсором мыши

16. Поскольку EICAR представляет собой приложение MS DOS, то при его запуске откроется окно сеанса MS DOS, которое сразу же после выполнения программы закроется. Для того, чтобы увидеть сообщение про то, что EICAR - это тестовый вирус, нужно запустить его через командную строку.

Воспользуйтесь системным меню Пуск / Программы/ Стандартные / Командная строка

В открывшемся окне перейдите к каталогу Test. Для этого нужно набрать команду

cd C:\Test

и нажать клавишу Enter

17. Перейдя к нужному каталогу, запустите файл eicar.com, набрав команду
eicar.com
и нажав Enter

18. Ознакомьтесь с сообщением, которое вывел EICAR

19. Закройте окно командной строки, набрав
exit
и нажав клавишу Enter

Задание 2. Тестирование с помощью EICAR

В этом задании нужно будет протестировать способность установленного Антивируса обнаруживать вирусы на примере базового тестового вируса EICAR. Предлагается это сделать с помощью задачи поиска вирусов, запускаемой из контекстного меню объектов.

В задании нужно будет при выключенной постоянной защите перейти к папке с тестовыми файлами , найти в ней eicar.com и проверить его на вирусы.

Антивирус должен найти вирус в eicar.com и запросить дальнейшие действия у пользователя. Поскольку EICAR неизлечим, функция лечения недоступна. Такие файлы всегда рекомендуется удалять, что и нужно будет выбрать в этом задании.

Дополнительно нужно проследить, что удаленные файлы не удаляются, а сначала перемещаются в резервное хранилище.

1. Перейдите к папке с тестовыми вирусами

2. Вызовите контекстное меню файла eicar.com и выберите пункт Проверить на вирусы (Сканировать… и др.)

3. Как результат, почти одновременно должны появиться два окна1). Сначала окно статистики выполнения задачи поиска вирусов

4. Поверх него в левом углу экрана - окно с запросом действия.

Обратите внимание, что окно запроса действия разделено на две области. Вверху - информация об обнаруженном вирусе: имя вируса с гиперссылкой на его описание2) и полный путь к зараженному файлу.

Ниже, в группе Действие, приводится описание заражения файла (в данном случае написано, что файл заражен вирусом EICAR и лечение его невозможно). Рядом расположены кнопки: Лечить, Удалить, Пропустить. Поскольку вылечить EICAR нельзя, то первая кнопка неактивна.

Вы можете либо пропустить, либо удалить eicar.com. Поскольку как уже говорилось ранее, все зараженные файлы удаляются не насовсем, а всего лишь перемещаются в изолированное резервное хранилище, в случае невозможности лечения рекомендуется выбирать удаление.

Нажмите Удалить

5. Обратите внимание на информационное сообщения, появившееся на несколько секунд в левом нижнем углу экрана

6. После того как Вы выбрали действие, Антивирус применит его к инфицированному файлу, в данном случае - удалит eicar.com. Это сразу же отобразится в окне статистики. Изучите представленные в нем данные и нажмите Закрыть

7. Проверьте, что удаленный файл eicar.com появился в резервном хранилище. Для этого откройте главное окно интерфейса, дважды кликните на иконке Антивируса в системной панели

8. В открывшемся окне обратите внимание на группу "Статистика" в информационной части окна.

Несмотря на то, что eicar.com был обнаружен задачей проверки по требованию, а сейчас Вы находитесь в разделе Защита, значение поля Обнаружено увеличилось на единицу. Нужно помнить,

что в этом окне выводится общая статистика

9. Перейдите к разделу Сервис, а затем к подразделу Файлы данных

10. Обратите внимание на сводную информацию о резервном хранилище, расположенную в группе "Резервное хранилище". Теперь в нем хранится один файл и следовательно размер резервного хранилище уже отличен от нуля3).

Перейдите к окну с подробной информацией о резервном хранилище, нажав на группу "Резервное хранилище"

11. Ознакомьтесь с внешним видом окна резервного хранилища. Для того, чтобы получить управление над каким-либо объектом из резервного хранилища, его нужно выделить.

