

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)

«27» мая 2022 г

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ


«Анализ защищенности компьютерных систем»
(Наименование дисциплины)

Код направления подготовки/ специальности	10.04.01
Наименование направления подготовки/ специальности	Информационная безопасность
Наименование направленности	Интеллектуальные средства обеспечения безопасности объектов
Форма обучения	очная

Санкт-Петербург– 2022

Лист согласования рабочей программы дисциплины


Программу составил (а)

<u>доц.,к.т.н.,доц.</u>	 <u>27.05.22</u>	<u>В.А. Мыльников</u>
(должность, уч. степень, звание)	(подпись, дата)	(инициалы, фамилия)

Программа одобрена на заседании кафедры № 33

«27» мая 2022 г, протокол № 10


Заведующий кафедрой № 33

<u>д.т.н.,доц.</u>	 <u>27.05.22</u>	<u>С.В. Беззатеев</u>
(уч. степень, звание)	(подпись, дата)	(инициалы, фамилия)

Ответственный за ОП ВО 10.04.01(01)

<u>доц.,к.т.н.,доц.</u>	 <u>27.05.22</u>	<u>В.А. Мыльников</u>
(должность, уч. степень, звание)	(подпись, дата)	(инициалы, фамилия)

Заместитель директора института №3 по методической работе

<u></u>	 <u>27.05.22</u>	<u>Н.В. Решетникова</u>
(должность, уч. степень, звание)	(подпись, дата)	(инициалы, фамилия)

Аннотация

Дисциплина «Анализ защищенности компьютерных систем» входит в образовательную программу высшего образования – программу магистратуры по направлению подготовки/специальности 10.04.01 «Информационная безопасность» направленности «Интеллектуальные средства обеспечения безопасности объектов». Дисциплина реализуется кафедрой «№33».

Дисциплина нацелена на формирование у выпускника следующих компетенций:

ПК-5 «Способен разрабатывать требования по защите и формировать политики безопасности компьютерных систем и сетей»

Содержание дисциплины охватывает круг вопросов, связанных изучением терминологии, понятийного аппарата и общих подходов к обеспечению информационной безопасности автоматизированных систем.

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 экзамена.

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

Целью преподавания дисциплины «Анализ защищенности компьютерных систем» является изучение терминологии, понятийного аппарата и общих подходов к обеспечению информационной безопасности автоматизированных систем и анализу их защищенности.

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-5 Способен разрабатывать требования по защите и формировать политики безопасности компьютерных систем и сетей	ПК-5.3.1 знает виды политик безопасности компьютерных систем и сетей ПК-5.У.1 умеет формулировать задания по безопасности компьютерных систем ПК-5.В.1 владеет разработкой профилей защиты и заданий по безопасности

2. Место дисциплины в структуре ОП

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

- «Теоретические основы компьютерной безопасности»,
- «Теория систем и системный анализ».

Знания, полученные при изучении материала данной дисциплины, имеют как самостоятельное значение, так и могут использоваться при написании выпускной квалификационной работы магистра.

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
		№3
1	2	3
Общая трудоемкость дисциплины, ЗЕ/ (час)	3/ 108	3/ 108
Из них часов практической подготовки	34	34
Аудиторные занятия, всего час.	51	51
в том числе:		
лекции (Л), (час)	17	17
практические/семинарские занятия (ПЗ), (час)		
лабораторные работы (ЛР), (час)	17	17
курсовой проект (работа) (КП, КР), (час)	17	17
экзамен, (час)	36	36

Самостоятельная работа , всего (час)	21	21
Вид промежуточной аттестации: зачет, дифф. зачет, экзамен (Зачет, Дифф. зач, Экз.**)	Экз.	Экз.

Примечание: ** кандидатский экзамен

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 3					
Раздел 1. Управление рисками.	5		4		10
Раздел 2. Методики построения систем защиты информации.	4		4		8
Раздел 3. Методики и программные продукты для оценки рисков.	4		4		10
Раздел 4. Разработка рекомендаций по снижению рисков нарушения безопасности защищенной информационной системы.	4		5		10
Выполнение курсовой работы				17	
Итого в семестре:	17		17	17	21
Итого	17	0	17	17	21

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	Тема 1.1. Модель безопасности с полным перекрытием. Тема 1.2. Стандарты в области информационной безопасности, использующие концепцию управление рисками ISO/IEC 15408. Тема 1.3. Критерии оценки безопасности информационных технологий. Тема 1.4. Стандарты ISO/IEC 17799/27002 и 27001
2	Тема 2.1. Модель многоуровневой защиты. Тема 2.2. Анализ существующих подходов построения систем защиты информации. Тема 2.3. Технические мероприятия по снижению уровня риска.
3	Тема 3.1. Методика CRAMM. Тема 3.2. Методика FRAP. Тема 3.3. Методика OCTAVE. Тема 3.4. Методика RiskWatch.

