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

«Комплексные системы защиты информации в правоохранительной сфере»
(Наименование дисциплины)

| | |
|---|---|
| Код направления подготовки/ специальности | 10.05.05 |
| Наименование направления подготовки/ специальности | Безопасность информационных технологий в правоохранительной сфере |
| Наименование направленности | Организация и технологии защиты информации (в информационных системах) |
| Форма обучения | очная |

Санкт-Петербург– 2023

Лист согласования рабочей программы дисциплины

Программу составил (а)

| д.т.н.,доц. | 25.05.23 | С.В. Беззатеев |
|---|---|---|
| (должность, уч. степень, звание) | (подпись, дата) | (инициалы, фамилия) |

Программа одобрена на заседании кафедры № 33

«25» мая 2023 г, протокол № 10

Заведующий кафедрой № 33

| д.т.н.,доц. | 25.05.23 | С.В. Беззатеев |
|---|---|---|
| (уч. степень, звание) | (подпись, дата) | (инициалы, фамилия) |

Ответственный за ОП ВО 10.05.05(05)

| доц.,к.т.н.,доц. | 25.05.23 | В.А. Мыльников |
|---|---|---|
| (должность, уч. степень, звание) | (подпись, дата) | (инициалы, фамилия) |

Заместитель директора института №3 по методической работе

| | 25.05.23 | Н.В. Решетникова |
|---|---|---|
| (должность, уч. степень, звание) | (подпись, дата) | (инициалы, фамилия) |

Аннотация

Дисциплина «Комплексные системы защиты информации в правоохранительной сфере» входит в образовательную программу высшего образования – программу специалитета по направлению подготовки/ специальности 10.05.05 «Безопасность информационных технологий в правоохранительной сфере» направленности «Организация и технологии защиты информации (в информационных системах)». Дисциплина реализуется кафедрой «№33».

Дисциплина нацелена на формирование у выпускника следующих компетенций:

ПК-7 «Способен формировать и поддерживать в актуальном состоянии автоматизированные базы и банки данных, использовать информационно-поисковые и логико-аналитические системы»

ПК-8 «Способен анализировать структуру и содержание информационных массивов и информационных процессов на предмет выявления угроз безопасности»

Содержание дисциплины охватывает круг вопросов, связанных с наиболее важными понятиями в сфере создания и эксплуатации автоматизированных систем защиты информации (АСЗИ), раскрывает вопросы нормативно-методической регламентации функциональной структуры (архитектуры) подсистем безопасности защищенных компьютерных систем (КС), функциональные требования безопасности к продуктам и системам информационных технологий (ИТ), жизненный цикл, порядок создания и эксплуатации защищенных КС, продуктов и систем ИТ, удовлетворяющих требованиям информационной безопасности.

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 дисциплины «Комплексные системы защиты информации в правоохранительной сфере» – формирование компетентности разработки и эксплуатации автоматизированных систем защиты информации отдельных компонентов автоматизированных систем, с учетом требований нормативно-технической и методической документации по обеспечению безопасности информации. – изучение безопасности информации в автоматизированных системах и освоение методик оценки данных угроз; - изучение методов, способов, средств, последовательности и содержания этапов разработки автоматизированных систем и подсистем безопасности автоматизированных систем в правоохранительной сфере; изучение основных мер по защите информации в автоматизированных системах; - изучение содержания и порядка деятельности персонала по эксплуатации защищенных автоматизированных систем.

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-7 Способен формировать и поддерживать в актуальном состоянии автоматизированные базы и банки данных, использовать информационно-поисковые и логико-аналитические системы | ПК-7.З.1 знать назначение информационно-поисковых, логико-аналитических и экспертных систем, их тактико-технические характеристики и порядок применения в правоохранительных органах<br>ПК-7.З.2 знать сущность и методики информационного и аналитического поиска, источники информации, необходимые для их осуществления<br>ПК-7.З.3 знать понятие и структуру автоматизированной базы данных (программное обеспечение, банк данных, база знаний, система управления базами данных и т.д.)<br>ПК-7.У.1 уметь разрабатывать модели данных, администрировать автоматизированные базы и банки данных<br>ПК-7.В.1 владеть навыками освоения и внедрения в практику администрирования новых технологий работы с базами данных |
| Профессиональные компетенции | ПК-8 Способен анализировать структуру и содержание информационных массивов и информационных процессов на | ПК-8.З.1 знать методики проведения анализа оперативной обстановки, правила оформления результатов криминального анализа<br>ПК-8.З.2 знать классификацию источников угроз и нарушителей информационной безопасности<br>ПК-8.У.1 уметь проводить анализ |

| | | |
|---|---|---|
| | предмет выявления угроз безопасности | вероятности реализации угрозы и ущерба от ее возникновения<br>ПК-8.В.1 владеть навыками использования информационных сервисов для автоматизации прикладных и информационных процессов анализа систем защиты информации |

