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)

«26» мая 2022 г

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

«Технологии защиты от скрытой передачи данных»
(Наименование дисциплины)

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

Санкт-Петербург– 2022

Лист согласования рабочей программы дисциплины

Программу составил (а)

проф.,к.т.н.,проф. 26.05.22 С.Г. Фомичева
(должность, уч. степень, звание) (подпись, дата) (инициалы, фамилия)

Программа одобрена на заседании кафедры № 33

«27» мая 2021 г, протокол № 10

Заведующий кафедрой № 33

д.т.н.,доц. 26.05.22 С.В. Беззатеев
(уч. степень, звание) (подпись, дата) (инициалы, фамилия)

Ответственный за ОП ВО 10.05.05(05)

доц.,к.т.н.,доц. 26.05.22 В.А. Мытьников
(должность, уч. степень, звание) (подпись, дата) (инициалы, фамилия)

Заместитель директора института №3 по методической работе

(должность, уч. степень, звание) 26.05.22 Н.В. Решетникова
(подпись, дата) (инициалы, фамилия)

Аннотация

Дисциплина «Технологии защиты от скрытой передачи данных» 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-1 «Способен принимать участие в создании системы защиты информации на объекте информатизации»

ПК-4 «Способен организовывать и проводить мероприятия по контролю за обеспечением защиты информации, в том числе сведений, составляющих государственную тайну, проводить анализ эффективности системы защиты информации»

ПК-6 «Способен применять технологии получения, накопления, хранения, обработки, анализа, интерпретации и использования информации в ходе профессиональной деятельности, работать с различными источниками информации, информационными ресурсами и технологиями; проводить информационно-поисковую работу с последующим использованием данных при решении профессиональных задач»

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

Содержание дисциплины охватывает круг вопросов, связанных с связанных с задачами скрытой передачи информации, помехоустойчивой аутентификации, защиты информации от несанкционированного копирования, отслеживания распространения информации по сетям связи, поиска информации в мультимедийных базах данных.

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

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

Общая трудоемкость освоения дисциплины составляет 4 зачетных единицы, 144 часа.

Язык обучения по дисциплине «русский»

1. Перечень планируемых результатов обучения по дисциплине

1.1. Цели преподавания дисциплины

1.2. Целями преподавания дисциплины является изучение студентами особенностей применения стеганографии и предъявляемых к ней требования, атаки на стегано системы и технологии противодействия им, оценки стойкости стеганографических систем и условия их достижения, а также алгоритмы встраивания информации в изображения, видеопоследовательности и аудио сигналы. В результате изучения дисциплины у студентов должны сформироваться знания, умения и навыки, позволяющие проводить самостоятельный стеганографический анализ информационных процессов, формируемых в системах инфокоммуникаций, как изучаемых в настоящей дисциплине, так и находящихся за ее рамками.

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

1.4. 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-1 Способен принимать участие в создании системы защиты информации на объекте информатизации	ПК-1.У.1 уметь проектировать, разрабатывать, внедрять и эксплуатировать системы защиты информации ПК-1.В.1 владеть навыками поддержания требуемого уровня информационной безопасности объекта информатизации
Профессиональные компетенции	ПК-4 Способен организовывать и проводить мероприятия по контролю за обеспечением защиты информации, в том числе сведений, составляющих государственную тайну, проводить анализ эффективности системы защиты информации	ПК-4.З.1 знать понятие и содержание политики информационной безопасности, показатели качества и эффективности системы безопасности предприятия ПК-4.У.1 уметь выделять объекты защиты и строить концепцию информационной безопасности, регулировать меры по обеспечению информационной безопасности ПК-4.В.1 владеть навыками разработки положений, регламентов и процессов взаимодействия структурных элементов объекта информатизации
Профессиональные компетенции	ПК-6 Способен применять технологии получения, накопления,	ПК-6.З.1 знать способы сбора, предобработки, хранения, модификации данных

	хранения, обработки, анализа, интерпретации и использования информации в ходе профессиональной деятельности, работать с различными источниками информации, информационными ресурсами и технологиями; проводить информационно-поисковую работу с последующим использованием данных при решении профессиональных задач	
Профессиональные компетенции	ПК-8 Способен анализировать структуру и содержание информационных массивов и информационных процессов на предмет выявления угроз безопасности	ПК-8.З.2 знать классификацию источников угроз и нарушителей информационной безопасности ПК-8.У.1 уметь проводить анализ вероятности реализации угрозы и ущерба от ее возникновения

