

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ
ФЕДЕРАЦИИ
федеральное государственное автономное образовательное учреждение высшего
образования
"САНКТ-ПЕТЕРБУРГСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
АЭРОКОСМИЧЕСКОГО ПРИБОРОСТРОЕНИЯ"

Кафедра № 33

УТВЕРЖДАЮ

Руководитель направления

проф., д.т.н., доц.

(должность, уч. степень, звание)

С.В. Беззатеев

(инициалы, фамилия)



(подпись)

«25» мая 2023 г

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

«Защита от вредоносных программ»

(Наименование дисциплины)

Код направления подготовки/ специальности	10.05.03
Наименование направления подготовки/ специальности	Информационная безопасность автоматизированных систем
Наименование направленности	Безопасность открытых информационных систем
Форма обучения	очная

Санкт-Петербург– 2023

Аннотация

Дисциплина «Защита от вредоносных программ» входит в образовательную программу высшего образования – программу специалитета по направлению подготовки/ специальности 10.05.03 «Информационная безопасность автоматизированных систем» направленности «Безопасность открытых информационных систем». Дисциплина реализуется кафедрой «№33».

Дисциплина нацелена на формирование у выпускника следующих компетенций:

ПК-2 «Способен формировать требования к защите информации в открытых информационных системах»

ПК-9 «Способен осуществлять работы по оценке работоспособности и эффективности применяемых программно-аппаратных средств защиты информации»

ПК-11 «Способен проводить оценку уровня информационной безопасности открытых информационных систем»

Содержание дисциплины охватывает круг вопросов, связанных с приобретением основных навыков безопасной работы на компьютере и общим представлением о методах построения систем антивирусной защиты. Для достижения этой цели на примерах изучаются базовые классы вредоносных программ, принципы действия антивирусных средств и технологии защиты от вирусов. Рассматриваются основы теории компьютерных вирусов, современные тенденции развития угроз, связанных с применением программного обеспечения, принципы и технологии, используемые для борьбы с вредоносными программами и другими сетевыми угрозами, общие принципы построения систем антивирусной защиты, а также примеры построения антивирусной защиты компьютерной сети.

Преподавание дисциплины предусматривает следующие формы организации учебного процесса: лекции, лабораторные работы, самостоятельная работа студента, консультации.

Программой дисциплины предусмотрены следующие виды контроля: текущий контроль успеваемости, промежуточная аттестация в форме зачета.

Общая трудоемкость освоения дисциплины составляет 3 зачетных единицы, 108 часов.

Язык обучения по дисциплине «русский»

1. Перечень планируемых результатов обучения по дисциплине

1.1. Цели преподавания дисциплины

Цель преподавания дисциплины «Защита от вредоносных программ» состоит в получении студентами необходимых знаний, умений и навыков в области проектирования и реализации систем антивирусной защиты, применения современного программного обеспечения, принципов и технологий, используемых для борьбы с вредоносными программами и другими сетевыми угрозами.

1.2. Дисциплина входит в состав части, формируемой участниками образовательных отношений, образовательной программы высшего образования (далее – ОП ВО).

1.3. Перечень планируемых результатов обучения по дисциплине, соотнесенных с планируемыми результатами освоения ОП ВО.

В результате изучения дисциплины обучающийся должен обладать следующими компетенциями или их частями. Компетенции и индикаторы их достижения приведены в таблице 1.

