

1. Общие сведения о дисциплине (модуле).

Целью освоения дисциплины «Основы информационной безопасности» является формирование у обучающихся компетенций в соответствии с требованиями самостоятельно утвержденного образовательного стандарта высшего образования (СУОС) по направлению подготовки бакалавриата «Инфокоммуникационные технологии и системы связи».

Задачами освоения дисциплины «Основы информационной безопасности» являются:

- формирование умений работать с организационно-правовой документацией по защите информации, оценивать угрозы объектам защиты информации, выстраивать комплексную систему защиты информации на предприятии, выявлять и расследовать инциденты информационной безопасности;
- приобретение навыков расследования компьютерных преступлений;
- освоение базовых приемов решения практических задач по темам дисциплины.

2. Планируемые результаты обучения по дисциплине (модулю).

Перечень формируемых результатов освоения образовательной программы (компетенций) в результате обучения по дисциплине (модулю):

ОПК-3 - Способен применять методы поиска, хранения, обработки, анализа и представления в требуемом формате информации из различных источников и баз данных, соблюдая при этом основные требования информационной безопасности.

Обучение по дисциплине (модулю) предполагает, что по его результатам обучающийся будет:

Знать:

- методы поиска, хранения, обработки, анализа и представления в требуемом формате информации, требования информационной безопасности, а также основные причины и особенности современных информационных и мобильных угроз;
- основные методы и средства защиты информации в информационных системах;
- правовые основы обеспечения защиты информации.

Уметь:

- применять основные требования информационной безопасности на практике, самостоятельно анализировать и оценивать угрозы информационной безопасности; - классифицировать угрозы информационной безопасности с целью создания эффективной системы защиты от угроз.

Владеть:

- методами поиска, хранения, обработки, анализа и представления в требуемом формате информации из различных источников и баз данных, соблюдая при этом основные требования информационной безопасности, а также методами и примерами обеспечения информационной безопасности.

3. Объем дисциплины (модуля).

3.1. Общая трудоемкость дисциплины (модуля).

Общая трудоемкость дисциплины (модуля) составляет 5 з.е. (180 академических часа(ов)).

3.2. Объем дисциплины (модуля) в форме контактной работы обучающихся с педагогическими работниками и (или) лицами, привлекаемыми к реализации образовательной программы на иных условиях, при проведении учебных занятий:

Тип учебных занятий	Количество часов	
	Всего	Семестр №6
Контактная работа при проведении учебных занятий (всего):	48	48
В том числе:		
Занятия лекционного типа	16	16
Занятия семинарского типа	32	32

3.3. Объем дисциплины (модуля) в форме самостоятельной работы обучающихся, а также в форме контактной работы обучающихся с педагогическими работниками и (или) лицами, привлекаемыми к реализации образовательной программы на иных условиях, при проведении промежуточной аттестации составляет 132 академических часа (ов).

3.4. При обучении по индивидуальному учебному плану, в том числе при ускоренном обучении, объем дисциплины (модуля) может быть реализован полностью в форме самостоятельной работы обучающихся, а также в форме контактной работы обучающихся с педагогическими работниками и (или) лицами, привлекаемыми к реализации образовательной программы на иных условиях, при проведении промежуточной аттестации.

4. Содержание дисциплины (модуля).

4.1. Занятия лекционного типа.

№ п/п	Тематика лекционных занятий / краткое содержание
1	ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ И ЗАЩИТА ИНФОРМАЦИИ: БАЗОВЫЕ ПОНЯТИЯ И ОРГАНИЗАЦИЯ Рассматриваемые вопросы: - проблема понятия «информационная безопасность»; - общие методы обеспечения информационной безопасности Российской Федерации; - организационная основа системы обеспечения информационной безопасности.
2	ИНФОРМАЦИЯ КАК ПРЕДМЕТ И ОБЪЕКТ ЗАЩИТЫ Рассматриваемые вопросы: - защищаемая информация; - виды защищаемой информации ограниченного доступа.
3	УГРОЗЫ ЗАЩИЩАЕМОЙ ИНФОРМАЦИИ Рассматриваемые вопросы: - классификация угроз защищаемой информации; - каналы и методы несанкционированного доступа к конфиденциальной информации.
4	МЕТОДОЛОГИЯ ЗАЩИТЫ ИНФОРМАЦИИ Рассматриваемые вопросы: - виды и методы защиты информации; - методы и средства защиты информации; - ресурсное обеспечение защиты информации; - создание системы защиты информации в организации.