Выделите строку "Заражен: вирус EICAR-Test-File"

12. Как только был выбран объект, стали активными кнопки управления им: Удалить и Восстановить. Напомним, что восстанавливать файлы из резервного хранилища настоятельно не рекомендуется.

Удалите eicar.com, нажав Удалить

13. Убедитесь, что резервное хранилище теперь пусто и закройте окно статистики, нажав Закрыть

Задание 3. Лечение инфицированных файлов

Выполнив задание 2, можно с уверенностью сказать, что установленный Антивирус обнаруживать вирусы умеет. Теперь нужно проверить, умеет ли он лечить. Это можно сделать, повторив действия предыдущего задания, только для излечимого тестового вируса CURE-EICAR. Однако мы поступим иначе. Проверим, как работает постоянная защита, а именно ее компонент, отвечающий за проверку файловой системы, Файловый Антивирус.

Для этого нужно включить постоянную защиты и затем попытаться получить доступ к cure-eicar.com.

1. В главном окне интерфейса перейдите к разделу Защита

2. Включите постоянную защиту, нажав Пуск ( ).

3. Убедитесь, что это произошло, проследив за изменениями во внешнем виде окна

4. Обратите внимание, что иконка Антивируса в системной панели снова стала цветной и прочтите появившееся информационное сообщение

5. Откройте папку C:\Test.

Поскольку ранее в задании 2, на шаге 4, было дано указание удалить файл eicar.com, а не пропустить, в папке осталось только два файла, cure-eicar.com и susp-eicar.com

6. Поскольку постоянная защита ответственна за проверку всех файлов "на лету", она с помощью компонента Файловый Антивирус должна перехватить наше обращение к cure-eicar.com, на лету вылечить и отдать нам только то, что осталось. В данном случае - 4-байтный файл, содержащий "CURE". Проверим это.

Обратитесь в файлу cure-eicar.com, один раз щелкнув по нему курсором мыши и не задевая иконку файла susp-eicar.com

7. Антивирус сразу же должен обнаружить, что Вы пытаетесь обратить к зараженному файлу. Как результат - выводится окно с запросом действия, которое нужно применить к найденному вирусу1)

8. Как и в предыдущем случае, окно разделено на две части и содержит описание ситуации и кнопки для выбора действия. Единственное отличие состоит в возможности лечения - это указано в описании файла ("Лечение возможно"), кнопка Лечить активна.

Вылечите файл cure-eicar.com, нажав Лечить

9. Об успешном результате лечения сообщает информационное окно

10. Проверьте, что оставшийся в папке C:\Test файл cure-eicar.com имеет размер всего 4 байта

11. Убедитесь, что перед лечением файл был помещен в резервное хранилище.

Для этого в главном окне интерфейса перейдите к подразделу Файлы данных и нажмите на группу "Резервное хранилище"

12. Проверьте, что теперь резервное хранилище содержит cure-eicar.com, причем его размер равен 73 байтам

13. Очистите резервное хранилище, выделив строку с EICAR и нажав Удалить

Задание 4. Помещение файлов на карантин

Как видно из предыдущих заданий, перед каждым своим вмешательством Антивирус копирует исходный файл в специальную защищенную папку, называемую резервным хранилищем. Из нее файлы рекомендуется только удалять, поскольку они или признаны инфицированными и при этом неизлечимыми, или были успешно вылечены и следует использовать их вылеченную копию.

В этом задании изучается второе хранилище Антивируса, карантин.

На карантин ставятся все подозрительные файлы - то есть такие, которые по всем признакам инфицированы, но вердикт об их неизлечимости пока не вынесен. Может быть, при следующем обновлении антивирусных баз в них будет добавлена информация, позволяющая это сделать, или же свидетельствующая о неизлечимости. В первом случае можно будет провести повторную проверку карантина и вылечить теперь уже допускающие лечение файлы, во втором - удалить с перемещением в резервное хранилище.

Еще одно отличие карантина от резервного хранилища состоит в том, что на карантин можно ставить объекты вручную, например если они у пользователя все же вызывают подозрения, несмотря на отрицательный ответ антивируса.