Таблица 1 – Перечень компетенций и индикаторов их достижения

Категория (группа) компетенции	Код и наименование компетенции	Код и наименование индикатора достижения компетенции
Профессиональные компетенции	ПК-2 Способен формировать требования к защите информации в открытых информационных системах	ПК-2.3.4 знать последствия от нарушения свойств безопасности информации
Профессиональные компетенции	ПК-9 Способен осуществлять работы по оценке работоспособности и эффективности применяемых программно-аппаратных средств защиты информации	ПК-9.3.4 знать криптографические алгоритмы и особенности их программной реализации
Профессиональные компетенции	ПК-11 Способен проводить оценку уровня информационной безопасности открытых информационных систем	ПК-11.В.2 владеть навыками оценки эффективности применяемых средств защиты информации, определение их уровня защищенности

2. Место дисциплины в структуре ОП

Дисциплина может базироваться на знаниях, ранее приобретенных обучающимися при изучении следующих дисциплин:

- Технологии защиты от скрытой передачи данных
- Распределенные сети хранения данных
- Распределенные информационные системы
- Программно-аппаратные средства обеспечения информационной безопасности

Знания, полученные при изучении материала данной дисциплины, имеют как самостоятельное значение, так и используются при изучении других дисциплин:

- Технологии защиты электронных платежей
- Защита банковской информации
- Научно-исследовательская работа
- Производственная преддипломная практика
- Защита информации в сенсорных сетях
- Разработка мобильных приложений
- Проектирование безопасных информационных систем
- Разработка и эксплуатация защищенных автоматизированных систем

3. Объем и трудоемкость дисциплины

Данные об общем объеме дисциплины, трудоемкости отдельных видов учебной работы по дисциплине (и распределение этой трудоемкости по семестрам) представлены в таблице 2.

Таблица 2 – Объем и трудоемкость дисциплины

Вид учебной работы	Всего	Трудоемкость по семестрам
		№8
1	2	3
Общая трудоемкость дисциплины, ЗЕ/ (час)	3/ 108	3/ 108
Из них часов практической подготовки	34	34
Аудиторные занятия, всего час.	68	68
в том числе:		
лекции (Л), (час)	34	34
практические/семинарские занятия (ПЗ), (час)		
лабораторные работы (ЛР), (час)	34	34
курсовой проект (работа) (КП, КР), (час)		
экзамен, (час)		
Самостоятельная работа, всего (час)	40	40
Вид промежуточной аттестации: зачет, дифф. зачет, экзамен (Зачет, Дифф. зач, Экз.**)	Зачет	Зачет

4. Содержание дисциплины

4.1. Распределение трудоемкости дисциплины по разделам и видам занятий.

Разделы, темы дисциплины и их трудоемкость приведены в таблице 3.

Таблица 3 – Разделы, темы дисциплины, их трудоемкость

Разделы, темы дисциплины	Лекции (час)	ПЗ (СЗ) (час)	ЛР (час)	КП (час)	СРС (час)
Семестр 8					
Раздел 1. Общая информация	2				4
Раздел 2. История компьютерных вирусов	2				4
Раздел 3. Классификация вирусов	2				4
Раздел 4. Признаки присутствия на компьютере вредоносных программ	2				4
Раздел 5. Методы защиты от вредоносных программ	2				4

Раздел 6. Основы работы антивирусных программ	4				4
Раздел 7. Классификация антивирусов	2				4
Раздел 8. Антивирусная защита компьютера	2		4		4
Раздел 9. Антивирусная защита компьютерной сети	4		8		4
Раздел 10. Антивирусная защита мобильных пользователей	4		8		4
Раздел 11. Антивирусная защита компьютерных систем	8		14		4
Итого в семестре:	34		34		40
Итого	34	0	34	0	40

Практическая подготовка заключается в непосредственном выполнении обучающимися определенных трудовых функций, связанных с будущей профессиональной деятельностью.

4.2. Содержание разделов и тем лекционных занятий.

Содержание разделов и тем лекционных занятий приведено в таблице 4.