## 2. Место дисциплины в структуре ОП

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

- Теория вероятностей и математическая статистика»
- «Математическая логика и теория алгоритмов»
- «Дискретная математик»
- «Вычислительная математика»
- «Информатика и информационные технологии в правоохранительной деятельности»
- «Математические основы обработки информации»
- «Языки программирования»
- «Технологии и методы программирования»
- «Основы информационной безопасности»
- «Программно-аппаратная защита информации»
- «Системы и сети передачи информации»
- «Теория систем и системный анализ»
- «Моделирование систем»
- «Интеллектуальные системы и технологии»

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

- Техническая защита информации
- Организационная защита информации
- Управление информационной безопасностью
- Теория информации
- Предметно-ориентированные автоматизированные информационные системы

## 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 |
|---|---|---|
| | | №9 |
| 1 | 2 | 3 |
| ***Общая трудоемкость дисциплины***, ЗЕ/ (час) | 3/ 108 | 3/ 108 |
| ***Из них часов практической подготовки*** | 17 | 17 |
| ***Аудиторные занятия***, всего час. | 34 | 34 |
| 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) | | |
| экзамен, (час) | | |
| ***Самостоятельная работа***, всего (час) | 74 | 74 |
| ***Вид промежуточной аттестации*:** зачет, дифф. зачет, экзамен (Зачет, Дифф. зач, Экз.**) | Зачет | Зачет |

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 9 | | | | | |
| Раздел 1. Понятие и особенности автоматизированной системы защиты информации<br>Тема 1.1. Функционал автоматизированной системы защиты информации.<br>Тема 1.2. Организация администрирования автоматизированных систем. Административный персонал и работа с пользователями.<br>Тема 1.3. Управление, тестирование и эксплуатация автоматизированных систем.<br>Тема 1.4. Методы, способы и средства обеспечения отказоустойчивости автоматизированных систем. | 2 | | 2 | | 10 |
| Раздел 2. Критерии оценки защищенности автоматизированных систем<br>Тема 2.1. Международные и российские стандарты оценки защищенности. Классы защищенности АС.<br>Тема 2.2. Общий подход к формированию критериев оценки безопасности информационных технологий.<br>Тема 2.3. Модели угроз и зашиты объекта оценки. Последовательность формирования требований и спецификаций.<br>Тема 2.4. Понятие профиля защиты и его особенности. Требования общих критериев и результаты оценки. | 4 | | 4 | | 16 |
| Раздел 3. Особенности эксплуатации автоматизированных систем защиты информации<br>Тема 3.1. Анализ информационной инфраструктуры автоматизированной системы и ее безопасности.<br>Тема 3.2. Разработка и ведение эксплуатационной документации защищенных автоматизированных систем<br>Тема 3.2. Методы мониторинга и аудита, выявления угроз информационной безопасности автоматизированных систем. | 4 | | 4 | | 16 |

| | | | | | |
|---|---|---|---|---|---|
| Раздел 4. Разработка автоматизированных систем защиты информации<br>Тема 4.1. Общие требования по разработке автоматизированных систем защиты информации<br>Тема 4.2. Работы на стадиях и этапах создания автоматизированных систем защиты информации<br>Тема 4.3. Требования по защите сведений о создаваемой автоматизированной системе. | 4 | | 4 | | 16 |
| Раздел 5. Стадии и этапы разработки автоматизированных систем<br>Тема 5.1. Жизненный цикл автоматизированной системы.<br>Тема 5.2. Оценка угроз безопасности автоматизированных систем<br>Тема 5.3. Особенности разработки информационных систем персональных данных.<br>Тема 5.4. Реализация моделей безопасности автоматизированных систем<br>Тема 5.5. Администрирование информационной безопасности автоматизированных систем | 3 | | 3 | | 16 |
| Итого в семестре: | 17 | | 17 | | 74 |
| Итого | 17 | 0 | 17 | 0 | 74 |
| | | | | | |

