Автономная некоммерческая организация высшего образования «Открытый институт»

"УТВЕРЖДАЮ"

Ректор _____ Д.А. Котов

"____" _____ _____ года

Защита информации

Рабочая программа

Направление/специальность: Информатика и вычислительная техника

Форма обучения: заочная

г. Цхинвал
2019

Оглавление

ИНФОРМАТИКА И ВЫЧИСЛИТЕЛЬНАЯ ТЕХНИКА
Дисциплина: "Защита информации"
Общие данные

Трудоемкость		
Общая трудоемкость в часах	252	Цикл ООП: Вариативная часть
Общая трудоемкость в ЗЕ	7	

Учебная работа							
Виды учебной работы	**Всего часов**	**1 курс**	**2 курс**	**3 курс**	**4 курс**	**5 курс**	**6 курс**
Лекции	6	-	-	-	-	6	-
Практические занятия	10	-	-	-	-	10	-
Самостоятельная работа	223	-	-	-	-	223	-
Лабораторная работа	-	-	-	-	-	-	-
КСР	13	-	-	-	-	13	-

Форма и курс промежуточной аттестации						
Зачет/Экзамен					Э	

Цель дисциплины: Сформировать практические правила защиты информации, научить проводить анализ угроз безопасности, приобрести навыки защиты информации; изучить методы и средства обеспечения защиты информации.

Результаты обучения по дисциплине (курсу)

В результате изучения дисциплины (курса) обучающийся должен:

- Знать следующие теоретические положения дисциплины: Защита информации в IP-сетях; Основы криптографии; Теоретические основы информационной безопасности

- Уметь

* Использовать специальные методы для достижения профессиональных задач;
* Применять полученную теоретическую базу в практической деятельности и при освоении смежных дисциплин;

- Владеть

* Навыками разрешения профессиональных проблем, опираясь на полученные знания и умения в указанной предметной области;

ИНФОРМАТИКА И ВЫЧИСЛИТЕЛЬНАЯ ТЕХНИКА
Дисциплина: "Защита информации"

Тематический план

Раздел 1. Теоретические основы информационной безопасности

Тема 1. Базовые понятия
Тема 2. Общая схема процесса обеспечения безопасности
Тема 3. Идентификация, аутентификация, управление доступом. Защита от несанкционированного доступа
Тема 4. Парольные системы аутентификации
Тема 5. Модели безопасности
Тема 6. Модель Харрисона-Рузо-Ульмана
Тема 7. Модель Белла-ЛаПадула
Тема 8. Ролевая модель безопасности
Тема 9. Процесс построения и оценки системы обеспечения безопасности. Стандарт ISO/IEC 15408

Раздел 2. Основы криптографии

Тема 1. Основные понятия. Классификация шифров
Тема 2. Виды шифров
Тема 3. Симметричные шифры
Тема 4. Схема Фейстеля
Тема 5. Шифр DES
Тема 6. Шифр ГОСТ 28147-89
Тема 7. Шифр Blowfish
Тема 8. Управление криптографическими ключами для симметричных шифров
Тема 9. Протокол Kerberos
Тема 10. Асимметричные шифры
Тема 11. Основные понятия
Тема 12. Распределение ключей по схеме Диффи-Хеллмана
Тема 13. Криптографическая сисRSA
Тема 14. Криптографическая сисЭль-Гамаля
Тема 15. Совместное использование симметричных и асимметричных шифров
Тема 16. Хэш-функции
Тема 17. Хэш-функции без ключа
Тема 18. Алгоритм SHA-1
Тема 19. Хэш-функции с ключом
Тема 20. Инфраструктура открытых ключей. Цифровые сертификаты

Раздел 3. Защита информации в IP-сетях

Тема 1. Протокол защиты электронной почты S/MIME
Тема 2. Протоколы SSL и TLS
Тема 3. Протоколы IPSec и распределение ключей
Тема 4. Протокол AH
Тема 5. Протокол ESP
Тема 6. Протокол SKIP
Тема 7. Протоколы ISAKMP и IKE
Тема 8. Протоколы IPSec и трансляция сетевых адресов
Тема 9. Межсетевые экраны

ЛЕКЦИИ

5 КУРС

Лекция № 1. К разделам учебной программы:

к разделу № 1. Теоретические основы информационной безопасности

6 часов

ПРАКТИЧЕСКИЕ ЗАНЯТИЯ

5 КУРС

Основы криптографии № 1. На тематику учебной программы:

к разделу № 0.

4 часа

Защита информации в IP-сетях № 2. На тематику учебной программы:

к разделу № 0.