Таблица 4 – Содержание разделов и тем лекционного цикла

Номер раздела	Название и содержание разделов и тем лекционных занятий
1	Общая информация. Дается понятие вредоносного кода, описаны способы проникновения вирусов на компьютер, последствия заражения компьютера, административные методы борьбы с вирусомисателями, уголовная ответственность
2	История компьютерных вирусов. Рассказывается как и когда появились первые вирусы, их дальнейшее развитие, мутации, принципы действия, дается перечень и краткое описание глобальных эпидемий
3	Классификация вирусов. Рассматриваются существующие типы вредоносных программ. Даются их определения, характеристики, способы распространения, вредоносная нагрузка, жизненный цикл
4	Признаки присутствия на компьютере вредоносных программ. Рассматриваются признаки, по которым можно определить заражен ли компьютер, методы обнаружения подозрительных файлов, а также действия пользователя в случае поражения компьютера вредоносной программой
5	Методы защиты от вредоносных программ. Рассматриваются существующие способы защиты компьютера от проникновения вирусов, их классификация, описания, действия, выполняемые компонентами в процессе работы
6	Основы работы антивирусных программ. Дается определение антивирусных программ, описываются существующие методы обнаружения вирусов, дополнительные средства обеспечения антивирусной безопасности, рассматриваются основные элементы антивирусной защиты
7	Классификация антивирусов. Описывается действие антивирусных программ, критерии выбора антивирусных продуктов для обеспечения эффективной защиты компьютера от проникновения вирусов
8	Антивирусная защита компьютера. Рассматриваются назначение и принципы действия программ, необходимых для полноценной и эффективной защиты компьютеров от вредоносного воздействия
9	Антивирусная защита компьютерной сети. Дается понятие локальной сети, элемента локальной сети. Рассматриваются основные

	принципы построения и управления системой антивирусной защиты локальных сетей
10	Антивирусная защита мобильных пользователей. Рассматриваются угрозы заражения мобильных пользователей, принципы действия вирусов для мобильных телефонов и средства защиты от вирусов
11	Антивирусная защита компьютерных систем. Дается понятие компьютерной системы, элемента системы. Рассматриваются основные принципы построения и управления системой антивирусной защиты компьютерных систем

4.3. Практические (семинарские) занятия

Темы практических занятий и их трудоемкость приведены в таблице 5.

Таблица 5 – Практические занятия и их трудоемкость

№ п/п	Темы практических занятий	Формы практических занятий	Трудоемкость, (час)	Из них практической подготовки, (час)	№ раздела дисциплины
Учебным планом не предусмотрено					
Всего					

4.4. Лабораторные занятия

Темы лабораторных занятий и их трудоемкость приведены в таблице 6.

Таблица 6 – Лабораторные занятия и их трудоемкость

№ п/п	Наименование лабораторных работ	Трудоемкость, (час)	Из них практической подготовки, (час)	№ раздела дисциплины
Семестр 8				
1	Установка, предварительная настройка и работа с антивирусной программой	4	4	8
2	Диагностика и оценка качества антивирусной программы	4	4	9
3	Настройка обновлений антивирусных баз	4	4	9
4	Разработка сетевой политики защиты от вредоносных программ	4	4	10
5	Подбор и анализ программного обеспечения для защиты от вредоносных программ в сети	4	4	10
6	Установка комплексной защиты от вредоносных программ	4	4	11
7	Настройка параметров комплексной защиты	4	4	11
8	Документирование процессов защиты от вредоносных программ	4	4	11
9	Тестирование системы защиты	2	2	11
Всего		34	34	

4.5. Курсовое проектирование/ выполнение курсовой работы

Учебным планом не предусмотрено

4.6. Самостоятельная работа обучающихся

Виды самостоятельной работы и ее трудоемкость приведены в таблице 7.

Таблица 7 – Виды самостоятельной работы и ее трудоемкость

Вид самостоятельной работы	Всего, час	Семестр 8, час
1	2	3
Изучение теоретического материала дисциплины (ТО)	30	30
Курсовое проектирование (КП, КР)		
Расчетно-графические задания (РГЗ)		
Выполнение реферата (Р)		
Подготовка к текущему контролю успеваемости (ТКУ)	5	5
Домашнее задание (ДЗ)		
Контрольные работы заочников (КРЗ)		
Подготовка к промежуточной аттестации (ПА)	5	5
Всего:	40	40

5. Перечень учебно-методического обеспечения

для самостоятельной работы обучающихся по дисциплине (модулю)

Учебно-методические материалы для самостоятельной работы обучающихся указаны в п.п. 7-11.