1. Дайте постоянной защите обнаружить последний из созданных в первом задании тестовый вирус SUSP-EICAR. Для это повторите действия предыдущего задания, но относительно файла susp-eicar.com.

Сначала перейдите к папке C:\Test и нажмите один раз на иконку файла susp-eicar.com

2. Антивирус просканирует этот файл и обнаружит его подозрительным. В результате выведется окно с просьбой выбрать необходимое действие.

Вам будет предложено три варианта: поместить на карантин, удалить или пропустить. Поскольку файл признан подозрительным, лечение невозможно (иначе бы было предложено его сначала вылечить).

Нажмите Карантин

3. Обратите внимание, что после помещения susp-eicar.com на карантин, в папке Test остался только вылеченный в предыдущем задании cure-eicar.com

4. Теперь проследите, что susp-eicar.com появился на карантине. Для этого откройте главное окно антивируса и перейдите к подразделу Файлы данных

5. Обратите внимание на сводную статистику по карантину и щелкните на группе "Карантин"

6. Вспомните, что для файлов, которые антивирус помещал в резервное хранилище вердикт был однозначен - заражен. В карантин же помещаются файлы с более мягким статусом – возможно, заражен. Таким образом, помещение на карантин подразумевает, что в дальнейшем этот вердикт может быть изменен. А изменен он может быть только при проверке с другими, более новыми или полными антивирусными базами. Поэтому по умолчанию после каждого обновления антивирусных баз все файлы на карантине перепроверяются, а для запуска перепроверки вручную на закладке Карантин есть кнопка Проверить все и контекстное меню любого объекта карантина содержит пункт Проверить

7. Выделите строку с susp-eicar.com и щелкнув на нем правой клавишей мыши, выведите контекстное меню.

Обратите внимание на пункт Отправить. Если на компьютере установлен почтовый агент, воспользовавшись этим пунктом можно быстро сформировать и отправить в службу технической поддержки Лаборатории Касперского письмо с просьбой проверить выбранный файл

8. Закройте окно статистики, нажав Закрыть

7.4.3. Примерные темы курсовой работы (проекта) (при наличии)

Курсовые работы (проекты) учебным планом не предусмотрены

7.5. Методические материалы, определяющие процедуры оценивания знаний, умений, навыков и (или) опыта профессиональной деятельности, характеризующие этапы формирования компетенций

Процедура проведения промежуточной аттестации и текущего контроля успеваемости регламентируется локальным нормативным актом, определяющим порядок организации и проведения текущего контроля успеваемости и промежуточной аттестации обучающихся.

Процедура оценивания формирования компетенций при проведении текущего контроля приведена в п. 7.2.

Типовые контрольные задания или иные материалы текущего контроля приведены в п. 7.3.

Промежуточная аттестация по дисциплине проводится в форме зачета.

7.6. Критерии оценивания сформированности компетенций при проведении промежуточной аттестации

	Уровень освоения и оценка			
	Оценка «неудовлетворительно»	Оценка «удовлетворительно»	Оценка «хорошо»	Оценка «отлично»
	«не зачтено»	«зачтено»		
Критерии оценивания	Уровень освоения компетенции «недостаточный». Компетенции не сформированы. Знания отсутствуют, умения и навыки не сформированы	Уровень освоения компетенции «пороговый». Компетенции сформированы. Сформированы базовые структуры знаний. Умения фрагментарны и носят репродуктивный характер. Демонстрируется низкий уровень самостоятельности практического навыка.	Уровень освоения компетенции «продвинутый». Компетенции сформированы. Знания обширные, системные. Умения носят репродуктивный характер, применяются к решению типовых заданий. Демонстрируется достаточный уровень самостоятельности устойчивого практического навыка.	Уровень освоения компетенции «высокий». Компетенции сформированы. Знания аргументированные, всесторонние. Умения успешно применяются к решению как типовых, так и нестандартных творческих заданий. Демонстрируется высокий уровень самостоятельности, высокая адаптивность практического навыка