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** | **Понятие и особенности автоматизированной системы защиты информации**<br>Тема 1.1. Функционал автоматизированной системы защиты информации. (демонстрация слайдов)<br>Тема 1.2. Организация администрирования автоматизированных систем. Административный персонал и работа с пользователями. (демонстрация слайдов)<br>Тема 1.3. Управление, тестирование и эксплуатация автоматизированных систем. (демонстрация слайдов)<br>Тема 1.4. Методы, способы и средства обеспечения отказоустойчивости автоматизированных систем (демонстрация слайдов) |
| **2** | **Критерии оценки защищенности автоматизированных систем**<br>Тема 2.1. Международные и российские стандарты оценки защищенности. Классы защищенности АС. (демонстрация слайдов)<br>Тема 2.2. Общий подход к формированию критериев оценки безопасности информационных технологий. (демонстрация слайдов)<br>Тема 2.3. Модели угроз и зашиты объекта оценки. Последовательность формирования требований и спецификаций. (демонстрация слайдов) |

| | |
|---|---|
| | Тема 2.4. Понятие профиля защиты и его особенности. Требования общих критериев и результаты оценки. (демонстрация слайдов) |
| **3** | **Особенности эксплуатации автоматизированных систем в защищенном исполнении**<br>Тема 3.1. Анализ информационной инфраструктуры автоматизированной системы и ее безопасности. (демонстрация слайдов)<br>Тема 3.2. Разработка и ведение эксплуатационной документации защищенных автоматизированных систем. (демонстрация слайдов)<br>Тема 3.2. Методы мониторинга и аудита, выявления угроз информационной безопасности автоматизированных систем. (демонстрация слайдов) |
| **4** | **Разработка автоматизированных систем в защищенном исполнении**<br>Тема 4.1. Общие требования по разработке автоматизированных систем защиты информации. (демонстрация слайдов)<br>Тема 4.2. Работы на стадиях и этапах создания автоматизированных систем защиты информации. (демонстрация слайдов)<br>Тема 4.3. Требования по защите сведений о создаваемой автоматизированной системе. (демонстрация слайдов) |
| **5** | **Стадии и этапы разработки автоматизированных систем**<br>Тема 5.1. Жизненный цикл автоматизированной системы. (демонстрация слайдов)<br>Тема 5.2. Оценка угроз безопасности автоматизированных систем (демонстрация слайдов)<br>Тема 5.3. Особенности разработки информационных систем персональных данных. (демонстрация слайдов)<br>Тема 5.4. Реализация моделей безопасности автоматизированных систем (демонстрация слайдов)<br>Тема 5.5. Администрирование информационной безопасности автоматизированных систем (демонстрация слайдов) |

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 9 | | | | |
| 1 | «Описание объекта исследования с точки | 4 | 4 | 1,2 |

| | | | | |
|---|---|---|---|---|
| | зрения администратора по информационной безопасности» | | | |
| 2 | «Построение инфологических моделей, защищенных ИС» | 4 | 4 | 3 |
| 3 | «Разработка политик безопасности информации» | 4 | 4 | 3,4 |
| 4 | «Сбор логов событий информационной безопасности в AirSIEM» | 5 | 4 | 4,5 |
| | Всего | 17 | | |

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 9, час |
|---|---|---|
| 1 | 2 | 3 |
| Изучение теоретического материала дисциплины (ТО) | 20 | 20 |
| Курсовое проектирование (КП, КР) | - | - |
| Расчетно-графические задания (РГЗ) | - | - |
| Выполнение реферата (Р) | - | - |
| Подготовка к текущему контролю успеваемости (ТКУ) | 14 | 14 |
| Домашнее задание (ДЗ) | - | - |
| Контрольные работы заочников (КРЗ) | - | - |
| Подготовка к промежуточной аттестации (ПА) | 20 | 20 |
| Всего: | 74 | 74 |