6. Перечень печатных и электронных учебных изданий

Перечень печатных и электронных учебных изданий приведен в таблице 8.

Таблица 8– Перечень печатных и электронных учебных изданий

Шифр/ URL адрес	Библиографическая ссылка	Количество экземпляров в библиотеке (кроме электронных экземпляров)
Х М 48	Мельников, В. П. Информационная безопасность и защита информации [Текст] : учебное пособие / В. П. Мельников, С. А. Клейменов, А. М. Петраков ; ред. С. А Клейменов. - 5-е изд., стер. - М. : Академия, 2011. - 331 с. : табл. - (Высшее профессиональное образование. Информатика и вычислительная техника). - Библиогр.: с. 327 - 328 (36 назв.). - ISBN 978-5-7695-7738-3 : 420.99 р. Издание имеет гриф УМО по университетскому и политехническому образованию.	26
621.391 В 74	Вопросы передачи и защиты информации [Текст] : сборник статей / С.-Петербург. гос. ун-т аэрокосм. приборостроения ; ред. Е. А. Крук. - СПб. : Изд-во ГУАП, 2011. - 332 с. : рис., табл. - Библиогр. в конце ст. - ISBN 978-5-8088-0666-5 : Б. ц.	7
004.9 И 17	Ивакин, Ян Альбертович. Информационные технологии в управлении качеством, защита информации [Текст] : учебное пособие / Я. А. Ивакин ; С.-Петербург. гос. ун-т аэрокосм. приборостроения. - СПб. : Изд-во ГУАП, 2013. - 62 с. : рис. - Библиогр.: с. 61(6 назв.). - ISBN 978-5-8088-0804-1 : Б. ц.	70

Х Б 82	Борисов, М. А. Основы организационно-правовой защиты информации [Текст] : [учебное пособие] / М. А. Борисов, О. А. Романов. - 2-е изд. - М. : Книжный дом "Либроком" : URSS, 2012. - 203 с. - (Основы защиты информации). - Библиогр.: с. 150-155. - ISBN 978-5-397-02483-9 : 282.70 р.	20
004 Р 69	Романьков, В. А. Введение в криптографию [Текст] : курс лекций / В. А. Романьков. - 2-е изд., испр. и доп. - М. : ФОРУМ, 2012. - 240 с. - Библиогр.: с. 233 - 234 (28 назв.). - Предм. указ.: с. 235 - 239. - ISBN 978-5-91134-573-0 : 337.92 р.	10
Х Б 82	Борисов, М. А. Основы организационно-правовой защиты информации [Текст] : [учебное пособие] / М. А. Борисов, О. А. Романов. - 2-е изд. - М. : Книжный дом "Либроком" : URSS, 2012. - 203 с. - (Основы защиты информации). - Библиогр.: с. 150-155. - ISBN 978-5-397-02483-9 : 282.70 р.	20
004 Р 69	Романьков, В. А. Введение в криптографию [Текст] : курс лекций / В. А. Романьков. - 2-е изд., испр. и доп. - М. : ФОРУМ, 2012. - 240 с. - Библиогр.: с. 233 - 234 (28 назв.). - Предм. указ.: с. 235 - 239. - ISBN 978-5-91134-573-0 : 337.92 р.	10

7. Перечень электронных образовательных ресурсов информационно-телекоммуникационной сети «Интернет»

Перечень электронных образовательных ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины приведен в таблице 9.

Таблица 9 – Перечень электронных образовательных ресурсов информационно-телекоммуникационной сети «Интернет»

URL адрес	Наименование
http://www.intuit.ru/	Национальный Открытый Университет «ИНТУИТ»

8. Перечень информационных технологий

8.1. Перечень программного обеспечения, используемого при осуществлении образовательного процесса по дисциплине.