4	Тема 4.1. Идентификация и аутентификация. Тема 4.2. Протокол Kerberos. Тема 4.3. Инфраструктура открытых ключей. Цифровые сертификаты. Тема 4.4. Протокол защиты электронной почты S/MIME. Тема 4.5. Протокол IPSec.
---	--

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 3				
1	Методики построения систем защиты Информации Lifecycle Security	2	2	1
2	Методика управления рисками, предлагаемая Microsoft	2	2	2
3	Критерии оценки безопасности информационных технологий.	2	2	1
4	Исследование методики CRAMM построения систем защиты информации	2	2	2, 3
5	Исследование методики OCTAVE построения систем защиты информации	2	2	2, 3
6	Исследование методики RiskWatch построения Систем защиты информации	2	2	2, 3
7	Разработка модели многоуровневой защиты	2	2	2
8	Разработка рекомендаций по снижению рисков нарушения безопасности защищенной информационной системы	2	2	2
9	Инфраструктура открытых ключей. Цифровые сертификаты.	1	1	4
Всего		17	17	

4.5. Курсовое проектирование/ выполнение курсовой работы

Цель курсовой работы: освоение методов и средств защиты информации. Часов практической подготовки: 17.

Примерные темы заданий на курсовую работу приведены в разделе 10 РПД.

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 3, час
1	2	3
Изучение теоретического материала дисциплины (ТО)	8	8
Курсовое проектирование (КП, КР)		
Расчетно-графические задания (РГЗ)		
Выполнение реферата (Р)		
Подготовка к текущему контролю успеваемости (ТКУ)	4	4
Домашнее задание (ДЗ)	9	9
Контрольные работы заочников (КРЗ)		
Подготовка к промежуточной аттестации (ПА)		
Всего:	21	21

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)
004 Б 91	Бураков, М. В. Базы данных и язык SQL [Текст]: учебное пособие / М. В. Бураков, Р. Р. Латыпова; С.-Петерб. гос. ун-т аэрокосм. приборостроения. - СПб.: Изд-во ГУАП, 2014. - 120 с.	50
004.4 М 15	Маклафлин, Б. PHP и MySQL. Исчерпывающее руководство [Текст] = PHP & MySQL. The missing manual / Б. Маклафлин. - 2-е изд. - СПб.: ПИТЕР, 2014. - 544 с.	30
004 М 87	Мошак Н. Н. Организация безопасного доступа к информационным ресурсам [Текст]: учебное пособие / Н. Н. Мошак, Т. М. Татарникова. - СПб.: Изд-во ГУАП, 2014. - 121 с.	40
004 К 56	Коваленко, В. В. Проектирование информационных систем [Текст]: учебное пособие / В. В. Коваленко. - М.: ФОРУМ: ИНФРА-М, 2015. - 320 с.	10
004.4 К 60	Колисниченко, Д. Н. PHP и MySQL. Разработка веб-приложений [Текст] / Д. Н. Колисниченко. - 5-е изд. - СПб. : БХВ - Петербург, 2015. - 592 с.	5

004 К 56	Коваленко, В. В. Проектирование информационных систем: учебное пособие / В. В. Коваленко. - М.: ФОРУМ: ИНФРА-М, 2015. -320 с.	10
004 М87	Мошак Н.Н. Безопасность информационных систем: Учеб. пособие/ Н.Н.Мошак – СПб.: ГУАП, 2019. – 169 с. ISBN 978-5-8088-1414-1	40
004 М87	Мошак Н.Н. Безопасность информационных систем: учеб. -метод. пособие/ Н.Н.Мошак – СПб.: ГУАП, 2020. – 73 с.	30
004 М87	Мошак Н.Н. Защита информационных систем: учеб. -метод. пособие/ Н.Н.Мошак – СПб.: ГУАП, 2020. – 154 с.	30
004 М87	Мошак Н.Н. Основы управления информационной безопасностью: Учеб. пособие/ Н.Н.Мошак; под ред. В.В. Овчинникова. – СПб.: ГУАП, 2022. – 141 с. ISBN 978-5-8088-1711-1	40
http://znanium.com/catalog.php?bookinfo=405313	Безопасность и управление доступом в информационных системах: Учебное пособие / А.В. Васильков, И.А. Васильков. - М.: Форум: НИЦ ИНФРА-М, 2013. - 368 с.	