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»

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
		№8
1	2	3
Общая трудоемкость дисциплины, ЗЕ/ (час)	4/ 144	4/ 144
Из них часов практической подготовки	51	51
Аудиторные занятия, всего час.	85	85
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)	17	17
экзамен, (час)	36	36
Самостоятельная работа, всего (час)	23	23
***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 8					
Раздел 1. Механизм функционирования скрытого канала в автоматизированной системе Тема 1.1. Понятие и характеристики скрытого канала связи Тема 1.2. Классификация скрытых каналов	4				4

Раздел 2. Скрытые каналы по памяти Тема 2.1 Сокрытие данных в растровых изображениях Тема 2.2 Сокрытие данных в частотной области изображений Тема 2.3. Оценка методов встраивания данных в изображения	8		10		6
Раздел 3. Скрытые каналы по времени Тема 3.1 Скрытые каналы инфокоммуникационных сетях Тема 3.2; Скрытые каналы в IP-сетях	8		10		4
Раздел 4. Типовые схемы стегано систем Тема 4.1. Эталонная модель взаимодействия стеганографических систем Тема 4.2. Схемы стегано систем без ключа Тема 4.3. Схемы стегано систем с ключами	6		6		4
Раздел 5. Атаки на стегано системы и их выявление Тема 5.1. Классификация атак на стегано системы Тема 5.2. Оценка качества стегано системы Тема 5.3. Требования при проектировании стегано систем	8		8		5
Выполнение курсовой работы				17	
Итого в семестре:	34		34	17	23
Итого	34	0	34	17	23

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	**Механизм функционирования скрытого канала в автоматизированной системе** Тема 1.1. Понятие и характеристики скрытого канала связи (демонстрация слайдов) Тема 1.2. Классификация скрытых каналов (демонстрация слайдов)
2	**Скрытые каналы по памяти** Тема 2.1 Сокрытие данных в растровых изображениях (демонстрация слайдов) Тема 2.2 Сокрытие данных в частотной области изображений (демонстрация слайдов) Тема 2.3. Оценка методов встраивания данных в изображения (демонстрация слайдов)
3	**Скрытые каналы по времени** Тема 3.1 Скрытые каналы инфокоммуникационных сетях (демонстрация слайдов) Тема 3.2; Скрытые каналы в IP-сетях (демонстрация слайдов)
4	**Типовые схемы стегано систем** Тема 4.1. Эталонная модель взаимодействия стеганографических систем (демонстрация слайдов) Тема 4.2. Схемы стегано систем без ключа (демонстрация слайдов)

	Тема 4.3. Схемы стегано систем с ключами (демонстрация слайдов)
5	**Атаки на стегано системы и их выявление** Тема 5.1. Классификация атак на стегано системы (демонстрация слайдов) Тема 5.2. Оценка качества стегано системы (демонстрация слайдов) Тема 5.3. Требования при проектировании стегано 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 8				
1	Использование скрытых каналов по памяти	6	4	2
2	Использование растровых изображений для сокрытия информации	6	4	2,4
3	Сокрытие ЦВЗ методом Коха-Жао	6	4	2,4
4	Извлечение ЦВЗ из JPEG-контейнера методом Коха-Жао	8	6	2,4,5
5	Скрытые каналы в TCP/IP-сетях	8	6	3,5
Всего		34		

4.5. Курсовое проектирование/ выполнение курсовой работы

Цель курсовой работы: Цель курсовой работы: формирование компетенций комплексного применения знаний и навыков анализа скрытых каналов передачи информации.