## 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) |
|---|---|---|
| 37<br>Г 72 | Государственная итоговая аттестация : методические указания по подготовке к государственному экзамену и написанию и защите выпускной квалификационной | 5 |

| | | |
|---|---|---|
| | работы / С.-Петерб. гос. ун-т аэрокосм. приборостроения ; сост.: С. Г. Фомичева, Т. Н. Елина, В. А. Мыльников. - Санкт-Петербург : Изд-во ГУАП, 2021. - 79 с. : рис., табл. - Библиогр.: с. 79 (10 назв.). - Б. ц. - Текст : непосредственный. | |
| 004<br>Ф 76 | Фомичева, Светлана Григорьевна.<br>Обработка информации в распределенных системах : учебное пособие / С. Г. Фомичева ; С.-Петерб. гос. ун-т аэрокосм. приборостроения. - Санкт-Петербург : Изд-во ГУАП, 2020. - 132 с. ; 131 с. : рис. - Библиогр.: с. 123 (17 назв.). - ISBN 978-5-8088-1487-5 : Б. ц. - Текст : непосредственный | 5 |
| 004<br>Б 39 | Беззатеев, Сергей Валентинович (д-р техн. наук, доц.).<br>Программирование задач по обеспечению информационной безопасности : лабораторный практикум / С. В. Беззатеев, С. Г. Фомичева ; С.-Петерб. гос. ун-т аэрокосм. приборостроения. - Санкт-Петербург : Изд-во ГУАП, 2020. - 89 с. : рис., табл. - Библиогр.: с. 88 (10 назв.). - Б. ц. - Текст : непосредственный. | 5 |
| 004<br>З-62 | Зима, В. М.<br>Безопасность глобальных сетевых технологий / В. М. Зима, А. А. Молдовян, Н. А. Молдовян. - 2-е изд. - СПб. : БХВ - Петербург, 2015. - 368 с. : рис. - (Мастер систем). - Библиогр.: с. 351 - 353 (31 назв.).- Предм. указ.:с. 354 - 362. - ISBN 978-5-94157-213-7 : 419.00 р. - Текст : непосредственный | 7 |
| 007<br>В 67 | Волкова, В. Н.<br>Теория систем и системный анализ : учебник для академического бакалавриата / В. Н. Волкова, А. А. Денисов ; Нац. исслед. С.-Петерб. гос. политехн. ун-т. - 2-е изд., перераб. и доп. - М. : Юрайт, 2015. - 616 с. : рис. - (Бакалавр. Академический курс). - Предм. указ.: с. 600 - 606. - Имен. указ.: с. 607 - 609. - Библиогр.: с. 610 - 616 (109 назв.). - ISBN 978-5-9916-4783-0 : 870.87 р. - Текст : непосредственный. Имеет гриф УМО высшего образования | 10 |
| 004<br>И 85 | Исаев, Г. Н.<br>Проектирование информационных систем : учебное пособие / Г. Н. Исаев. - 2-е изд., стер. - М. : ОМЕГА-Л, 2015. - 424 с. | 5 |

| | | |
|---|---|---|
| | : рис., табл. - (Высшее техническое образование). - Библиогр.: с. 421 - 424 (61 назв.) . - ISBN 978-5-370-03507-4 : 401.60 р. - Текст : непосредственный.<br>На стр. 7 - 8: Список сокращений | |
| 004<br>Б 24 | Баранова, Е. К.<br>Информационная безопасность и защита информации : учебное пособие / Е. К. Баранова, А. В. Бабаш. - 3-е изд., перераб. и доп. - М. : РИОР : ИНФРА-М, 2017. - 322 с. : рис., табл. - (Высшее образование). - Библиогр.: с. 313 - 316 (56 назв.). - ISBN 978-5-369-01450-9 (РИОР). - ISBN 978-5-16-011164-3 (ИНФРА-М) : 942.63 р. - Текст : непосредственный.<br>Имеет гриф УМО по образованию в области прикладной информатики | 5 |
| 004.4<br>И 46 | Ильина, Дарья Викторовна.<br>Проектирование и разработка безопасных веб-приложений : учебное пособие / Д. В. Ильина ; С.-Петерб. гос. ун-т аэрокосм. приборостроения. - Санкт-Петербург : Изд-во ГУАП, 2019. - 43 с. : рис. - Библиогр.: с. 42 (2 назв.). - ISBN 978-5-8088-1434-9 : Б. ц. - Текст : непосредственный. | 5 |
| 004.7<br>К 95 | Кучин, Николай Валентинович (доц.).<br>Многоуровневые системы и облачные вычисления : учебное пособие / Н. В. Кучин, А. Ю. Молчанов ; С.-Петерб. гос. ун-т аэрокосм. приборостроения. - СПб. : Изд-во ГУАП, 2018. - 136 с. : рис. - Библиогр.: с. 133 (14 назв.). - ISBN 978-5-8088-1250-5 : Б. ц. - Текст : непосредственный | 4 |

## 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 |
|---|---|
| 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 таблице12.