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://e.lanbook.com/view/book/1121/	Безопасность Oracle глазами аудитора: нападение и защита/А.М. Поляков ДМК Пресс, 2010, 336 с.
http://e.lanbook.com/view/book/1122/	Защита компьютерной информации/В.Ф. Шаньгин. - ДМК Пресс, 2010. 544 с.
http://www.znanium.com/bookread.php?book=175658	Комплексная система защиты информации на предприятии: учебное пособие/Н.В. Гришина. - М.: Форум, 2009, 240 с.
http://e.lanbook.com/view/book/1919/	Обеспечение безопасности организаций и производственных объектов: Практическое пособие для руководителей и работников предприятий и организаций/Петров С.В. ЭНАС, 2007, 224 с.

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
1	Операционная система MS Windows
2	Пакет MS Office
3	VMware ESXi

8.2. Перечень информационно-справочных систем,используемых при осуществлении образовательного процесса по дисциплине
Перечень используемых информационно-справочных систем представлен втаблице 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 таблице12.

Таблица 12 – Состав материально-технической базы

№ п/п	Наименование составной частиматериально-технической базы	Номер аудитории (при необходимости)
1	Лекционная аудитория	
2	Компьютерный класс	

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
Экзамен	Список вопросов к экзамену.
Выполнение курсовой работы	Экспертная оценка на основе требований к содержанию курсовой работы по дисциплине.

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»	– 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.
Оценка компетенции 5-балльная шкала	Характеристика сформированных компетенций

«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.
«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
1	<p>Модель безопасности с полным перекрытием.</p> <p>Модель нарушителя.</p> <p>Оценка информационных рисков.</p> <p>Обработка информационных рисков.</p> <p>Управление рисками.</p> <p>Табличные методы оценки рисков.</p> <p>Архитектура информационной системы</p> <p>Современные стандарты в области информационной безопасности,использующие концепцию управление рисками ISO/IEC 15408.</p> <p>Оценочные стандарты ИБ.</p> <p>Ценность ресурсов ИС.</p> <p>Критерии оценки безопасности информационных систем.</p> <p>Стандарты управления ИБ</p> <p>Модель многоуровневой защиты.</p> <p>Анализ существующих подходов построения систем защиты информации.</p> <p>Технические мероприятия по снижению уровня риска.</p>	ПК-5.3.1

2	<p>Сравнительные характеристики методов анализа рисков.</p> <p>Методика CRAMM. Недостатки.</p> <p>Методика CRAMM. Стадии исследования.</p> <p>Методика FRAP. Этапы оценки рисков.</p> <p>Методика FRAP. Построение матрицы рисков.</p> <p>Методика OCTAVE. Фазы анализа рисков.</p> <p>Методика OCTAVE. Построение профиля угрозы.</p> <p>Методика RiskWatch. Критерии оценки.</p> <p>Методика RiskWatch. Характеристика программного продукта. Эффект от внедрения.</p> <p>Идентификация и аутентификация.</p> <p>Протокол Kerberos.</p> <p>Инфраструктура открытых ключей. Цифровые сертификаты.</p> <p>Защита электронной почты.</p> <p>Протокол S/MIME.</p> <p>Протокол IPSec.</p> <p>Организационные мероприятия по защите информации в ИС</p>	ПК-5.У.1
3	<p>Программа генерирует N-символьные пароли следующим образом: в качестве символов используются десятичные цифры, а также строчные и прописные латинские буквы в любом порядке (в латинском алфавите 26 знаков). Все символы кодируются одним и тем же минимально возможным количеством бит и записываются на диск.</p> <p>Программа сгенерировала 128 паролей и записала их в файл подряд, без дополнительных символов. Размер полученного файла составил 1,5 Кбайта. Какова длина пароля (N)?</p> <p>Данные объемом 16 Мбайт поступают на компьютер по линии со скоростью передачи данных 32 Мбит/сек. После получения 4 Мбайт компьютер начинает одновременно передавать эти данные по другой линии связи со скоростью 4 Мбит/сек. Сколько секунд пройдет от начала приема данных по высокоскоростному каналу до полной передачи их по низкоскоростному каналу?</p>	ПК-5.В.1

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
	Учебным планом не предусмотрено	

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
-------	--

1	Источники, риски и формы атак на компьютерные системы
2	Модели безопасности информационных систем
3	Защита информации в современных операционных системах
4	Защита информации в сети
5	Виды политик информационной безопасности
6	Математические модели информационной безопасности
7	Технологии аутентификации
8	Защита информации на прикладном уровне
9	Система отслеживания вторжений