Перечень используемого программного обеспечения представлен в таблице 10.

Таблица 10– Перечень программного обеспечения

№ п/п	Наименование
	Не предусмотрено

8.2. Перечень информационно-справочных систем, используемых при осуществлении образовательного процесса по дисциплине

Перечень используемых информационно-справочных систем представлен в таблице 11.

Таблица 11– Перечень информационно-справочных систем

№ п/п	Наименование
	Не предусмотрено

9. Материально-техническая база

Состав материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине, представлен в таблице 12.

Таблица 12 – Состав материально-технической базы

№ п/п	Наименование составной части материально-технической базы	Номер аудитории (при необходимости)
1	Лекционная аудитория	
2	Компьютерная лаборатория	

10. Оценочные средства для проведения промежуточной аттестации

10.1. Состав оценочных средств для проведения промежуточной аттестации обучающихся по дисциплине приведен в таблице 13.

Таблица 13 – Состав оценочных средств для проведения промежуточной аттестации

Вид промежуточной аттестации	Перечень оценочных средств
Зачет	Список вопросов; Тесты; Задачи.

10.2. В качестве критериев оценки уровня сформированности (освоения) компетенций обучающимися применяется 5-балльная шкала оценки сформированности компетенций, которая приведена в таблице 14. В течение семестра может использоваться 100-балльная шкала модульно-рейтинговой системы Университета, правила использования которой, установлены соответствующим локальным нормативным актом ГУАП.

Таблица 14 – Критерии оценки уровня сформированности компетенций

Оценка компетенции 5-балльная шкала	Характеристика сформированных компетенций
«отлично» «зачтено»	<ul style="list-style-type: none"> – обучающийся глубоко и всесторонне усвоил программный материал; – уверенно, логично, последовательно и грамотно его излагает; – опираясь на знания основной и дополнительной литературы, тесно привязывает усвоенные научные положения с практической деятельностью направления; – умело обосновывает и аргументирует выдвигаемые им идеи; – делает выводы и обобщения; – свободно владеет системой специализированных понятий.
«хорошо» «зачтено»	<ul style="list-style-type: none"> – обучающийся твердо усвоил программный материал, грамотно и по существу излагает его, опираясь на знания основной литературы; – не допускает существенных неточностей; – увязывает усвоенные знания с практической деятельностью направления; – аргументирует научные положения; – делает выводы и обобщения; – владеет системой специализированных понятий.
«удовлетворительно» «зачтено»	<ul style="list-style-type: none"> – обучающийся усвоил только основной программный материал, по существу излагает его, опираясь на знания только основной литературы; – допускает несущественные ошибки и неточности; – испытывает затруднения в практическом применении знаний направления; – слабо аргументирует научные положения; – затрудняется в формулировании выводов и обобщений; – частично владеет системой специализированных понятий.

Оценка компетенции	Характеристика сформированных компетенций
5-балльная шкала	
«неудовлетворительно» «не зачтено»	<ul style="list-style-type: none"> – обучающийся не усвоил значительной части программного материала; – допускает существенные ошибки и неточности при рассмотрении проблем в конкретном направлении; – испытывает трудности в практическом применении знаний; – не может аргументировать научные положения; – не формулирует выводов и обобщений.

10.3. Типовые контрольные задания или иные материалы.

Вопросы (задачи) для экзамена представлены в таблице 15.

Таблица 15 – Вопросы (задачи) для экзамена

№ п/п	Перечень вопросов (задач) для экзамена	Код индикатора
	Учебным планом не предусмотрено	

Вопросы (задачи) для зачета / дифф. зачета представлены в таблице 16.