В курсовой работе должны быть решены следующие задачи:

1) Оценка актуальности разрабатываемой информационной системы
2) Построение диаграммы IDEF0, DFD бизнес-процессов разрабатываемой системы. Выявление скрытых каналов передачи информации.
3) Проектирование архитектуры информационной системы и системы мониторинга скрытых каналов передачи информации
4) Разработка серверной и клиентских частей разрабатываемой системы
5) Анализ уязвимостей и угроз информационной безопасности разрабатываемой системы

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 8, час
1	2	3
Изучение теоретического материала дисциплины (ТО)	10	10
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)	8	8
Всего:	23	23

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)
[004.9 Д 24]	Дворкович В. П. Цифровые видеоинформационные системы (теория и практика)/ В. П. Дворкович, А. В. Дворкович. - М.: Техносфера, 2012. - 1008 с.	5
	Цифровая стеганография / Грибунин В. Г., Оков И. Н., Туринцев И.В. – М.: СОЛОН-ПРЕСС, 2009 – 272с.	
	Стеганография, цифровые водяные знаки и стеганоанализ: монография / А.В. Аграновский, А.В. Балакин, В.Г. Грибунин, С.А. Сапожников. – М.: Вузовская книга, 2009. – 220 с.	
004.7(075) И 74]	Информационная безопасность открытых систем: учебник: в 2 т./ С. В. Запечников [и др.]. - М.:Горячая линия - Телеком. - Т.	25

	2: Средства защиты всетях. - М., 2008. - 558 с	
[004.056(075) Т 33]	Теория информационной безопасности и методология защиты информации: методические указания к выполнению лабораторных работ № 1 -4/ С. В. Беззатеев, Е. М. Линский, А. Д. Фомин. С.- Петерб. гос. ун-т аэрокосм. приборостроения; сост.: - СПб: ГОУ ВПО "СПбГУАП", 2007. - 35 с.	88

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
https://e.lanbook.com/book/5192	Рябко Б.Я., Фионов А.Н. Основы современной криптографии и стеганографии. Издательство: «Горячая линия-Телеком», 2011. 232 с.
http://e.lanbook.com/view/book/1122/	Шаньгин В.Ф. Защита компьютерной информации. ДМК Пресс, 2010. 544 с
http://e.lanbook.com/view/book/1113/	Петренко С.А., Петренко А.А. Аудит безопасности Intranet. ДМК Пресс, 2010. 386 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
	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
Экзамен	Список вопросов к экзамену; Экзаменационные билеты; Задачи; Тесты.
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.
«хорошо» «зачтено»	– 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.

Оценка компетенции 5-балльная шкала	Характеристика сформированных компетенций
«удовлетворительно» «зачтено»	– 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»	– 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.	Стеганография. Основные понятия и определения	ПК-1.У.1
2.	Стеганография. Области применения.	ПК-1.В.1
3.	Математическая модель типичной стегано системы.	ПК-4.З.1
4.	Стеганографические протоколы.	ПК-4.У.1
5.	Классификация атак на стегано системы.	ПК-4.В.1
6.	Методы противодействия атакам на стегано системы.	ПК-6.З.1
7.	Понятие стеганографической стойкости. Абсолютно стойкая стегано система.	ПК-8.З.2
8.	Внедрение индивидуальных меток (ЦВЗ). Построение меток.	ПК-8.У.1
9.	Встраивание информации в текстовые файлы. Классификация алгоритмов.	ПК-1.У.1
10.	Встраивание информации в текстовые файлы. Описание алгоритмов.	ПК-1.В.1
11.	Встраивание информации в неподвижное изображение. Классификация алгоритмов.	ПК-4.З.1
12.	Встраивание информации в неподвижное изображение. Описание алгоритма встраивания в НЗБ.	ПК-4.У.1
13.	Встраивание информации в неподвижное изображение. Описание любого форматного алгоритма встраивания.	ПК-4.В.1
14.	Встраивание информации в неподвижное изображение. Описание любого алгоритма встраивания в палитру.	ПК-6.З.1
15.	Встраивание информации в неподвижное изображение. Описание любого алгоритма встраивания в частотной области.	ПК-8.З.2
16.	Методы скрытия информации в аудио сигналах. Перечислить существующие подходы.	ПК-8.У.1
17.	Скрытие информации в видеопоследовательностях. Перечислить существующие подходы.	ПК-1.У.1