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>Идентификация и аутентификации применяются для ...</p> <ul style="list-style-type: none"> · регистрации событий безопасности · выявления попыток несанкционированного доступа · обеспечения целостности данных · для ограничения доступа случайных и незаконных субъектов информационной системы к её объектам <p>Анализ накопленной информации, проводимый оперативно, в реальном времени или периодически называется – ...</p> <ul style="list-style-type: none"> · Аудит <p>Анализ накопленной информации, проводимый оперативно, в реальном времени или периодически называется ...</p> <ul style="list-style-type: none"> · аудит · идентификация · аутентификации · шифрование <p>Оперативный аудит с автоматическим реагированием на выявленные нештатные ситуации называется ...</p> <ul style="list-style-type: none"> · активным <p>Оперативный аудит с автоматическим реагированием на выявленные нештатные ситуации называется ...</p> <ul style="list-style-type: none"> · активным · оперативным · неотложным · автоматическим <p>Управление доступом, представляющее собой разграничение доступа между поименованными субъектами и поименованными объектами, называется ...</p> <ul style="list-style-type: none"> · дискретное · мандатное · принудительное · статистическое <p>Аутентификация, которая обеспечивает защиту только от несанкционированных действий</p> <p>в системах, где нарушитель не может во время сеанса работы прочитать аутентификационную информацию, называется ...</p> <ul style="list-style-type: none"> · статической · устойчивой · постоянной · переменной <p>Примером средства ... аутентификации являются традиционные постоянные пароли.</p> <ul style="list-style-type: none"> · статической · устойчивой 	ПК-5.У.1

<ul style="list-style-type: none"> · постоянной · переменной <p>Аутентификация, которая использует динамические данные аутентификации, меняющиеся с каждым сеансом работы, называется</p> <p>...</p> <ul style="list-style-type: none"> · устойчивой · статической · постоянной · переменной <p>Реализациями ... аутентификации являются системы, использующие одноразовые пароли и электронные подписи.</p> <ul style="list-style-type: none"> · устойчивой · статической · постоянной · переменной 	
--	--

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.

11. Методические указания для обучающихся по освоению дисциплины

11.1. 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 обучающимися 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:

Раздел 1. Управление рисками.

Тема 1.1. Модель безопасности с полным перекрытием.

Тема 1.2. Стандарты в области информационной безопасности, использующие концепцию управление рисками ISO/IEC 15408.

Тема 1.3. Критерии оценки безопасности информационных технологий. Тема 1.4.

Стандарты ISO/IEC 17799/27002 и 27001.

Раздел 2. Методики построения систем защиты информации. Тема 2.1.

Модель многоуровневой защиты.

Тема 2.2. Анализ существующих подходов построения систем защиты информации.

Тема 2.3. Технические мероприятия по снижению уровня риска. Раздел 3.

Методики и программные продукты для оценки рисков. Тема 3.1. Методика CRAMM.

Тема 3.2. Методика FRAP. Тема 3.3.

Методика OCTAVE. Тема 3.4. Методика

RiskWatch.

Раздел 4. Разработка рекомендаций по снижению рисков нарушения безопасности защищенной информационной системы.

Тема 4.1. Идентификация и аутентификация. Тема 4.2.

Протокол Kerberos.

Тема 4.3. Инфраструктура открытых ключей. Цифровые сертификаты. Тема 4.4.

Протокол защиты электронной почты S/MIME.

Тема 4.5. Протокол IPSec..

11.2. Методические указания для обучающихся по выполнению 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 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

Вариант задания по каждой лабораторной работе обучающийся получает в соответствии с номером в списке группы. Перед проведением лабораторной работы обучающемуся следует внимательно ознакомиться с методическими указаниями по ее выполнению. В соответствии с заданием обучающийся должен подготовить необходимые данные, получить от преподавателя допуск к выполнению лабораторной работы, выполнить указанную последовательность действий, получить требуемые результаты, оформить и защитить отчет по лабораторной работе.

Структура и форма отчета о лабораторной работе

Отчет о лабораторной работе должен включать в себя: титульный лист, формулировку задания, теоретические положения, используемые при выполнении лабораторной работы, описание процесса выполнения лабораторной работы, полученные результаты и выводы.