Таблица 16 – Вопросы (задачи) для зачета / дифф. зачета

№ п/п	Перечень вопросов (задач) для зачета / дифф. зачета	Код индикатора
1	<p>Понятие вредоносного кода, описаны способы проникновения вирусов на компьютер</p> <p>Последствия заражения компьютера</p> <p>Административные методы борьбы с вирусомисателями, уголовная ответственность</p> <p>История компьютерных вирусов</p> <p>Классификация вирусов</p> <p>Признаки присутствия на компьютере вредоносных программ</p> <p>Методы обнаружения подозрительных файлов</p> <p>Действия пользователя в случае поражения компьютера вредоносной программой</p> <p>Методы защиты от вредоносных программ.</p>	ПК-2.3.4
2	<p>Действия, выполняемые компонентами в процессе работы</p> <p>Основы работы антивирусных программ.</p> <p>Дополнительные средства обеспечения антивирусной безопасности</p> <p>Основные элементы антивирусной защиты</p> <p>Критерии выбора антивирусных продуктов для обеспечения эффективной защиты компьютера от проникновения вирусов</p> <p>Назначение и принципы действия программ, необходимых для полноценной и эффективной защиты компьютеров от вредоносного воздействия</p>	ПК-9.3.4
3	<p>Принципы построения и управления системой антивирусной защиты локальных сетей</p> <p>Угрозы заражения мобильных пользователей</p> <p>Принципы действия вирусов для мобильных телефонов</p> <p>Средства защиты от вирусов мобильных систем</p> <p>Антивирусная защита компьютерных систем.</p> <p>Принципы построения системой антивирусной защиты компьютерных систем</p> <p>Управление системой антивирусной защиты компьютерных систем</p>	ПК-11.В.2

Перечень тем для курсового проектирования/выполнения курсовой работы представлены в таблице 17.

Таблица 17 – Перечень тем для курсового проектирования/выполнения курсовой работы

№ п/п	Примерный перечень тем для курсового проектирования/выполнения курсовой работы
	Учебным планом не предусмотрено

Вопросы для проведения промежуточной аттестации в виде тестирования представлены в таблице 18.

Таблица 18 – Примерный перечень вопросов для тестов

№ п/п	Примерный перечень вопросов для тестов	Код индикатора
	<p>1. Абстрактное описание системы, без связи с ее реализацией, дает модель политики безопасности Белла-ЛаПадула На основе анализа угроз С полным перекрытием Лендвера</p> <p>2. В модели политики безопасности Лендвера многоуровневая информационная структура называется контейнером массивом множеством объектом</p> <p>3. В модели политики безопасности Лендвера ссылка на сущность, если это идентификатор сущности, называется прямой простой циклической косвенной</p> <p>4. Выделения пользователем и администраторам только тех прав доступа, которые им необходимы это принцип минимизации привилегий принцип простоты и управляемости ИС принцип многоуровневой защиты принцип максимизации привилегий</p> <p>5. Главным параметром криптосистемы является показатель криптостойкости скорости шифрования безошибочности шифрования надежности функционирования</p> <p>6. Два ключа используются в криптосистемах с открытым ключом двойного шифрования симметричных с закрытым ключом</p> <p>7. Длина исходного ключа в ГОСТ 28147-89 (бит) 256 56 128 64</p> <p>8. Для решения проблемы правильности выбора и надежности</p>	

	<p>функционирования средств защиты в «Европейских критериях» вводится понятие адекватности средств защиты унификации средств защиты надежности защиты информации оптимизации средств защиты</p> <p>9. Достоинствами аппаратной реализации криптографического закрытия данных являются высокая производительность и простота целостность и безопасность доступность и конфиденциальность практичность и гибкость</p> <p>10. Достоинством дискретных моделей политики безопасности является простой механизм реализации числовая вероятностная оценка надежности высокая степень надежности динамичность</p> <p>11. Достоинством модели политики безопасности на основе анализа угроз системе является числовая вероятностная оценка надежности высокая степень надежности динамичность простой механизм реализации</p> <p>12. Если средства защиты могут быть преодолены только государственной спецслужбой, то согласно «Европейским критериям» безопасность считается высокой сверхвысокой стандартной базовой</p> <p>13. Если средство защиты способно противостоять отдельным атакам, то согласно «Европейским критериям» безопасность считается базовой стандартной низкой средней</p> <p>14. Защита с применением меток безопасности согласно «Оранжевой книге» используется в системах класса V1 C2 V2 C1</p> <p>15. Из перечисленного: 1) анализ потенциального злоумышленника; 2) оценка возможных затрат; 3) оценка возможных потерь; 4) анализ потенциальных угроз — процесс анализа рисков при разработке системы защиты ИС включает 3, 4 2, 4 1, 3 1, 2</p>	
--	-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	--