4.2. Занятия семинарского типа.

Практические занятия

№ п/п	Тематика практических занятий/краткое содержание
1	Оценка уязвимостей информационных технологий Рассматриваемые вопросы: - оценка уязвимостей информационных технологий с использованием единой системы определения величины уязвимостей CVSS V2 и V3.
2	Основы проведения аудита информационной безопасности. Рассматриваемые вопросы: - основы проведения аудита информационной безопасности. Пассивный поиск информации.
3	Активный поиск информации Рассматриваемые вопросы: - активный поиск информации; - построение частной модели угроз безопасности информации и модели нарушителя в информационной системе организации.
4	Управление доступом в компьютерной системе. Рассматриваемые вопросы: - методы управления доступом в компьютерной системе.

№ п/п	Тематика практических занятий/краткое содержание
5	Парольная аутентификация. Рассматриваемые вопросы: - оценка стойкости парольной защиты; - генераторы паролей.
6	Простые шифровальные системы. Рассматриваемые вопросы: - построение и применение простых шифровальных систем.
7	Атака на зашифрованный текст Рассматриваемые вопросы: - атака на зашифрованный текст с использованием анализа частотности текста.
8	Симметричное и асимметричное шифрование. Рассматриваемые вопросы: - стандарты симметричного и асимметричного шифрования.
9	Электронная подпись. Рассматриваемые вопросы: - система Gpg4Win; - изучение инфраструктуры открытых ключей (PKI).
10	Стеганография. Рассматриваемые вопросы: - применене стеногрфии.
11	Анализ кадров Ethernet. Рассматриваемые вопросы: - использование программы Wireshark для анализа кадров Ethernet.
12	DLP-система Рассматриваемые вопросы: - DLP-система STAFFCOP ENTERPRISE.
13	Сканирование уязвимостей веб-приложений, серверов и компьютеров. Рассматриваемые вопросы: - инструменты для сканирования уязвимостей веб-приложений, серверов и компьютеров.
14	Тестирование безопасности Рассматриваемые вопросы: - практика тестирования безопасности с использованием Web Security Dojo.
15	Обеспечение безопасности Рассматриваемые вопросы: - обеспечение безопасности в Linux-системе.
16	Настройка идентификации и аутентификации Рассматриваемые вопросы: - настройка идентификации и аутентификации в Astra Linux.

4.3. Самостоятельная работа обучающихся.

№ п/п	Вид самостоятельной работы
1	Подготовка к практическим занятиям
2	Работа с лекционным материалом, литературой, самостоятельное изучение разделов (тем) дисциплины(модуля)
3	Выполнение курсового проекта.

4	Подготовка к промежуточной аттестации.
5	Подготовка к текущему контролю.

4.4. Примерный перечень тем курсовых проектов

Курсовой проект по дисциплине "Основы информационной безопасности" - это комплексная самостоятельная работа обучающегося. Темой курсового проекта является "Шифрование информации различными алгоритмами". Исходные данные выбираются согласно варианту:

Вариант 0

Исходное сообщение:
 Основными каналами телеграфной связи на железнодорожном транспорте являются каналы частотного телеграфирования
 $p=13$ и $g=3$

Вариант 1

Исходное сообщение:
 Характеристика узловой системы телеграфной сети железнодорожного транспорта и классификация видов телеграфной связи
 $p=11$ и $g=3$

Вариант 2

Исходное сообщение:
 Скелетная схема организации телеграфной связи управления железной дороги составляется по атласу железных дорог
 $p=13$ и $g=3$