Таблица 12 – Состав материально-технической базы

| № п/п | Наименование составной части материально-технической базы | Номер аудитории (при необходимости) |
|---|---|---|
| 1 | Лекционная аудитория | |
| 2 | Мультимедийная лекционная аудитория | |
| 3 | Компьютерный класс | |

## 10. Оценочные средства для проведения промежуточной аттестации

10.1. Состав оценочных средствдля 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;<br>Тесты;<br>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<br>5-балльная шкала | Характеристика сформированных компетенций |
|---|---|
| «отлично»<br>«зачтено» | – обучающийся глубоко и всесторонне усвоил программный материал;<br>– уверенно, логично, последовательно и грамотно его излагает;<br>– опираясь на знания основной и дополнительной литературы, тесно привязывает усвоенные научные положения с практической деятельностью направления;<br>– умело обосновывает и аргументирует выдвигаемые им идеи;<br>– делает выводы и обобщения; |

| Оценка компетенции<br>5-балльная шкала | Характеристика сформированных компетенций |
|---|---|
| | – свободно владеет системой специализированных понятий. |
| «хорошо»<br>«зачтено» | – обучающийся твердо усвоил программный материал, грамотно и по существу излагает его, опираясь на знания основной литературы;<br>– не допускает существенных неточностей;<br>– увязывает усвоенные знания с практической деятельностью направления;<br>– аргументирует научные положения;<br>– делает выводы и обобщения;<br>– владеет системой специализированных понятий. |
| «удовлетворительно»<br>«зачтено» | – обучающийся усвоил только основной программный материал, по существу излагает его, опираясь на знания только основной литературы;<br>– допускает несущественные ошибки и неточности;<br>– испытывает затруднения в практическом применении знаний направления;<br>– слабо аргументирует научные положения;<br>– затрудняется в формулировании выводов и обобщений;<br>– частично владеет системой специализированных понятий. |
| «неудовлетворительно»<br>«не зачтено» | – обучающийся не усвоил значительной части программного материала;<br>– допускает существенные ошибки и неточности при рассмотрении проблем в конкретном направлении;<br>– испытывает трудности в практическом применении знаний;<br>– не может аргументировать научные положения;<br>– 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. | Понятие, виды и структура автоматизированных систем (по РД 50-680-88)<br>Организационная структура, схемы организации работ при проектировании АС и организационные формы проектного коллектива<br>Содержание и специфика управленческого цикла при проектировании АС<br>Методы планирования и управления проектами.<br>Диаграммы Гантта, сетевые графики проектов<br>Автоматизированные системы управления проектами | ПК-7.З.1 |