Перечень тем контрольных работ по дисциплине обучающихся заочной формы обучения, представлены в таблице 19.

Таблица 19 – Перечень контрольных работ

№ п/п	Перечень контрольных работ
	Не предусмотрено

10.4. Методические материалы, определяющие процедуры оценивания индикаторов, характеризующих этапы формирования компетенций, содержатся в локальных нормативных актах ГУАП, регламентирующих порядок и процедуру проведения текущего контроля успеваемости и промежуточной аттестации обучающихся ГУАП.

10. Методические указания для обучающихся по освоению дисциплины

Цель преподавания дисциплины «Защита от вредоносных программ» состоит в получении студентами необходимых знаний, умений и навыков в области проектирования и реализации систем антивирусной защиты, применения современного программного обеспечения, принципов и технологий, используемых для борьбы с вредоносными программами и другими сетевыми угрозами.

Методические указания для обучающихся по освоению лекционного материала

Основное назначение лекционного материала – логически стройное, системное, глубокое и ясное изложение учебного материала. Назначение современной лекции в рамках дисциплины не в том, чтобы получить всю информацию по теме, а в освоении фундаментальных проблем дисциплины, методов научного познания, новейших достижений научной мысли. В учебном процессе лекция выполняет методологическую, организационную и информационную функции. Лекция раскрывает понятийный аппарат конкретной области знания, её проблемы, дает цельное представление о дисциплине, показывает взаимосвязь с другими дисциплинами.

Планируемые результаты при освоении обучающимся лекционного материала:

- получение современных, целостных, взаимосвязанных знаний, уровень которых определяется целевой установкой к каждой конкретной теме;
- получение опыта творческой работы совместно с преподавателем;
- развитие профессионально–деловых качеств, любви к предмету и самостоятельного творческого мышления.
- появление необходимого интереса, необходимого для самостоятельной работы;
- получение знаний о современном уровне развития науки и техники и о прогнозе их развития на ближайшие годы;
- научиться методически обрабатывать материал (выделять главные мысли и положения, приходить к конкретным выводам, повторять их в различных формулировках);
- получение точного понимания всех необходимых терминов и понятий.

Лекционный материал может сопровождаться демонстрацией слайдов и использованием раздаточного материала при проведении коротких дискуссий об особенностях применения отдельных тематик по дисциплине.

Структура предоставления лекционного материала:

- Изложение лекционного материала;
- Представление теоретического материала преподавателем в виде слайдов;
- Освоение теоретического материала по практическим вопросам;
- Список вопросов по теме для самостоятельной работы студента (Табл.21).

Методические указания для обучающихся по прохождению лабораторных работ

В ходе выполнения лабораторных работ обучающийся должен углубить и закрепить знания, практические навыки, овладеть современной методикой и техникой эксперимента в соответствии с квалификационной характеристикой обучающегося. Выполнение лабораторных работ состоит из экспериментально-практической, расчетно-аналитической частей и контрольных мероприятий.

Выполнение лабораторных работ обучающимся является неотъемлемой частью изучения дисциплины, определяемой учебным планом, и относится к средствам, обеспечивающим решение следующих основных задач у обучающегося:

- приобретение навыков исследования процессов, явлений и объектов, изучаемых в рамках данной дисциплины;
- закрепление, развитие и детализация теоретических знаний, полученных на лекциях;
- получение новой информации по изучаемой дисциплине;
- приобретение навыков самостоятельной работы с лабораторным оборудованием и приборами.