Вариант 3

Исходное сообщение:
 Анализ систем организации телеграфной связи на железнодорожном транспорте и выбор телеграфных станций
 $p=19$ и $g=7$

Вариант 4

Исходное сообщение:
 Выбор каналообразующей аппаратуры производится с учетом обеспечения высокой устойчивости действия телеграфной связи
 $p=19$ и $g=5$

Вариант 5

Исходное сообщение:
Расчет нагрузки каналов телеграфной станции производится для часа на ибольшого значения потоков телеграфных сообщений

$$p=7 \text{ и } g=3$$

Вариант 6

Исходное сообщение:
Техническое задание на определение среднесуточной нагрузки проектируемой станции абонентского телеграфирования

$$p=13 \text{ и } g=7$$

Вариант 7

Исходное сообщение:
Точный расчет и выбор оптимального варианта организации телеграфной связи и размещения оборудования

$$p=17 \text{ и } g=11$$

Вариант 8

Исходное сообщение:
Характеристика и принципы организации телеграфной связи по системе абонентского телеграфирования и общего пользования

$$p=19 \text{ и } g=13$$

Вариант 9

Исходное сообщение:
Расчет телеграфной нагрузки для определения числа потребных каналов и необходимого количества оборудования для станции

$$p=17 \text{ и } g=7$$

Ключи шифрования:

K1=Фамилия

K2=ddmm (день и месяц рождения, 4 цифры, цифру 0, если она есть в дате, заменить на 9)

Число M:

Если последняя цифра номера зачетной книжки – прос...

5. Перечень изданий, которые рекомендуется использовать при освоении дисциплины (модуля).

№ п/п	Библиографическое описание	Место доступа
-------	----------------------------	---------------

1	Нестеров, С. А. Основы информационной безопасности : учебник для вузов / С. А. Нестеров. — Санкт-Петербург : Лань, 2021. — 324 с. — ISBN 978-5-8114-6738-9.	https://e.lanbook.com/book/165837
2	Рейн, Т. С. Основы информационной безопасности : учебное пособие / Т. С. Рейн, В. В. Торгулькин. — Кемерово : КемГУ, 2024. — 117 с. — ISBN 978-5-8353-3270-0.	https://e.lanbook.com/book/427526

6. Перечень современных профессиональных баз данных и информационных справочных систем, которые могут использоваться при освоении дисциплины (модуля).

Информационный портал Научная электронная библиотека eLIBRARY.RU (www.elibrary.ru);

Научно-техническая библиотека РУТ (МИИТ) (<http://library.miit.ru>);

Поисковые системы «Яндекс» для доступа к тематическим информационным ресурсам;

Электронно-библиотечная система издательства «Лань» — <http://e.lanbook.com/>;

Электронно-библиотечная система «УМЦ» — <http://www.umczdt.ru/>;

Электронно-библиотечная система «ZNANIUM.COM» — <http://www.znanium.com/>

7. Перечень лицензионного и свободно распространяемого программного обеспечения, в том числе отечественного производства, необходимого для освоения дисциплины (модуля).

Программное обеспечение для проведения занятий семинарского типа включает в себя программные продукты общего применения: операционная система Windows, пакет Microsoft Office, браузер с установленным Adobe Flash Player, Adobe Acrobat или его аналог

8. Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине (модулю).

Учебные аудитории для проведения учебных занятий, оснащенные компьютерной техникой и наборами демонстрационного оборудования.

9. Форма промежуточной аттестации:

Зачет в 6 семестре.

Курсовой проект в 6 семестре.

10. Оценочные материалы.

Оценочные материалы, применяемые при проведении промежуточной аттестации, разрабатываются в соответствии с локальным нормативным актом РУТ (МИИТ).

Авторы:

директор академии

А.В. Горелик

Согласовано:

Директор

Д.В. Паринов

Руководитель образовательной
программы

А.С. Киселёва

Председатель учебно-методической
комиссии

Д.В. Паринов