| | | |
|---|---|---|
| 2. | Безопасность АС, ее составляющие. Основные способы и механизмы обеспечения безопасности информации в АС<br>Органы управления и планирования эксплуатации защищенных АС<br>Эксплуатационная документация на АС (изделия ИТ). Руководства пользователя и администратора<br>Конструкторские эксплуатационные документы на ТСО и ПО, эксплуатационные документы предприятия | ПК-7.З.2 |
| 3. | Классификация, идентификация (инвентаризация, каталогизация) и оценивание (категорирование) объектов защиты в АС<br>Общие положения по эксплуатации изделий, комплексов, средств деятельности. Составляющие организационных и технических мероприятий по эксплуатации<br>Особенности эксплуатации КС (АС) и защищенных КС (АС в защищенном исполнении). Администрирование КС (АС) | ПК-7.З.3 |
| 4. | Классификация (каталогизация), идентификация, спецификация и оценивание угроз безопасности в АС<br>Содержание процесса разработки и ввода в действие изделий (систем) ИТ. Уровни представления проектных решений<br>Проектирование АС как особый вид деятельности, объекты проектирования при создании АС (по РД 50-680-88)<br>Методология (методы и средства) проектирования АС<br>Каноническое (индивидуальное) проектирование АС. Технологическая схема этапов технического и рабочего проектирования<br>Типовое проектирование АС и его методы. Технологическая схема проектирования<br>Управление процессом проектирования АС, его компоненты и специфика | ПК-7.У.1 |
| 5. | Человеческий фактор в угрозах безопасности. Модель нарушителя безопасности информации в АС<br>Жизненный цикл, стадии создания и содержание работ по созданию АС, особенности создания АС в защищенном исполнении (по ГОСТ 34.601-90, ГОСТ Р 51583)<br>Классификация изделий ИТ и функциональные пакеты требований безопасности. Классы защищенности изделий ИТ и пакеты требований доверия безопасности (по ГОСТ Р ИСО/МЭК 15408-2002)<br>Структура, порядок разработки, регистрации и опубликования профилей защиты для изделий ИТ (по ГОСТ Р ИСО/МЭК 15408-2002)<br>Структура, назначение и порядок разработки задания по безопасности при создании изделий ИТ, соотношение между профилем защиты и заданием по безопасности. Техническое задание на создание системы ИТ (по ГОСТ Р ИСО/МЭК 15408-2002) | ПК-7.В.1 |
| 6. | Декомпозиция назначения, целей и задач | ПК-8.З.1 |

| | | |
|---|---|---|
| | функционирования АС. Функциональная структура АС и функциональные требования к защищенным СВТ, АС, продуктам и системам ИТ<br>Услуги (сервисы) безопасности при взаимодействии открытых систем и механизмы безопасности, их реализующие (по ГОСТ Р ИСО 7498-1-99), взаимоотношение между услугами защиты и уровнями взаимодействия по 7-ми уровневой эталонной модели ВО | |
| 7. | Система и структура функциональных требований по защите от НСД к информации в СВТ), классы защищенности СВТ<br>Особенности Технического задания на создание АС в защищенном исполнении. Составляющие общих требований к АСЗИ и структуру функциональных требований (по ГОСТ Р 51624) | ПК-8.З.2 |
| 8. | Система и структура функциональных требований по защите от НСД в АС), группы и классы защищенности АС<br>Техническое задание на создание АС, требования по структуре, содержанию, порядку разработки, оформления, согласования и утверждения (по ГОСТ 34.602-89) | ПК-8.У.1 |
| 9. | Общая структура требований безопасности к изделиям и системам ИТ, классыфункциональных требований безопасности (по ГОСТ Р ИСО/МЭК 15408-2002. Ч.2)<br>Жизненный цикл изделий (продуктов и систем) ИТ, общая схема и последовательность создания изделий ИТ | ПК-8.В.1 |

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 |
|---|---|---|
| | Различают следующие уровни управления ИБ организации<br>1) Стратегический<br>2) Тактический<br>3) Промежуточный<br>4) Оперативный<br>К преимуществам использования SIEM систем относят –<br>1) Оперативный контроль защищенности на всех уровнях системы<br>2) Не требуется высокая квалификация оператора SIEM системы<br>3) Использование документно-ориентированных баз данных | ПК-7.З.1 |

| | | |
|---|---|---|
| | Снижение стоимости владения системой | |
| | При проведении обследования организации основными источниками информации являются<br>1) Документы организации, процедуры<br>2) Политики организации<br>3) Результаты интервьюирования сотрудников<br>4) Технологические карт | ПК-7.З.2 |
| | single loss expectancy - SLE<br>1) ожидаемый годовой ущерб<br>2) Величина ожидаемого разового ущерба<br>3) ежегодная частота возникновения риска<br>4) стоимость актива для каждого риска | ПК-7.З.3 |
| | национальная база данных уязвимостей США;:<br>1) Common Vulnerabilities and Exposures<br>2) National Vulnerability Database<br>3) Open Sourced Vulnerability Database<br>4) Public Vulnerability Database | ПК-7.У.1 |
| | Вектор угрозы – это<br>1) Набор скалярных значений<br>2) текстовая строка, которая содержит значения, связанные с каждой метрикой<br>3) Массив элементов<br>4) нет правильного ответа | ПК-7.В.1 |
| | C:[N,L,H] метрика указывает насколько сильно в случае успешного использования уязвимости пострадает<br>1) Доступность<br>2) Конфиденциальность<br>3) Целостность<br>4) Надежность | ПК-8.З.1 |
| | У вектора уязвимости<br>CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:L/I:L/A:N<br>Значение метрики S:U означает<br>1) user<br>2) unique<br>3) unchanged<br>4) updated | ПК-8.З.2 |
| | Низкой вероятности реализации угроз соответствуют критерии<br>1) отсутствует мотивация для реализации j-ой угрозы<br>2) отсутствует требуемая статистика по фактам реализации j-ой угрозы безопасности информации<br>3) отсутствуют объективные предпосылки к реализации j-ой угрозы безопасности информации<br>4) возможная частота реализации j-ой угрозы не превышает 1 раза в 5 лет<br>Политика информационной безопасности позволяет<br>1) определить «правила игры» для всех сотрудников организации и третьих лиц<br>2) Разработать архитектуру защищаемой ИС<br>3) составить общую основу для защиты всех влияющих на ОИБ активов организации, в рамках которой определяются правила разграничения доступа к этим | ПК-8.У.1 |