Задание и требования к проведению лабораторных работ (ЛР)

- В задании должно быть четко сформулирована задача, выполняемая в ЛР;
- Описаны входные и выходные данные для проведения ЛР;
- ЛР должна выполняться на основе полученных теоретических знаниях;
- Выполнение ЛР должно осуществляться на основе методических указаний, предоставляемых преподавателем;
- ЛР должна выполняться в специализированном компьютерном классе и может быть доработана студентом в домашних условиях, если позволяет ПО;
- Итогом выполненной ЛР является отчет.

Структура и форма отчета о лабораторной работе

- Постановка задачи;
- Входные и выходные данные;
- Содержание этапов выполнения;
- Обоснование полученного результата (вывод);
- Список используемой литературы.

Требования к оформлению отчета о лабораторной работе

- Лабораторная работа (ЛР) предоставляется в печатном/или электронном виде;
- ЛР должна соответствовать структуре и форме отчета представленной выше;
- ЛР должна иметь титульный лист (ГОСТ 7.32-2001 издания 2008 года) с названием и подписью студента(ов), который(ые) ее сделал(и) и оформил(и);
- Студент должен защитить ЛР. Отметка о защите должна находиться на титульном листе вместе с подписью преподавателя.

Методические указания для обучающихся по прохождению самостоятельной работы

В ходе выполнения самостоятельной работы, обучающийся выполняет работу по заданию и при методическом руководстве преподавателя, но без его непосредственного участия.

Для обучающихся по заочной форме обучения, самостоятельная работа может включать в себя контрольную работу.

В процессе выполнения самостоятельной работы, у обучающегося формируется целесообразное планирование рабочего времени, которое позволяет им развивать умения и навыки в усвоении и систематизации приобретаемых знаний, обеспечивает высокий уровень успеваемости в период обучения, помогает получить навыки повышения профессионального уровня.

Методическими материалами, направляющими самостоятельную работу обучающихся являются:

- учебно-методический материал по дисциплине;
- методические указания по выполнению контрольных работ (для обучающихся по заочной форме обучения).

Методические указания для обучающихся по прохождению промежуточной аттестации

Промежуточная аттестация обучающихся предусматривает оценивание промежуточных и окончательных результатов обучения по дисциплине. Она включает в себя:

- экзамен – форма оценки знаний, полученных обучающимся в процессе изучения всей дисциплины или ее части, навыков самостоятельной работы, способности применять их для решения практических задач. Экзамен, как правило, проводится в период экзаменационной сессии и завершается аттестационной оценкой «отлично», «хорошо», «удовлетворительно», «неудовлетворительно».

- зачет – это форма оценки знаний, полученных обучающимся в ходе изучения учебной дисциплины в целом или промежуточная (по окончании семестра) оценка знаний обучающимся по отдельным разделам дисциплины с аттестационной оценкой «зачтено» или «не зачтено».

- дифференцированный зачет – это форма оценки знаний, полученных обучающимся при изучении дисциплины, при выполнении курсовых проектов, курсовых работ, научно-исследовательских работ и прохождении практик с аттестационной оценкой «отлично», «хорошо», «удовлетворительно», «неудовлетворительно».

Система оценок при проведении промежуточной аттестации осуществляется в соответствии с требованиями Положений «О текущем контроле успеваемости и промежуточной аттестации студентов ГУАП, обучающихся по программам высшего образования» и «О модульно-рейтинговой системе оценки качества учебной работы студентов в ГУАП».

Лист внесения изменений в рабочую программу дисциплины

Дата внесения изменений и дополнений. Подпись внесшего изменения	Содержание изменений и дополнений	Дата и № протокола заседания кафедры	Подпись зав. кафедрой