знания	Обучающийся демонстрирует: -существенные пробелы в знаниях учебного материала; -допускаются принципиальные ошибки при ответе на основные вопросы билета, отсутствует знание и понимание основных понятий и категорий; -непонимание сущности дополнительных вопросов в рамках заданий билета.	Обучающийся демонстрирует: -знания теоретического материала; -неполные ответы на основные вопросы, ошибки в ответе, недостаточное понимание сущности излагаемых вопросов; -неуверенные и неточные ответы на дополнительные вопросы.	Обучающийся демонстрирует: -знание и понимание основных вопросов контролируемого объема программного материала; - знания теоретического материала -способность устанавливать и объяснять связь практики и теории, выявлять противоречия, проблемы и тенденции развития; -правильные и конкретные, без грубых ошибок, ответы на поставленные вопросы.	Обучающийся демонстрирует: -глубокие, всесторонние и аргументированные знания программного материала; -полное понимание сущности и взаимосвязи рассматриваемых процессов и явлений, точное знание основных понятий, в рамках обсуждаемых заданий; -способность устанавливать и объяснять связь практики и теории, -логически последовательные, содержательные, конкретные и исчерпывающие ответы на все задания билета, а также дополнительные вопросы экзаменатора.
умения	При выполнении практического задания билета обучающийся продемонстрировал недостаточный уровень умений. Практические задания не выполнены Обучающийся не отвечает на вопросы билета при дополнительных наводящих вопросах преподавателя.	Обучающийся выполнил практическое задание билета с существенными неточностями. Допускаются ошибки в содержании ответа и решении практических заданий. При ответах на дополнительные вопросы было допущено много неточностей.	Обучающийся выполнил практическое задание билета с небольшими неточностями. Показал хорошие умения в рамках освоенного учебного материала. Предложенные практические задания решены с небольшими неточностями. Ответил на большинство дополнительных вопросов.	Обучающийся правильно выполнил практическое задание билета. Показал отличные умения в рамках освоенного учебного материала. Решает предложенные практические задания без ошибок Ответил на все дополнительные вопросы.

владение навыками	Не может выбрать методику выполнения заданий. Допускает грубые ошибки при выполнении заданий, нарушающие логику решения задач. Делает некорректные выводы. Не может обосновать алгоритм выполнения заданий.	Испытывает затруднения по выбору методики выполнения заданий. Допускает ошибки при выполнении заданий, нарушения логики решения задач. Испытывает затруднения с формулированием корректных выводов. Испытывает затруднения при обосновании алгоритма выполнения заданий.	Без затруднений выбирает стандартную методику выполнения заданий. Допускает ошибки при выполнении заданий, не нарушающие логику решения задач Делает корректные выводы по результатам решения задачи. Обосновывает ход решения задач без затруднений.	Применяет теоретические знания для выбора методики выполнения заданий. Не допускает ошибок при выполнении заданий. Самостоятельно анализирует результаты выполнения заданий. Грамотно обосновывает ход решения задач.

Оценка по дисциплине зависит от уровня сформированности компетенций, закрепленных за дисциплиной, и представляет собой среднее арифметическое от выставленных оценок по отдельным результатам обучения (знания, умения, владение навыками).

Оценка «отлично»/«зачтено» выставляется, если среднее арифметическое находится в интервале от 4,5 до 5,0.

Оценка «хорошо»/«зачтено» выставляется, если среднее арифметическое находится в интервале от 3,5 до 4,4.

Оценка «удовлетворительно»/«зачтено» выставляется, если среднее арифметическое находится в интервале от 2,5 до 3,4.

Оценка «неудовлетворительно»/«не зачтено» выставляется, если среднее арифметическое находится в интервале от 0 до 2,4.