18.	Скрытие информации в видеопоследовательностях. Описание любого алгоритма.	ПК-1.В.1
19.	Статистические методы стегано анализа	ПК-4.З.1
20.	Скрытые каналы в IP-сетях (Свойства каналов)	ПК-4.У.1
21.	Скрытые каналы в IP-сетях (Типы каналов)	ПК-4.В.1
22.	Существующие реализации стегано систем. Описание любого пакета	ПК-6.З.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.	Разработка экспертной системы оценки наличия скрытых каналов в IP-сетях IT-инфраструктуры
2.	Разработка автоматизированной системы формирования комплекса средств защиты от передачи данных в скрытых каналах в IP-сетях
3.	Разработка экосистемы для защиты от вредоносных программ
4.	Разработка системы защиты от передачи данных в скрытых каналах в сверточных нейронных сетях
5.	Разработка метода словообразования в лингвистической стеганографии
6.	Разработка корпоративной системы многофакторной аутентификации
7.	Управление идентификацией на базе технологии блокчейн
8.	Разработка протокола оценки бихевиористики в IT системах
9.	Разработка системы анализа консолидированных данных в озерах событий безопасности
10.	Разработка интеллектуального контрольно-пропускного пункта
11.	Решение проблем эволюции криптовымогателей
12.	Решение проблем защиты пользователей Интернета от негативных аудио- и видеозакладокзащиты пользователей Интернета от негативных аудио- и видеозакладок
13.	Цифровой профиль клиента банка с точки зрения информационной безопасности
14.	Решение проблем разработки схем электронной цифровой подписи и алгоритмов шифрования с открытым ключом для использования в перспективных отечественных СКЗИ

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
1.	Основные достоинства и недостатки биометрической аутентификации:	ПК-1.У.1

	• (Правильный ответ) высокая надежность • (Правильный ответ) высокая стоимость • низкая стоимость внедрения	
2.	Для каких сетей сертификат «Красной книги» считается устаревшим? • для локальных • (Правильный ответ) для беспроводных сетей • для интернета	ПК-1.В.1
3.	Какой уровень безопасности соответствует уровню B2 шкалы «Оранжевой книги»? • минимальная защита (ненормируемая) • контролируемая защита доступа • защита с метками безопасности • (Правильный ответ) структурированная защита • защита по усмотрению	ПК-4.З.1
4.	Какие из этих видов атак относятся к атакам на отказ в обслуживании? • добавление • (Правильный ответ) отказ в доступе к информации • (Правильный ответ) отказ в доступе к приложениям • подслушивание	ПК-4.У.1
5.	Атака на отказ в доступе к системе направлена на: • уничтожение информации • приложения обработки информации • (Правильный ответ) вывод из строя компьютерной системы • блокирование каналов связи	ПК-4.В.1
6.	Какие из этих описаний характеризует централизованные DoS-атаки? • (Правильный ответ) это злонамеренные действия, выполняемые для запрещения легальному пользователю доступа к системе, сети, приложению или информации • (Правильный ответ) для осуществления атаки система-отправитель посылает огромное количество TCP SYN-пакетов (пакетов с синхронизирующими символами) к системе-получателю, игнорируя ACK-пакеты, добиваясь переполнения буфера очереди соединений • в осуществлении атаки участвует большое количество систем, которыми управляет одна главная система и один хакер. Выход системы из строя достигается путем огромного объема передаваемых данных	ПК-6.З.1
7.	Какую из возможных угроз для безопасности системы труднее всего обнаружить? • ошибки конфигурации • слабые пароли • (Правильный ответ) переполнение буфера	ПК-8.З.2
8.	Выберите верное утверждение: • прослушивание (снифинг) работают только в сетях с разделяемой пропускной способностью с сетевыми концентраторами – хабами; использование коммутаторов обеспечивает достаточно надежную защиту от	ПК-8.У.1