Требования к оформлению отчета о лабораторной работе

По каждой лабораторной работе выполняется отдельный отчет. Титульный лист оформляется в соответствии с шаблоном (образцом) приведенным на сайте ГУАП (www.guar.ru) в разделе «Сектор нормативной документации». Текстовые и графические материалы оформляются в соответствии с действующими ГОСТами и требованиями, приведенными на сайте ГУАП (www.guar.ru) в разделе «Сектор нормативной документации».

Методические указания по прохождению лабораторных работ:

1. [004.056(075) Т 33] Беззатеев С. В. Теория информационной безопасности и методология защиты информации: методические указания к выполнению лабораторных работ № 1. - СПб.: ГОУ ВПО "СПбГУАП", 2007. Кол-во экз. в библиот. – 88.

2. [519.7 М 34] И. Л. Ерош, М. Ю. Литвинов, Н. В. Соловьев. Математические основы защиты информации: методические указания к выполнению лабораторных работ. СПб.: ГОУ ВПО "СПбГУАП", 2008. - 31 с. Кол-во экз. в библи. – 74.

11.3. Методические указания для обучающихся по прохождению курсового проектирования/выполнения курсовой работы

Курсовой проект/ работа проводится с целью формирования у обучающихся опыта комплексного решения конкретных задач профессиональной деятельности.

Курсовой проект/ работа позволяет обучающемуся:

- систематизировать и закрепить полученные теоретические знания и практические умения по профессиональным учебным дисциплинам и модулям в соответствии с требованиями к уровню подготовки, установленными программой учебной дисциплины, программой подготовки специалиста соответствующего уровня, квалификации;
- применить полученные знания, умения и практический опыт при решении комплексных задач, в соответствии с основными видами профессиональной деятельности по направлению/ специальности/ программе;
- углубить теоретические знания в соответствии с заданной темой;
- сформировать умения применять теоретические знания при решении нестандартных задач;
- приобрести опыт аналитической, расчётной, конструкторской работы и сформировать соответствующие умения;
- сформировать умения работы со специальной литературой, справочной, нормативной и правовой документацией и иными информационными источниками;
- сформировать умения формулировать логически обоснованные выводы, предложения и рекомендации по результатам выполнения работы;
- развить профессиональную письменную и устную речь обучающегося;
- развить системное мышление, творческую инициативу,
- самостоятельность, организованность и ответственность за принимаемые решения;
- сформировать навыки планомерной регулярной работы над решением поставленных задач.

Структура пояснительной записки курсового проекта/ работы

1. Постановка задачи
2. Основная часть
3. Расчетная/аналитическая часть
4. Выводы

Требования к оформлению пояснительной записки курсового проекта/ работы

- Оформление с использованием стилей
- MS Word (OO Writer) или TeX
- Наличие оглавления
- Наличие ссылок на литературу
- Наличие подписей к картинкам

Титульный лист оформляется в соответствии с шаблоном (образцом) приведенным на сайте ГУАП (www.guap.ru) в разделе «Сектор нормативной документации». Текстовые и графические материалы оформляются в соответствии с действующими ГОСТами и требованиями, приведенными на сайте ГУАП (www.guap.ru) в разделе «Сектор нормативной документации».

11.4. 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 является учебно-методический материал по дисциплине.

Для развития у студентов навыков самостоятельного овладения теоретическим материалом ряд тем дисциплины на лекционных занятиях дается обзорно, что предполагает их самостоятельное детальное изучение.

Перечень тем для самостоятельного изучения:

- Модель безопасности с полным перекрытием.
- Стандарты в области информационной безопасности, использующие концепцию управление рисками ISO/IEC 15408.
- Критерии оценки безопасности информационных технологий.
- Стандарты ISO/IEC 17799/27002 и 27001.
- Технические мероприятия по снижению уровня риска.
- Методика CRAMM.
- Методика FRAP.
- Методика OCTAVE.
- Методика RiskWatch.
- Протокол защиты электронной почты S/MIME.

11.5. Методические указания для обучающихся по прохождению текущего контроля успеваемости.

Текущий контроль успеваемости предусматривает контроль качества знаний обучающихся, осуществляемого в течение семестра с целью оценивания хода освоения дисциплины.

Текущий контроль успеваемости предусматривает контроль качества знаний обучающихся, осуществляемого в течение семестра с целью оценивания хода освоения дисциплины. Форма проведения текущего контроля – защита отчетов по лабораторным работам. Результаты текущего контроля учитываются при проведении промежуточной аттестации в соответствии с требованиями СТО ГУАП. СМК 3.76 «Положение о текущем контроле успеваемости и промежуточной аттестации студентов и аспирантов ГУАП, обучающихся по образовательным программам высшего образования».

11.6. 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.

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».

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