8. Учебно-методическое и материально-техническое обеспечение дисциплины (модуля)

8.1. Перечень основной и дополнительной литературы, необходимой для освоения дисциплины (модуля)

№ п/п	Автор, название, место издания, издательство, год издания учебной и учебно-методической литературы	Количество экземпляров/электронный адрес ЭБС
	Основная литература	
1	Нерсесянц А. А., Защита информации, Ростов-на-Дону: Северо-Кавказский филиал Московского технического университета связи и информатики, 2010	http://www.iprbookshop.ru/61295.html
2	Метелица Н. Т., Вычислительные сети и защита информации, Краснодар: Южный институт менеджмента, 2013	http://www.iprbookshop.ru/25962.html
	Дополнительная литература	
1	Ермаков Д. Г., Присяжный А. В., Применение антивирусных программ для обеспечения информационной безопасности, Екатеринбург: Уральский федеральный университет, ЭБС АСВ, 2013	http://www.iprbookshop.ru/66577.html

Обучающиеся из числа инвалидов и лиц с ОВЗ обеспечиваются печатными и (или) электронными образовательными ресурсами в формах, адаптированных к ограничениям их здоровья.

8.2. Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины (модуля)

Наименование ресурса сети «Интернет»	Электронный адрес ресурса
Компьютерные вирусы и вредоносное ПО	https://www.kaspersky.ru/resource-center/threats/computer-viruses-and-malware-facts-and-faqs
Компьютерные вирусы: история развития	https://habr.com/ru/post/497870/

8.3. Перечень современных профессиональных баз данных и информационных справочных систем

Наименование	Электронный адрес ресурса
Информационно-правовая система Гарант	\\law.lan.spbgasu.ru\GarantClient
Информационно-правовая система Консультант	\\law.lan.spbgasu.ru\ConsultantPlus ADM
Информационно-правовая база данных Кодекс	http://gasudata.lan.spbgasu.ru/docs/
Система дистанционного обучения СПбГАСУ Moodle	https://moodle.spbgasu.ru/
Электронно-библиотечная система издательства "Лань"	https://e.lanbook.com/
Электронно-библиотечная система издательства "ЮРАЙТ"	https://www.biblio-online.ru/
Периодические издания СПбГАСУ	https://www.spbgasu.ru/Universitet/Biblioteka/Periodicheskie_izdaniya/

8.4. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине, включая перечень лицензионного и свободно распространяемого программного обеспечения

Наименование	Способ распространения (лицензионное или свободно распространяемое)
Microsoft Windows 10 Pro	Договор № Д32009689201 от 18.12.2020г Программные продукты Майкрософт, договор № Д32009689201 от 18.12.2020 с АО "СофтЛайн Трейд": Windows 10, Project Professional 2016, Visio Professional 2016, Office 2016.
Microsoft Office 2016	Договор № Д32009689201 от 18.12.2020г Программные продукты Майкрософт, договор № Д32009689201 от 18.12.2020 с АО "СофтЛайн Трейд": Windows 10, Project Professional 2016, Visio Professional 2016, Office 2016.

8.5. Материально-техническое обеспечение дисциплины

Сведения об оснащенности учебных аудиторий и помещений для самостоятельной работы

Наименование учебных аудиторий и помещений для самостоятельной работы	Оснащенность оборудованием и техническими средствами обучения
47. Компьютерный класс	Рабочие места с ПК (стол компьютерный, системный блок, монитор, клавиатура, мышь), стол рабочий, подключение к компьютерной сети СПбГАСУ, выход в Internet.

47. Помещения для самостоятельной работы	Помещение для самостоятельной работы (читальный зал библиотеки, ауд. 217): ПК-23 шт., в т.ч. 1 шт.- ПК для лиц с ОВЗ (системный блок, монитор, клавиатура, мышь) с подключением к сети «Интернет» и обеспечением доступа в электронную информационно-образовательную среду СПбГАСУ. ПО Microsoft Windows 10, Microsoft Office 2016
47. Учебные аудитории для проведения практических занятий, курсового проектирования (выполнения курсовых работ), групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации	Учебная аудитория для проведения практических занятий, курсового проектирования (выполнения курсовых работ), групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации – комплект мультимедийного оборудования (персональный компьютер, мультимедийный проектор, экран, аудио-система), доска маркерная белая эмалевая, комплект учебной мебели, подключение к компьютерной сети СПбГАСУ, выход в Интернет.

Для инвалидов и лиц с ОВЗ обеспечиваются специальные условия для получения образования в соответствии с требованиями нормативно-правовых документов.