	прослушивания • (Правильный ответ) прослушивание (снифинг) хорошо работают в сетях с разделяемой пропускной способностью с сетевыми концентраторами – хабами; использование коммутаторов снижает эффективность снифинга • прослушивание (снифинг) работают только в сетях с коммутируемой средой, использующей коммутаторы; использование концентраторов исключает возможность снифинга	
9.	Требования к конфиденциальности файлов включают в себя: • (Правильный ответ) правильное управление ключами при использовании шифрования • контроль физической безопасности • (Правильный ответ) правильная настройка компьютерной системы	ПК-1.У.1
10.	Переключение по отказу: • (Правильный ответ) обеспечивает восстановление информации и сохранение производительности • предотвращает полную потерю информации при случайном или преднамеренном уничтожении файлов • защищает системы, информацию и производственные мощности от стихийных бедствий	ПК-1.В.1
11.	Для обеспечения конфиденциальности потока данных применяются методы: • (Правильный ответ) скрытия информации • аудита • физической защиты	ПК-1.У.1
12.	Требования к конфиденциальности файлов включают в себя: шифрование файлов • (Правильный ответ) идентификация и аутентификация • (Правильный ответ) правильное управление ключами при использовании шифрования	ПК-1.В.1
13.	Использование скрытия информации позволяет: • (Правильный ответ) обеспечить конфиденциальность потока данных • защитить от перехвата информации • предотвратить прослушивание	ПК-4.З.1
14.	Что должен включать минимум документации начального состояния системы? • (Правильный ответ) уровень обновления • (Правильный ответ) начальные конфигурации устройств • список всех файлов • (Правильный ответ) список работающих приложений и их версии	ПК-4.У.1
15.	Какие фазы методологии разработки требуют особого внимания при обсуждении вопросов безопасности? • (Правильный ответ) разработка • (Правильный ответ) реализация • определение целей • планирование	ПК-4.В.1

16.	Основным механизмом обнаружения вторжений является: • сетевое программное обеспечение для обнаружения вторжения • (Правильный ответ) антивирусное программное обеспечение • клиентское программное обеспечение для обнаружения вторжения • ручная проверка журнала • автоматическая проверка журнала	ПК-6.З.1
17.	Ответы на какие вопросы позволяют оценить эффективность систем резервного копирования? • (Правильный ответ) для каких систем проводится резервное копирование и как часто • какой объем данных содержится на резервных копиях • (Правильный ответ) как часто резервные копии перемещаются в архив • (Правильный ответ) выполнялась ли когда-либо проверка резервных копий • имеет ли хранилище резервных копий защиту от ядерного оружия	ПК-8.З.2
18.	При использовании какого экрана соединение между клиентом и сервером обрывается на экране? • (Правильный ответ) прикладного уровня • гибридного • с фильтрацией пакетов	ПК-8.У.1
19.	Играет ли порядок применения правил в межсетевом экране на функционирование сети? • (Правильный ответ) да, так от порядка зависит, как будут обрабатываться пакеты • зависит от того как настроен экран • нет, пакет обрабатывается всеми правилами, и если одно правило подходит, то трафик пропускается	ПК-1.У.1
20.	Межсетевой экран (firewall) — это: • устройство функцией которого является доставка трафика в пункт назначения в максимально короткие сроки • (Правильный ответ) устройство контроля доступа в сеть, предназначенное для блокировки всего трафика, за исключением разрешенных данных • устройство кэширующее сетевой трафик	ПК-1.В.1
21.	Как осуществляется доступ к внутренней сети пользователем подключенным через VPN? • (Правильный ответ) необходимо пройти процедуру аутентификации на сервере • нужно просто знать адрес сервера VPN • доступ к внутренней сети не может быть получен ни каким образом	ПК-1.У.1
22.	Какие типы VPN существуют? • серверные • (Правильный ответ) пользовательские • (Правильный ответ) узловые • многопользовательские	ПК-1.В.1

23.	Какие преимущества имеет аппаратная реализация VPN? • дешевизна • (Правильный ответ) скорость • (Правильный ответ) безопасность	ПК-4.З.1
24.	При каких условиях хеш-функция может называться безопасной? • функция является двусторонней • при выполнении функции два фрагмента информации одинакового объема получают одинаковую контрольную сумму • (Правильный ответ) крайне сложно сконструировать два фрагмента информации с получением одинаковой контрольной суммы при выполнении функции	ПК-4.У.1
25.	Принцип работы NIDS заключается в: • подключении ко всем системам и анализе их работы • выполнении обоих вышеуказанных действий • (Правильный ответ) перехвате сетевого трафика и его анализе	ПК-4.В.1
26.	Что является объектом мониторинга при обнаружении атак с помощью NIDS? • неудачные попытки входа • успешные FTP-соединения • (Правильный ответ) весь трафик, поступающий на потенциально атакуемые системы • успешные HTTP-соединения	ПК-6.З.1
27.	При работе с какими протоколами полезно записывать содержимое пакетов, при исследовании подозрительных событий? • UDP • TCP • (Правильный ответ) SMTP • (Правильный ответ) FTP • (Правильный ответ) HTTP	ПК-8.З.2
28.	Программа netstat предназначена для: • (Правильный ответ) выявления сетевых соединений активных в данный момент • выявления процессов поддерживающих открытое состояние порта • отображения всех активных процессов	ПК-8.У.1
29.	Какие устройства могут выполнять функции NAT? • (Правильный ответ) межсетевые экраны • DNS сервера • (Правильный ответ) маршрутизаторы • почтовые сервера	ПК-1.У.1
30.	Типами скрытых каналов являются каналы • (Правильный ответ) По памяти • (Правильный ответ) По времени • (Правильный ответ) Статистический • сетевой	ПК-1.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 представлен по ссылке: https://pro.guap.ru/inside#subjects/2403316

– 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

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 «Использование скрытых каналов по памяти»

Цель лабораторной работы: Реализация алгоритмов сокрытия информации в текстовых файлах путем изменения интервала между словами

Задание к лабораторной работе №1:

1) Изучить алгоритмы сокрытия и извлечения информации в текстовых файлах
2) Реализовать алгоритмы сокрытия и извлечения информации в текстовых файлах в средах программирования (C#, C++, Python), используя прототип решения в среде моделирования (MatLab)
3) Провести анализ наличия стегограмм в текстовом файле.
4) Оформить отчет по лабораторной работе

Ход лабораторной работы, структура и форма отчета о лабораторной работе и требования к оформлению отчета о лабораторной работе представлены по ссылке https://pro.guap.ru/get-task/96a53b5a16b9b66c7388e84db1d57f83

ЛАБОРАТОРНАЯ РАБОТА №2 «Использование растровых изображений для сокрытия информации»

Цель лабораторной работы: Реализация алгоритмов сокрытия информации в растровых изображениях с использованием стегоключей

Задание к лабораторной работе №2:

1) Изучить алгоритмы сокрытия и извлечения информации в файлах растровой графики

2) Разработать визуальный интерфейс для взаимодействия с растровыми файлами. Визуальные компоненты интерфейса должны обеспечивать диалоговые режимы ввода стегоключа, выбора файлов при их загрузке и сохранении, обеспечивать режим просмотра файлов с выделением позиций, в которых размещено стегосообщение.

3) Реализовать алгоритмы сокрытия и извлечения информации в растровых файлах в средах программирования (C#, C++, Python), используя прототип решения в среде моделирования (MatLab). При этом должна быть обеспечена схема 3 уровня защищенности (распределение стегосообщения по контейнеру, задаваемое некоторой функций, аргументом которой является стегоключ).

4) Провести анализ наличия стегограмм в растровом файле.

4) Оформить отчет по лабораторной работе

Ход лабораторной работы, структура и форма отчета о лабораторной работе и требования к оформлению отчета о лабораторной работе представлены по ссылке

https://pro.guap.ru/get-task/d5222364c1b1763b26fcd7d73a97dfbf

Лабораторная работа №3 «Сокрытие ЦВЗ методом Коха-Жао»

Цель лабораторной работы: реализовать сокрытие ФАЙЛОВ в частотной области растрового изображения методом Коха-Жао

Задание к лабораторной работе №3:

1) Изучить алгоритмы сокрытия информации в частотных областях растровой графики с использованием дискретного косинусного преобразования

2) К проекту, реализованному в лабораторной работе №2 добавить формы визуального интерфейса для взаимодействия с частотными областями растровых файлов. Визуальные компоненты интерфейса должны обеспечивать диалоговые режимы ввода стегоключа, выбора параметра качества стегокодирования, выбора файлов при их загрузке и сохранении, обеспечивать режим просмотра файлов с выделением позиций, в которых размещено стегосообщение.

3) Реализовать алгоритмы сокрытия информации в частоных областях растровых файлах в средах программирования (C#, C++, Python), используя прототип решения в среде моделирования (MatLab), основанный на сетоде Кохв-Жао. При этом должна быть обеспечена схема 3 уровня защищенности (распределение стегосообщения по контейнеру, задаваемое некоторой функций, аргументом которой является стегоключ).

4) Провести анализ наличия стегограмм в растровом файле.

4) Оформить отчет по лабораторной работе

Ход лабораторной работы, структура и форма отчета о лабораторной работе и требования к оформлению отчета о лабораторной работе представлены по ссылке

https://pro.guap.ru/get-task/ed8a909b1b37578f567fbe711196c5bc

Лабораторная работа №4 «Извлечение ЦВЗ из JPEG-контейнера методом Коха-Жао»

Цель лабораторной работы: реализовать извлечение ФАЙЛОВ из частотной области растрового изображения, сокрытых методом Коха-Жао

Задание к лабораторной работе №4:

1) Изучить алгоритмы извлечения информации в частотных областях растровой графики с использованием дискретного косинусного преобразования

2) К проекту, реализованному в лабораторной работе №3 добавить элементы визуального интерфейса для реализации декодирования стегоконтейнера из частотных областей растровых файлов. Визуальные компоненты интерфейса должны обеспечивать диалоговые режимы ввода стегоключа, выбора параметра качества стегокодирования, выбора файлов при их загрузке и сохранении, обеспечивать режим просмотра файлов с выделением позиций, в которых размещено стегосообщение.

3) Реализовать алгоритмы извлечения информации в частоных областях растровых файлах в средах программирования (C#, C++, Python), используя прототип решения в среде моделирования (MatLab), основанный методом Кохв-Жао. При этом должна быть обеспечена схема 3 уровня защищенности (распределение стегосообщения по контейнеру, задаваемое некоторой функций, аргументом которой является стегоключ).

4) Провести анализ наличия стегограмм в растровом файле.

4) Оформить отчет по лабораторной работе

Ход лабораторной работы, структура и форма отчета о лабораторной работе и требования к оформлению отчета о лабораторной работе представлены по ссылке

https://pro.guap.ru/get-task/b3a16538f93fae4825d2f2edfe8da3e0

Лабораторная работа №5 «Скрытые каналы в TCP/IP-сетях»

Цель лабораторной работы: Использование негласных возможности протоколов TCP/IP, которые могут быть использованы для построения скрытых каналов

Задание к лабораторной работе №5:

1) Изучить принципы работы протоколов TCP/IP
2) Изучить назначение и возможность модификации заголовков IP-пакетов и TCP-блоков (сегментов)
3) Разработать клиент-серверную реализацию сокрытия информации в IP-пакетах, рассмотренную в лекции 9.
4) Разработать серверную часть проекта, реализующую «сниффинг» каналов передачи информации по протоколам TCP/IP и выделение переданного стеганосообщения
5) Разработать клиентскую часть проекта, реализующую формирования IP-пакетов с инкапсулированным стеганосообщением в заданных по индивидуальному варианту полям IP=заголовка.
6) Определить пропускную способность скрытого канала
7) Оформить отчет по лабораторной работе

Ход лабораторной работы, структура и форма отчета о лабораторной работе и требования к оформлению отчета о лабораторной работе представлены по ссылке

https://pro.guap.ru/get-task/3529e9d0d3ed105a685d85657f47d4f0

11.5. 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.

В курсовой работе должны быть решены следующие задачи:

1) Оценка актуальности разрабатываемой информационной системы
2) Построение диаграммы IDEF0, DFD бизнес-процессов разрабатываемой системы. Выявление скрытых каналов передачи информации.
3) Проектирование архитектуры информационной системы и системы мониторинга скрытых каналов передачи информации
4) Разработка серверной и клиентских частей разрабатываемой системы
5) Анализ уязвимостей и угроз информационной безопасности разрабатываемой системы

Структура пояснительной записки курсового проекта/ работы

1) Введение
2) Оценка актуальности разрабатываемой информационной системы. Аналитический обзор прототипов разрабатываемой системы
3) Инфологическое моделирование разрабатываемой информационной системы. Выявление активов и критических элементов проектируемой системы
4) Проектирование архитектуры информационной системы
5) Проектирование клиент-серверной базы данных (ER-диаграмма)
6) Проектирование приложения доступа к данным. Результаты тестирования программного приложения
7) Оценка рисков эксплуатации информационной системы
8) Заключение.
9) Список литературы
10) Приложение (листинги исходных программных кодов)

.

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