| | | |
|---|---|---|
| | активам<br>сделать правильный выбор самой платформы для работы с активами, учитывая, какие инструментальные средства и процедуры будут использованы | |
| | Системный анализ только определение потребности и назначения ИС<br>1) только определение основных функциональных характеристик ИС<br>2) только оценка затрат и эффективности использования ИС<br>3) определение потребности и назначения ИС, ее основных функциональных характеристик ИС,<br>4) оценка затрат и эффективности использования<br>Актуализация угроз безопасности информации заключается в оценке<br>1) Вероятности реализации угрозы<br>2) Степени риска<br>3) Возможности реализации угрозы<br>4) Степени ущерба | ПК-8.В.1 |

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:

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

11.2. Методические указания для обучающихся по участию в семинарах - *учебным планом не предусмотрено* .

.

11.3. Методические указания для обучающихся по прохождению практических занятий - *учебным планом не предусмотрено*

11.4. 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

**Лабораторная работа № 1** «Описание объекта исследования с точки зрения администратора по информационной безопасности»

Цель лабораторной работы № 1: Построение различных моделей, отображающих архитектуру автоматизированной системы ограничений доступа к информации и проведение анализа мест и видов утечки информации. Оценка степени защищенности информации.

Задание к лабораторной работе №1

1) Выполнить оценку актуальности, разрабатываемой информационной
2) системы
3) Провести структурный системный анализ бизнес-процессов
4) предметной области. Построить диаграммы IDEF0 (AS-IS), DFD (ASIS), (при необходимости – IDEF3 (AS-IS).
5) Описать разработанные диаграммы

6) Выделить активы (критические элементы), подлежащие информационной защите

Структура и форма отчета о лабораторной работе

Отчет по лабораторным работам должна отражать не факт спроектированной системы защиты, а процесс проектирования, показывающий всю работу над проектом начиная от полученного исходного материала и наброска будущей защищенной информационной системы и заканчивая разработанным и протестированным программным пакетом, с обоснованием всех принятых в процессе проектирования решений. В содержании должна быть отражена структура отчета. Введение должно характеризовать ту сферу человеческой деятельности, для которой будет проектироваться приложение. При описании диаграмм должны быть изложены основные функциональные возможности будущей системы защиты информации, а также виды информации которые придется хранить и обрабатывать для достижения поставленной цели. В последующих лабораторных работах должны быть изложены этапы конструирования и функционирования программно-технических устройств защиты информации и технических объектов от несанкционированного доступа.

Требования к оформлению отчета о лабораторной работе

- Отчёт о лабораторной работе (ЛР) предоставляется в печатном/или электронном виде;
- Отчёт о лабораторной работе должен соответствовать структуре и форме отчета, представленной выше;
- Отчёт о лабораторной работе должен 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.

Ссылка на ЛР1 - https://pro.guap.ru/get-task/78006590fcaa9bfc1ad5022f9065d23b

**Лабораторная работа № 2** «Построение инфологических моделей, защищенных ИС»

Цель лабораторной работы № 2: Построение инфологических моделей, защищенных ИС и баз данных с защищенными полями и установленными правами и привилегиями доступа к данным Оценка степени защищенности информации.