6 часов

Перечень учебно-методического обеспечения для самостоятельной работы обучающихся по дисциплине

1. Методические указания по решению задач, направленных на проверку конкретных результатов обучения
2. Типовая рабочая тетрадь дисциплины

Защита информации

Фонд оценочных средств
Образцы заданий для оценки знаний, умений, навыков:

Отметьте темы, относящиеся к настоящей дисциплине:

- [ ] Штриховое кодирование продуктов питания
- [ ] Защита информации в IP-сетях
- [ ] Структура политического менталитета
- [ ] Воспитание в учебной и внеучебной деятельности школьников
- [ ] Протокол защиты электронной почты S/MIME

Отметьте темы, относящиеся к настоящей дисциплине:

- [ ] Основные понятия
- [ ] Протокол Kerberos
- [ ] Введение в историю костюма и моды
- [ ] Пути мирного урегулирования международных конфликтов
- [ ] Методы обработки изделий и способы их описания

Отметьте темы, относящиеся к настоящей дисциплине:

- [ ] Модель Харрисона-Рузо-Ульмана
- [ ] Великая Отечественная война. Послевоенные годы (1941—1950 гг.)
- [ ] Теоретические основы информационной безопасности
- [ ] Органические виды материи: организм, сообщество
- [ ] Технология сладких блюд, горячих и прохладительных напитков

Отметьте темы, относящиеся к настоящей дисциплине:

- [ ] Современные проблемы функционирования и регулирования российского потребительского рынка
- [ ] Психологическое тестирование. Личностные опросники
- [ ] Россия летом-осенью 1917 года. Альтернативы развития революции. Приход к власти большевиков.
- [ ] Основы криптографии
- [ ] Шифр Blowfish

Отметьте темы, относящиеся к настоящей дисциплине:

- [ ] Морфологический, словообразовательный и синтаксический уровни грамматического строя.
- [ ] Нечеткая временная сеть Петри с нечеткой структурой Ctfsf
- [ ] Основные понятия. Классификация шифров
- [ ] Совместное использование симметричных и асимметричных шифров
- [ ] Кристаллическое строение металлов

Отметьте темы, относящиеся к настоящей дисциплине:

- [ ] Модели безопасности
- [ ] Структура финансовой системы ФРГ
- [ ] Принципы адаптационной физической культуры
- [ ] ЧЕЛОВЕК И ТЕХНОСФЕРА. ФИЗИОЛОГИЯ ТРУДА
- [ ] Ролевая модель безопасности

Отметьте темы, относящиеся к настоящей дисциплине:

- [ ] Защита российского рынка от неблагоприятного воздействия иностранной конкуренции
- [ ] Информационные модели
- [ ] Мини - суд при разрешении корпоративных споров. Досудебные механизмы. Процессуальные элементы разрешения споров.
- [ ] Совместное использование симметричных и асимметричных шифров
- [ ] Хэш-функции

Отметьте темы, относящиеся к настоящей дисциплине:

- [ ] Межсетевые экраны
- [ ] Понятие права международных договоров
- [ ] Протокол защиты электронной почты S/MIME
- [ ] Сущность
- [ ] Понятие, формирование и распространение романо-германской правовой семьи

Отметьте темы, относящиеся к настоящей дисциплине:

- [ ] Определитель и его свойства
- [ ] Средства массовой коммуникации и суицидальное поведение
- [ ] Проектирование рабочего процесса
- [ ] Ролевая модель безопасности
- [ ] Криптографическая сисЭль-Гамаля

Отметьте темы, относящиеся к настоящей дисциплине:

- [ ] Протоколы ISAKMP и IKE
- [ ] Право частной собственности на землю
- [ ] Моменты случайной величины
- [ ] Педагогика – наука о воспитании
- [ ] Модель Белла-ЛаПадула

Отметьте темы, относящиеся к настоящей дисциплине:

- [ ] Кинетика сушки
- [ ] Инновационная инфраструктура: понятие и элементы
- [ ] Протокол AH
- [ ] Защита информации в IP-сетях
- [ ] Втулка

Отметьте темы, относящиеся к настоящей дисциплине:

- [ ] Протокол ESP
- [ ] ДЕНЬГИ И БАНКИ. Зачем использовать деньги?
- [ ] Синонимические средства языка как ресурсы стилистики
- [ ] Шифр DES
- [ ] Недобросовестная конкуренция

Отметьте темы, относящиеся к настоящей дисциплине:

- [ ] Процедура медиации и ее фазы. Значение фаз в медиации
- [ ] Биологические основы физической культуры
- [ ] Принципы создания САПР
- [ ] Протоколы ISAKMP и IKE
- [ ] Криптографическая сисЭль-Гамаля

Отметьте темы, относящиеся к настоящей дисциплине:

- [ ] Определение глубины заложения фундаментов
- [ ] Основные понятия
- [ ] Правовые особенности существования платежных систем
- [ ] Архитектура Древнего Египта
- [ ] Защита информации в IP-сетях

Отметьте темы, относящиеся к настоящей дисциплине:

- [ ] Протоколы IPSec и распределение ключей
- [ ] Стратегии межфирменной конкуренции
- [ ] Россия в XX веке
- [ ] Концептуальные основы системы планирования
- [ ] Ролевая модель безопасности

Отметьте темы, относящиеся к настоящей дисциплине:

- [ ] Действие нормативных правовых актов в пространстве, во времени и по кругу лиц
- [ ] Асимметричные шифры
- [ ] Протоколы ISAKMP и IKE
- [ ] Примордиализм как научное направление
- [ ] Проблемы реформирования жилищно-коммунального хозяйства в регионах

Отметьте темы, относящиеся к настоящей дисциплине:

- [ ] Самодеятельные движения и гражданские инициативы
- [ ] Хэш-функции без ключа
- [ ] Защита информации в IP-сетях
- [ ] Финансово-экономическое состояние жилищно-коммунального хозяйства
- [ ] Власть в структуре личности

Отметьте темы, относящиеся к настоящей дисциплине:

- [ ] Эффективность и качество образования
- [ ] Регрессионные модели с гетероскедастичными остатками
- [ ] Особенности усвоения учащимися с задержкой психического развития русского языка и математики
- [ ] Модели безопасности
- [ ] Общая схема процесса обеспечения безопасности

Отметьте темы, относящиеся к настоящей дисциплине:

- [ ] Простые (внутренние и внешние) противоречия
- [ ] Процедура психологического исследования семьи
- [ ] Организация учебно-тренировочного процесса
- [ ] Основы криптографии
- [ ] Совместное использование симметричных и асимметричных шифров

Отметьте темы, относящиеся к настоящей дисциплине:

- [ ] Международная система регистрации товарных знаков
- [ ] Управление криптографическими ключами для симметричных шифров
- [ ] Симметричные шифры
- [ ] Личные права и свободы
- [ ] Прокурорский надзор за исполнением законов в оперативно-розыскной деятельности

Перечень основной и дополнительной литературы

КРИПТОГРАФИЧЕСКАЯ ЗАЩИТА ИНФОРМАЦИИ: СИММЕТРИЧНОЕ ШИФРОВАНИЕ. Учебное пособие для вузов

Бабенко Л.К., Ищукова Е.А., Издательство: М.:Издательство Юрайт, 2018 г., ISBN: 978-5-9916-9244-1

Настоящее учебное пособие посвящено изучению основных аспектов современной криптографии, а именно ее большому разделу симметричным блочным шифрам. Большое количество наглядных примеров позволит освоить основные принципы применения криптографических алгоритмов. Вопросы для самоконтроля и задачи для самостоятельного решения будут способствовать закреплению изученного материала. Изученный материал позволит самостоятельно применять полученные знания на практике в области криптографии и в области криптоанализа.

ЗАЩИТА ИНФОРМАЦИИ: ОСНОВЫ ТЕОРИИ. Учебник для бакалавриата и магистратуры

Щеглов А.Ю., Щеглов К.А., Издательство: М.:Издательство Юрайт, 2018 г., ISBN: 978-5-534-04732-5

Цель учебника системное изложение основных принципов и методов математического моделирования, а также формального и неформального проектирования систем защиты информации, образующих основу теории защиты информации. В учебнике приводятся основы математической теории защиты инфомации, а также основополагающие подходы к построению СЗИ, что позволяет сформировать у обучающегося определенную систему взглядов на вопросы проектирования таких систем. Рассматриваемые в книге подходы к математическому моделированию для наглядности иллюстрируются простыми примерами.

Перечень информационных технологий, ПО, информационных систем

1. Персональный компьютер с OS MS Windows и подключением к Интернет
2. Пакет Open Office
3. Internet explorer
4. Электронная библиотечная система iprbookshop.ru
5. Мультимедиа-проектор
6. Информационно-правовая система

Описание материально-технической базы

1. Оборудованный учебный кабинет
2. Мультимедиа-проектор с экраном/доской
3. Усилитель звука
4. Компьютерный класс с ПК (OS MS Windows, дополнительным ПО, гарнитурами) и подключением к Интернет
5. Библиотечный фонд, включая ЭБС

Распределение самостоятельной работы по видам

Подготовка к занятиям	40
Подготовка ответов по ФОС	45
Рабочая тетрадь	6
Подготовка курсовой работы	-
Решение задач практикума	66
Изучение литературы	52
Методическая работа	2
Изучение нормативной базы	2
Работа с узловыми темами	6
Научно-исследовательская работа	4

Сведения о принятии, обновлении/внесении изменений

1. 09.03.2017 г. Ответственный: Котов Д.А.

2. 05.09.2018 г. Ответственный: Котов Д.А.

ИНФОРМАТИКА И ВЫЧИСЛИТЕЛЬНАЯ ТЕХНИКА: «ЗАЩИТА ИНФОРМАЦИИ»