Задание к лабораторной работе №2

1) Построить модель угроз разрабатываемой информационной системы
2) Построить модель нарушителя
3) Сформировать реестр актуализированных угроз для каждого актива
4) Оценить возможные риски
5) Провести структурный системный анализ бизнес-процессов предметной области. Построить диаграммы IDEF0 (TO-BE), DFD (TOBE), (при необходимости – IDEF3 (TO-BE).
6) Описать разработанные диаграммы
7) Оценить степень защищенности информации

При выполнении лабораторной работы студенту отводится роль администратора сети предприятия или администратора баз данных. В соответствии с заданной ролью необходимо спроектировать систему защиты информации для конкретного участка сети. Для решения данной задачи также необходимо:

1) Распределить участников сети по помещениям предприятия, учитывая разделение служащих предприятия на группы по заданному признаку.

2) Составить структурную схему своего участка сети с указанием возможных каналов утечки информации и проблем защиты.

Структура и форма отчета о лабораторной работе

Должны быть изложены этапы конструирования и функционирования программно-технических устройств защиты информации и технических объектов от несанкционированного доступа.

Ссылка на ЛР 2 - https://pro.guap.ru/get-task/a8e23daa5916a441df4694dfc8e89059

**Лабораторная работа № 3** «Разработка политик безопасности информации»

Цель лабораторной работы № 3: Оценка защищенности информационной системы, формирование корпоративной и частных политик информационной безопасности, реализующих требуемый уровень защищенности системы.

Задание к лабораторной работе №3

1) На основании предположений безопасности, при учете угроз и имеющихся уязвимостей (модели угроз, полученной в лабораторной работе № 1) сформулировать цели безопасности, определить класс и категорию защищенности информационной (автоматизированной) системы.
2) Руководствуясь ГОСТ Р ИСО/МЭК ТО 13335, ГОСТ Р ИСО/МЭК 17799 и ГОСТ Р ИСО/МЭК 27001 выполнить априорную оценку и приоритизацию рисков, а также соблюдение законодательных и нормативных актов для рассматриваемой информационной системы (Для оценки рекомендуется использовать программное средство MICROSOFT SECURITY ASSESSMENT TOOL) https://www.microsoft.com/ru-ru/download/details.aspx?id=12273)
3) Результаты экспертной оценки рисков ИБ, полученные на предыдущем шаге использовать для формирования корпоративной и необходимого числа частных политик, позволяющих привести защищаемую систему к соответствию ISO 17799 с учетом приоритизации рисков
4) Провести оценку защищенности, эксплуатируемой или проектируемой информационной системы с учетом адаптации правил политик информационной безопасности (красных кружков в экспертной оценке не должно остаться).
5) Выделить в политиках информационной безопасности внесенные изменения
6) Оформить отчет по лабораторной работе.

Ссылка на ЛР 3 - https://pro.guap.ru/get-task/72f5bfd68686b1c0ef4ae3a25fb7d448

**Лабораторная работа № 4** «Сбор логов событий информационной безопасности в AirSIEM»

Цель лабораторной работы № 4: разработать систему, которая позволяет анализировать регистрируемые в защищаемой инфраструктуре события, поступающие от различных источников, и обнаруживать атаки/сценарии атак/подозрительные действия/отклонения от нормы, формируя при необходимости соответствующие инциденты безопасности.

Задание к лабораторной работе №4

1) Сформировать технические политики ИБ
2) На основании разработанных политик информационной безопасности, профилей защиты и заданий по безопасности информационной (автоматизированной) системы и/или СЗИ, разработать архитектуру SIEM-системы
3) Развернуть SIEM-экосистему, используя проект AirSIEM https://github.com/fisher85/AirSIEM
4) Исходный код ядра корреляции - https://github.com/fisher85/AirSIEM/tree/master/AirSIEM
5) Реализовать подсистему сбора и хранения поступающих событий безопасности;

6) Оформить отчет по лабораторной работе.
Ссылка на ЛР 4 - https://pro.guap.ru/get-task/c2d006368e42beb0e8e4c26dc7612b6f

11.5. Методические указания для обучающихся по прохождению курсового проектирования/выполнения курсовой работы - *учебным планом не предусмотрено*

11.6. 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 обучающихсяявляются:

– учебно-методический материал по дисциплине;

– методические указания по выполнению контрольных работ (для обучающихся по заочной форме обучения).

11.7. 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.

11.8. 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 |
|---|---|---|---|
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |