Федеральное государственное автономное образовательное учреждение высшего образования
«Российский университет дружбы народов»

Факультет физико-математических и естественных наук

Рекомендовано МССН
38.00.00 «Экономика и управление»,
подгруппа 4 «Бизнес-информатика»

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Наименование дисциплины
Информационная безопасность

Рекомендуется для направления подготовки
38.03.05 – Бизнес-информатика

1. Цели и задачи дисциплины

Целью дисциплины является введение учащихся в предметную область защиты современных систем и сетей телекоммуникаций. В процессе преподавания курса решаются следующие задачи:

- изучаются основные уязвимости операционных систем;
- даётся понятие о защите компьютерных сетей.

2. Место дисциплины в структуре ОП ВО

Цикл, к которому относится дисциплина «Информационная безопасность»: Б1 «Дисциплины (модули)», обязательная часть.

В таблице приведены предшествующие и последующие дисциплины, направленные на формирование компетенций дисциплины в соответствии с матрицей компетенций ОП ВО.

Предшествующие и последующие дисциплины, направленные на формирование компетенций

Универсальные компетенции

Шифр и наименование компетенции	Предшествующие дисциплины	Последующие дисциплины (группы дисциплин)
УК-2	• Правоведение	-

Профессиональные компетенции (вид профессиональной деятельности: научно-исследовательский)

Шифр и наименование компетенции	Предшествующие дисциплины	Последующие дисциплины (группы дисциплин)
ПК-3	• Архитектура вычислительных систем • Операционные системы • Вычислительные системы, сети и телекоммуникации • Реляционные базы данных • Управление ИТ-сервисами и контентом	Распределенные системы

3. Требования к результатам освоения дисциплины

Процесс изучения дисциплины направлен на формирование следующих компетенций: УК-2, ПК-3.

Расшифровка компетенций

- УК-2. Способен определять круг задач в рамках поставленной цели и выбирать оптимальные способы их решения, исходя из действующих правовых норм, имеющихся ресурсов и ограничений.
  - УК-2.1. Знает необходимые для осуществления профессиональной деятельности правовые нормы и методологические основы принятия управленческого решения.
- ПК-3. Способен выполнять работы и управлять работами по созданию (модификации) и сопровождению ИС, автоматизирующих задачи организационного управления и бизнес-процессы.

– ПК-3.1. Знает основы архитектуры, устройства и функционирования информационно-вычислительных систем и сетевых подсистем инфокоммуникационной системы организации; основы современных операционных систем; сетевые протоколы.

В результате изучения дисциплины студент должен:

Знать:

- основные уязвимости операционных систем;
- основные уязвимости компьютерных сетей.

Уметь:

- применять в профессиональной деятельности основы информационной безопасности;
- осуществлять элементарную настройку безопасносных конфигурираций операционных систем для использования в профессиональной деятельности.

Владеть:

- навыками установки и элементарной настройки систем обеспечения информационной безопасности для использования в профессиональной деятельности;
- способностью использовать современные инструментальные средства информационной безопасности.

4. Объем дисциплины и виды учебной работы

Общая трудоёмкость дисциплины составляет 3 зачетных единицы.

Вид учебной работы	Всего часов	Модуль
Аудиторные занятия (всего)	54	54
Лекции	18	18
Практические занятия (ПЗ)		
Семинары (С)		
Лабораторные работы (ЛР)	36	36
Самостоятельная работа (всего)	54	54
Общая трудоемкость	108	108
Зачётных единиц	3	3

5. Содержание дисциплины

5.1. Содержание разделов дисциплины

№	Наименование раздела дисциплины	Содержание раздела
1	Основы безопасности сетевых информационных технологий	• Основы безопасности сетевых информационных технологий. • Применение межсетевых экранов для защиты корпоративных сетей.
2	Защита информации в современных операционных системах	• Практические вопросы защиты операционных систем.
3	Криптография	• Место и роль криптографии в обеспечении

№	Наименование раздела дисциплины	Содержание раздела
		безопасности информационных технологий. • Криптографические примитивы и механизмы. • Теоретические основы инфраструктуры открытых ключей. • Практические аспекты инфраструктуры открытых ключей. • Развертывание инфраструктуры открытых ключей.

5.2. Разделы дисциплин и виды занятий

№	Наименование раздела дисциплины	Лекц	Практ. зан.	Лаб. зан.	Сем.	СРС	Всего час.
1	Основы безопасности сетевых информационных технологий	6				18	24
2	Защита информации в современных операционных системах	6		24		18	48
3	Криптография	6		12		18	36
	Всего часов	18		36		90	108

6. Лабораторный практикум

№ раздела дисциплины	Наименование лабораторных работ	Трудоёмкость (час.)
2	Установка и конфигурация операционной системы на виртуальную машину	4
2	Дискреционное разграничение прав в Linux. Основные атрибуты	4
2	Дискреционное разграничение прав в Linux. Два пользователя	4
2	Дискреционное разграничение прав в Linux. Расширенные атрибуты	4
2	Дискреционное разграничение прав в Linux. Исследование влияния дополнительных атрибутов	4
2	Мандатное разграничение прав в Linux	4
3	Элементы криптографии. Однократное гаммирование	6
3	Элементы криптографии. Шифрование (кодирование) различных исходных текстов одним ключом	6
	Всего часов	36

7. Практические занятия (семинары)

Не предусмотрены.

8. Материально-техническое обеспечение дисциплины

Мультимедийная аудитория для проведения учебных занятий (в том числе для лекционного типа занятий, индивидуальных и групповых консультаций, текущего контроля и промежуточной аттестации).

Компьютерные (дисплейные) классы с доступом к сети Интернет и электронно-образовательной среде Университета для выполнения обучающимися лабораторных работ по дисциплине, для проведения обучающимися самостоятельной работы и компьютерного тестирования обучающихся (при необходимости).

9. Информационное обеспечение дисциплины

Программное обеспечение:

- ОС Linux.
- Средство виртуализации VirtualBox (лицензия GPL-2.0, PUEL).
- Офисный пакет LibreOffice (лицензия MPL-2.0).
- ПО для просмотра формата pdf (например, `evince` (лицензия GPL-2+ CC-BY-SA-3.0)).
- GNU Midnight Commander (Лицензия GNU GPL 3).
- Редактор `emacs` (лицензия GPL).
- Редактор `vi` (лицензия BSD).
- Компилятор `gcc` (лицензия GPL).
- Система управления версиями Git (Лицензия GNU GPL 2).

Базы данных, информационно-справочные и поисковые системы:

- Сайт библиотеки РУДН http://lib.rudn.ru/.
- Сайт ТУИС http://esystem.pfur.ru/.

10. Учебно-методическое обеспечение дисциплины

- Основная литература
  - Зегжда Д. П., Ивашко А. М. Основы безопасности информационных систем. — М.: Горячая линия — Телеком, 2016. — 452 с.
  - Мэйволд Э. Безопасность сетей. Эком, 2016 г., 528 с. — http://www.intuit.ru/department/security/netsec/
- Дополнительная литература
  - Шумский А. А. Системный анализ в защите информации. — Учебное пособие для вузов. — М.: Гелиос АРВ, 2005. — 224 с.
  - Полянская О.Ю., Горбатов В.С. Инфраструктуры открытых ключей. БИНОМ. Лаборатория знаний, Интернет-университет информационных технологий — ИНТУИТ.ру, 2007. — http://www.intuit.ru/department/security/pki/
  - Галатенко В. А. Основы информационной безопасности. Интернет-университет информационных технологий — ИНТУИТ.ру, 2008 г., 208 с. — http://www.intuit.ru/department/security/secbasics/
  - Галатенко В.А. Стандарты информационной безопасности. Интернет-университет информационных технологий — ИНТУИТ.ру, 2005. — http://www.intuit.ru/department/security/secst/

11. Методические указания для обучающихся по освоению дисциплины

Учебным планом на изучение дисциплины отводится один модуль. В дисциплине предусмотрены контактные часы в виде лекций и лабораторного практикума. В течение

модуля выполняются лабораторные работы, подготовка и презентация доклада и контрольные мероприятия.

11.1 Методические указания по самостоятельному освоению теоретического материала по дисциплине

Лекционный материал дисциплины охватывает темы, указанные в разделе 5.1 программы дисциплины. В ТУИС (http://esystem.rudn.ru) по темам лекций размещены презентации и водео записи лекиций. Рекомендуется по указанным темам в дополнение изучить литературу, указанную в п. 10 программы дисциплины и учебно-методические материалы в ТУИС (http://esystem.pfur.ru).

11.2 Методические указания по выполнению лабораторных работ

- Задания по лабораторным работам выполняются индивидуально каждым студентом в дисплейных классах в соответствии с календарным планом и методическими указаниями по выполнению лабораторных работ по дисциплине.
- Часть лабораторных работ предусматривает задания для индивидуальной самостоятельной работы студента, обязательные для выполнения.
- Выполнение заданий для самостоятельной работы позволяет студенту приобрести дополнительные навыки и закрепить знания по изучаемой теме.
- По результатам выполнения каждой лабораторной работы студентом готовится отчёт. Отчёты в электронном виде сдаются студентом на проверку через соответствующие разделы ТУИС (http://esystem.pfur.ru).
- В качестве ответа на лабораторную работу в ТУИС необходимо загрузить:
    1. Ссылку на скринкаст с выполнением лабораторной работы (на *youtube*).
    2. Ссылку на скринкаст с презентацией лабораторной работы (на *youtube*).
    3. Ссылку на репозиторий на *Github*.
    4. Следует загрузить отдельными файлами (не общим архивом): отчёт в `markdown`; отчёт в `docx` (сделанный из markdown); отчёт в `pdf` (сделанный из markdown); архив с исходными материалами `markdown` (текстовые файлы, скриншоты и т. д.); презентацию в `pdf` (сделанная из `markdown`);презентацию в `markdown`.
- Срок сдачи указан для каждой лабораторной работы. В случае сдачи лабораторной не в срок, ставится не более 50% от максимального балла.

11.3. Рекомендации по подготовке доклада

Доклад – это публичное развёрнутое изложение по заданной теме.

Целями подготовки доклада являются: - внесение знаний из дополнительной литературы; - систематизация материла по теме; - развитие навыков самостоятельной работы с литературой; - пробуждение познавательного интереса к научному познанию.

Основными задачами подготовки доклада являются: - выработка умений излагать содержание материала в короткое время; - выработка умений ориентироваться в материале и отвечать на вопросы; - выработка умений самостоятельно обобщать и представлять материал, делать выводы.

Доклад должен состоять из трех частей: вступление, основная часть и заключение.

Вступление должно содержать: название доклада, сообщение основной идеи, современную оценку предмета изложения, краткое перечисление рассматриваемых вопросов, форму изложения.

Основная часть должна раскрывать суть затронутой темы. Задача основной части - представить достаточно данных для того, чтобы слушатели заинтересовались темой и захотели ознакомиться с материалами. При этом логическая структура основного блока должна содержать наглядные материалы, аудио-визуальные или визуальные материалы (представление рисунков, таблиц графиков).

Заключение должно содержать ясное чёткое обобщение и краткие выводы.

Время доклада – 5–7 мин. Чтение доклада при выступлении запрещено.

11.4. Рекомендации по подготовке презентации доклада

Презентация представляет собой последовательность сменяющих друг друга слайдов. Количество слайдов пропорционально содержанию и продолжительности выступления. На первом слайде обязательно представляется тема выступления и сведения об авторе. На слайды помещается фактический и иллюстративный материал (таблицы, графики, фотографии и пр.), который является уместным и достаточным средством наглядности, помогает в раскрытии стержневой идеи доклада.

В этом случае к слайдам предъявляются следующие требования: - выбранные средства визуализации информации (таблицы, схемы, графики и т. д.) соответствуют содержанию; - использованы иллюстрации хорошего качества (высокого разрешения), с четким изображением, максимальное количество графической информации на одном слайде – 2 рисунка (графики, схемы и т.д.) с текстовыми комментариями (не более 2 строк к каждому).

Наиболее важная информация должна располагаться в центре экрана. Обычный слайд, без эффектов анимации, должен демонстрироваться на экране не менее 10–15 секунд. Слайд с анимациями в среднем должен находиться на экране не меньше 40–60 секунд (без учета времени на случайно возникшее обсуждение). Для всех слайдов презентации необходимо использовать один и тот же шаблон оформления, кегль – для заголовков – не меньше 24 пунктов, для информации – для информации не менее 18. Наилучшей цветовой гаммой для презентации являются контрастные цвета фона и текста (белый фон – чёрный текст; темно-синий фон – светло-желтый текст и т. д.). Рекомендуется не злоупотреблять прописными буквами и не смешивать разные типы шрифтов в одной презентации.

12. Фонд оценочных средств для проведения промежуточной аттестации обучающихся по дисциплине (модулю)

ФОС по дисциплине представлен в приложении к данной программе.

Программа составлена в соответствии с требованиями ОС ВО РУДН.

Разработчики:
профессор кафедры прикладной информатики
и теории вероятностей, д.ф.-м.н. Д.С. Кулябов

Руководитель программы
Заведующий кафедрой
прикладной информатики и теории вероятностей,
д.т.н., проф. К.Е. Самуйлов

Федеральное государственное автономное образовательное учреждение высшего образования
«Российский университет дружбы народов»

Факультет физико-математических и естественных наук

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

Наименование дисциплины
Информационная безопасность

Рекомендуется для направления подготовки
38.03.05 – Бизнес-информатика

Паспорт фонда оценочных средств по дисциплине

Дисциплина: Информационная безопасность
Направление: 38.03.05 – Бизнес-информатика

Код контролируемой компетенции или её части	Контролируемый раздел дисциплины	Контролируемая тема дисциплины	А 1. 1	А 1. 2	А 2	А 3	Баллы темы	Баллы раздела
УК-2, ПК-3	Р1	Т1.1				5	5	5
	Р1	Т1.2						
	Р2	Т2.1	36	12	16	10	74	74
	Р3	Т3.1	12	4		5	21	21
	Р3	Т3.2						
	Р3	Т3.3						
	Итого:		48	16	16	20	100	100

Разделы:

- Р1: Основы безопасности сетевых информационных технологий
- Р2: Защита информации в современных операционных системах
- Р3: Криптография

Темы:

- Т1.1: Основы безопасности сетевых информационных технологий
- Т1.2: Применение межсетевых экранов для защиты корпоративных сетей
- Т2.1: Практические вопросы защиты операционных систем
- Т3.1: Криптографические примитивы и механизмы
- Т3.2: Основы инфраструктуры открытых ключей
- Т3.3: Протоколы аутентификации

Активности:

- А1.1: Лабораторные работы. Выполнение.
- А1.2: Лабораторные работы. Самопроверка и взаимопроверка.
- А2: Доклады по темам.
- А3: Итоговый контроль знаний (тест).

Процесс изучения дисциплины направлен на формирование следующих компетенций:

УК-2, ПК-3.

Расшифровка компетенций

- УК-2. Способен определять круг задач в рамках поставленной цели и выбирать оптимальные способы их решения, исходя из действующих правовых норм, имеющихся ресурсов и ограничений.
  - УК-2.1. Знает необходимые для осуществления профессиональной деятельности правовые нормы и методологические основы принятия управленческого решения.

- ПК-3. Способен выполнять работы и управлять работами по созданию (модификации) и сопровождению ИС, автоматизирующих задачи организационного управления и бизнес-процессы.
  - ПК-3.1. Знает основы архитектуры, устройства и функционирования информационно-вычислительных систем и сетевых подсистем инфокоммуникационной системы организации; основы современных операционных систем; сетевые протоколы.

Балльно-рейтинговая система оценки уровня знаний

Сводная оценочная таблица дисциплины

Раздел	Тема	A1.1	A1.2	A2	A3	Баллы темы	Баллы раздела
P1	T1.1				5	5	5
P1	T1.2						
P2	T2.1	36	12	16	10	74	74
P3	T3.1	12	4		5	21	21
P3	T3.2						
P3	T3.3						
Итого:		48	16	16	20	100	100

Разделы:

- P1: Основы безопасности сетевых информационных технологий
- P2: Защита информации в современных операционных системах
- P3: Криптография

Темы:

- T1.1: Основы безопасности сетевых информационных технологий
- T1.2: Применение межсетевых экранов для защиты корпоративных сетей
- T2.1: Практические вопросы защиты операционных систем
- T3.1: Криптографические примитивы и механизмы
- T3.2: Основы инфраструктуры открытых ключей
- T3.3: Протоколы аутентификации

Активности:

- A1.1: Лабораторные работы. Выполнение.
- A1.2: Лабораторные работы. Самопроверка и взаимопроверка.
- A2: Доклады по темам.
- A3: Итоговый контроль знаний (тест).

Таблица соответствия баллов и оценок

Баллы БРС	Традиционные оценки в РФ	Баллы для перевода оценок	Оценки	Оценки ECTS
86–100	5	95–100	5+	A
		86–94	5	B
69–85	4	69–85	4	C

Баллы БРС	Традиционные оценки в РФ	Баллы для перевода оценок	Оценки	Оценки ECTS
51–68	3	61–68	3+	D
		51–60	3	E
0–50	2	31–50	2+	FX
		0–30	2	F

Правила применения БРС

- Раздел (тема) учебной дисциплины считаются освоенными, если студент набрал более 50% от возможного числа баллов по этому разделу (теме).
- Студент не может быть аттестован по дисциплине, если он не освоил все темы и разделы дисциплины, указанные в сводной оценочной таблице дисциплины.
- По решению преподавателя и с согласия студентов, не освоивших отдельные разделы (темы) изучаемой дисциплины, в течение учебного семестра могут быть повторно проведены мероприятия текущего контроля успеваемости или выданы дополнительные учебные задания по этим темам или разделам. При этом студентам за данную работу засчитывается минимально возможный положительный балл (51% от максимального балла).
- При выполнении студентом дополнительных учебных заданий или повторного прохождения мероприятий текущего контроля полученные им баллы засчитываются за конкретные темы. Итоговая сумма баллов не может превышать максимального количества баллов, установленного по данным темам.
- График проведения мероприятий текущего контроля успеваемости формируется в соответствии с календарным планом курса. Студенты обязаны сдавать все задания в сроки, установленные преподавателем.
- Время, которое отводится студенту на выполнение мероприятий текущего контроля успеваемости, устанавливается преподавателем. По завершении отведённого времени студент должен сдать работу преподавателю, вне зависимости от того, завершена она или нет.
- Использование источников (в том числе конспектов лекций и лабораторных работ) во время выполнения контрольных мероприятий возможно только с разрешения преподавателя.
- Отсрочка в прохождении мероприятий текущего контроля успеваемости считается уважительной только в случае болезни студента, что подтверждается наличием у него медицинской справки, заверенной круглой печатью КДЦ РУДН, предоставляемой преподавателю не позднее двух недель после выздоровления. В этом случае выполнение контрольных мероприятий осуществляется после выздоровления студента в срок, назначенный преподавателем. В противном случае отсутствие студента на контрольном мероприятии признается неуважительным.
- Если в итоге за семестр студент получил 0–50 баллов, то студенту разрешается добор необходимого (до 51) количества баллов путём повторного одноразового выполнения предусмотренных контрольных мероприятий, при этом по усмотрению преподавателя аннулируются соответствующие предыдущие результаты. Ликвидация задолженностей проводится в сроки, согласованные с деканатом.
- Баллы за доклады по темам фиксируются только после доклада во время контактных часов.
- Оценки за лабораторные работы состоят из оценки за выполнение лабораторной работы и оценки за совместное оценивание лабораторной работы.

- Доклады:
  - Темы докладов распределены по лекциям.
  - При представлении темы после лекции, к которой она привязана, оценка снижается.
  - Оценка формируется из следующих элементов:
    - оформление презентации;
    - как сделан доклад;
    - содержание доклада;
    - оформление доклада.
  - Оценка выставляется только после выкладывания на сайт презентации и текста доклада.
  - Для получения оценки обязательно представление презентации во время соответствующего лекционного занятия.

Примерный перечень оценочных средств

по дисциплине Информационная безопасность

Аудиторная работа

Наименование оценочного средства	Краткая характеристика оценочного средства	Представление оценочного средства в фонде
Лабораторная работа	Система практических заданий, направленных на формирование практических навыков у обучающихся	Фонд практических заданий
Презентация (защита) доклада	Средство контроля способностей обучающихся представить перед аудиторией результаты проделанной работы	Темы докладов

Самостоятельная работа

Наименование оценочного средства	Краткая характеристика оценочного средства	Представление оценочного средства в фонде
Подготовка отчетов по результатам выполнения лабораторных работ	Форма проверки качества выполнения студентами лабораторных работ в соответствии с утвержденной программой	Фонд практических заданий
Доклад	Продукт самостоятельной работы студента, представляющий собой публичное выступление по представлению полученных результатов решения определенной учебно-практической, учебно-исследовательской или научной темы	Темы докладов

Учебным планом на изучение дисциплины отводится один модуль. В дисциплине предусмотрен контактные часы в форме лабораторного практикума, контрольные мероприятия по проверке отчётов по лабораторным работам, подготовка и презентация доклада. Оценка ставится по результатам работы в семестре.

Оценивание результатов освоения дисциплины производится в соответствии с больно-рейтинговой системой.

Критерии оценки по дисциплине

95–100 баллов:

- полное и своевременное выполнение на высоком уровне лабораторных работ с оформлением отчетов, успешное прохождение контрольных мероприятий, предусмотренных программой курса;
- систематизированное, глубокое и полное освоение навыков и компетенций по всем разделам программы дисциплины;
- использование научной терминологии, стилистически грамотное, логически правильное изложение ответов на вопросы, умение делать обоснованные выводы;
- безупречное владение программным обеспечением, умение эффективно использовать его в постановке и решении научных и профессиональных задач;
- выраженная способность самостоятельно и творчески решать поставленные задачи;
- полная самостоятельность и творческий подход при изложении материала по программе дисциплины;
- полное и глубокое усвоение основной и дополнительной литературы, рекомендованной программой дисциплины и преподавателем.

86–94 балла:

- полное и своевременное выполнение на хорошем уровне лабораторных работ с оформлением отчетов, успешное прохождение контрольных мероприятий, предусмотренных программой курса;
- систематизированное, глубокое и полное освоение навыков и компетенций по всем разделам программы дисциплины;
- использование научной терминологии, стилистически грамотное, логически правильное изложение ответа на вопросы, умение делать обоснованные выводы;
- хорошее владение программным обеспечением, умение эффективно использовать его в постановке и решении научных и профессиональных задач;
- способность самостоятельно решать поставленные задачи в нестандартных производственных ситуациях;
- усвоение основной и дополнительной литературы, нормативных и законодательных актов, рекомендованных программой дисциплины и преподавателем.

69–85 баллов:

- своевременное выполнение на хорошем уровне лабораторных работ с оформлением отчетов, прохождение контрольных мероприятий, предусмотренных программой курса;
- хороший уровень культуры исполнения лабораторных работ;
- систематизированное и полное освоение навыков и компетенций по всем разделам программы дисциплины;
- владение программным обеспечением, умение использовать его в постановке и решении научных и профессиональных задач;
- способность самостоятельно решать проблемы в рамках программы дисциплины;
- усвоение основной литературы;

51–68 баллов:

- выполнение на удовлетворительном уровне лабораторных работ с оформлением отчетов, прохождение контрольных мероприятий, предусмотренных программой курса;
- систематизированное и полное освоение навыков и компетенций по всем разделам программы дисциплины;

- удовлетворительное владение программным обеспечением, умение использовать его в постановке и решении научных и профессиональных задач;
- способность решать проблемы в рамках программы дисциплины;
- удовлетворительное усвоение основной литературы;

31–50 баллов – НЕ ЗАЧТЕНО:

- не выполнение, несвоевременное выполнение или выполнение на неудовлетворительном уровне лабораторных работ, не прохождение контрольных мероприятий, предусмотренных программой курса;
- недостаточно полный объем навыков и компетенции в рамках программы дисциплины;
- неумение использовать в практической деятельности научной терминологии, изложение ответа на вопросы с существенными стилистическими и логическими ошибками;
- слабое владение программным обеспечением по разделам программы дисциплины, некомпетентность в решении стандартных (типовых) производственных задач;
- способность решать проблемы в рамках программы дисциплины;
- удовлетворительное усвоение основной литературы;

0–30 баллов – НЕ ЗАЧТЕНО:

- отсутствие умений, навыков, знаний и компетенции в рамках программы дисциплины;
- невыполнение лабораторных заданий, не прохождение контрольных мероприятий, предусмотренных программой курса; отказ от ответов по программе дисциплины;
- игнорирование занятий по дисциплине по неуважительной причине.

Темы докладов

- Общая проблематика информационной безопасности.
  - Основные информационные угрозы современности.
  - Ключевые принципы информационной безопасности: конфиденциальность, целостность, доступность, невозможность отказа.
  - Нормативные документы в области информационной безопасности.
  - Органы, обеспечивающие информационную безопасность.
  - Программно-аппаратные средства системы обеспечения информационной безопасности.
  - Организационная защита объектов информатизации.
  - Информационная безопасность предприятия.
  - Доктрина информационной безопасности Российской Федерации.
- Хакерские атаки.
  - Социальная инженерия.
  - Вредоносные программы. Вирусы и антивирусы.
  - Вредоносные программы. Черви.
  - Вредоносные программы. Троянские программы.
  - Вредоносные программы. Руткиты.
  - Фишинг.
- Угрозы сетевой безопасности.
  - Безопасность физического и канального уровней модели OSI. Сетевые анализаторы и «снифферы».
  - DoS: методы обнаружения DoS-атак и средства защиты от них.
  - Безопасность ARP. ARP-spoofing.
  - Безопасность сетевого уровня модели OSI и меры его защиты.
  - Безопасность транспортного уровня модели OSI и меры его защиты.
  - Безопасность прикладного уровня модели OSI и меры его защиты.
  - Характеристика и механизмы удалённых атак на распределенные вычислительные системы.
  - Характеристика и механизмы удаленных атак на хосты Internet.
  - Способы атак на DNS-сервер.
  - Классы угроз информационной безопасности.
- Административная защита сетей.
  - Межсетевые экраны.
  - Виртуальные частные сети.
  - IDS системы. Обзор, сравнение, отечественные лидеры, мировые лидеры.
  - Система обнаружения атак Snort.
  - Применение межсетевых экранов для защиты корпоративных сетей.
  - Пакетный фильтр на базе ОС Linux.
  - Шлюзы прикладного уровня. Противодействие сетевым атакам при помощи межсетевых экранов.
  - Фильтрация пакетов: параметры и правила фильтрации.
  - DLP системы. Обзор, сравнение, отечественные лидеры, мировые лидеры.
  - Системы резервного копирования.
- Критерии безопасности информационных систем.
  - Обеспечение высокой доступности (нейтрализация отказов и обслуживаемости).
  - Законодательный уровень информационной безопасности.
  - Информация как ценность. Понятие об информационных угрозах.
  - Информационное право и информационная безопасность.

  - Защита компьютерной информации и компьютерных систем от вредоносных программ
  - Концепция (политика) безопасности.
  - Государственная система защиты информации.
  - Защита персональных данных в социальных сетях.
  - Защита государственной и коммерческой тайны.
  - Государственная система лицензирования. Система лицензирования деятельности в области защиты государственной тайны.
  - Цели и задачи защиты информации. Организация защиты конфиденциальной информации.
  - Политика безопасности предприятия и ее содержание.
  - Создание и функции службы безопасности на предприятии.
- Формальные модели безопасности ОС.
  - Модели безопасности ОС.
  - Дискреционные модели доступа. Списки управления доступом.
  - Мандатные модели доступа.
  - Ролевые модели доступа.
  - SELinux.
  - Методы разграничения доступа. Общий обзор.
  - Режим секретности и конфиденциального делопроизводства.
  - Защита электронного документооборота на предприятии.
- Криптография.
  - Общие вопросы шифрования.
  - Хеш-функции.
  - Цифровая подпись.
  - Квантовое шифрование. Квантовая передача информации.
  - Система PGP.
  - Электронные цифровые подписи. Механизмы цифровой подписи.
  - Протокол Kerberos.
  - Инфраструктура открытых ключей.
  - Техники управления ключами. Основные концепции. Жизненный цикл управления ключами.
  - Идентификация и аутентификация, управление доступом.
  - Протоколирование и аудит, шифрование, контроль целостности.
  - Биометрия.
  - Технология единого входа (OpenID и т.п.).
  - Контрольные суммы.
  - Ассиметричные криптосистемы. Обзор, виды, применение.
  - Симметричные криптосистемы. Обзор, виды, применение.
- Программные уязвимости.
  - Переполнение буфера.
  - Нарушения безопасности доступа к памяти: переполнения буфера, висячие указатели.
  - Ошибки проверки вводимых данных: ошибки форматирующей строки, неверная поддержка интерпретации метасимволов командной оболочки.
  - Ошибки проверки вводимых данных: SQL-инъекция.
  - Ошибки проверки вводимых данных: инъекция кода.
  - Ошибки проверки вводимых данных: инъекция E-mail.
  - Ошибки проверки вводимых данных: межсайтовый скриптинг в веб-приложениях, межсайтовый скриптинг при наличии SQL-инъекции.
  - Состояния гонки: ошибки времени-проверки-ко-времени-использования, гонки символьных ссылок.

- Ошибки путаницы привилегий: подделка межсайтовых запросов в веб-приложениях.
- Эскалация привилегий. Shatter attack.
- Уязвимость нулевого дня.

Методические указания и шкала оценок.

Рекомендации по подготовке доклада.

Доклад – это публичное развёрнутое изложение по заданной теме.

Целями подготовки доклада являются: - внесение знаний из дополнительной литературы; - систематизация материла по теме; - развитие навыков самостоятельной работы с литературой.

Основными задачами подготовки доклада являются: - выработка умений излагать содержание материала в короткое время; - выработка умений ориентироваться в материале и отвечать на вопросы; - выработка умений самостоятельно обобщать и представлять материал, делать выводы.

Доклад должен состоять из трех частей: вступление, основная часть и заключение.

Вступление должно содержать: название доклада, сообщение основной идеи, современную оценку предмета изложения, краткое перечисление рассматриваемых вопросов. Основная часть состоит из нескольких разделов, постепенно раскрывающих тему. Возможно использование иллюстрации (графики, диаграммы, фотографии, карты, рисунки). Для обоснования темы используется ссылка на источники с доказательствами, взятыми из литературы. Изложение материала должно быть связным, последовательным и доказательным. Способ изложения материала должен носить конспективный или тезисный характер. Заключение должно содержать ясное четкое обобщение и краткие выводы.

Время доклада – 5-7 мин (2-5 машинописных листа текста с докладом). Чтение доклада при выступлении – запрещено.

Рекомендации по подготовке презентации доклада.

Презентация представляет собой последовательность сменяющих друг друга слайдов. Количество слайдов пропорционально содержанию и продолжительности выступления. На первом слайде обязательно представляется тема выступления и сведения об авторе. На слайды помещается фактический и иллюстративный материал (таблицы, графики, фотографии и пр.), который является уместным и достаточным средством наглядности, помогает в раскрытии стержневой идеи доклада.

В этом случае к слайдам предъявляются следующие требования: - выбранные средства визуализации информации (таблицы, схемы, графики и т. д.) соответствуют содержанию; - использованы иллюстрации хорошего качества (высокого разрешения), с четким изображением, максимальное количество графической информации на одном слайде – 2 рисунка (графики, схемы и т.д.) с текстовыми комментариями (не более 2 строк к каждому).

Наиболее важная информация должна располагаться в центре экрана. Обычный слайд, без эффектов анимации, должен демонстрироваться на экране не менее 10–15 секунд. Слайд с анимациями в среднем должен находиться на экране не меньше 40–60 секунд (без учета времени на случайно возникшее обсуждение). Для всех слайдов презентации необходимо использовать один и тот же шаблон оформления, кегль – для заголовков – не меньше 24 пунктов, для информации – для информации не менее 18. Наилучшей цветовой гаммой для презентации являются контрастные цвета фона и текста (белый фон – чёрный текст; темно-синий фон – светло-желтый текст и т. д.). Рекомендуется не злоупотреблять прописными буквами и не смешивать разные типы шрифтов в одной презентации.

Критерии оценки

Оценивается содержание доклада, качество подготовки презентации, качество изложения материала, качество ответов на вопросы

Фонд практических (лабораторных) заданий

по дисциплине Информационная безопасность

Предлагаются к выполнению 8 лабораторных работ. Отчёты по лабораторным работам выполняются студентом самостоятельно, на лабораторном занятии студент может получить консультацию и методические указания от преподавателя.

Лабораторная работа № 1. Установка и конфигурация операционной системы на виртуальную машину

- Пользуясь методическими указаниями установить и сконфигурировать операционную систему на виртуальную машину.

Лабораторная работа № 2. Дискреционное разграничение прав в Linux. Основные атрибуты

Цель работы

Получение практических навыков работы в консоли с атрибутами файлов, закрепление теоретических основ дискреционного разграничения доступа в современных системах с открытым кодом на базе ОС Linux

Лабораторная работа № 3. Дискреционное разграничение прав в Linux. Два пользователя

Цель работы

Получение практических навыков работы в консоли с атрибутами файлов для групп пользователей.

Лабораторная работа № 4. Дискреционное разграничение прав в Linux. Расширенные атрибуты

Цель работы

Получение практических навыков работы в консоли с расширенными атрибутами файлов.

Лабораторная работа № 5. Дискреционное разграничение прав в Linux. Исследование влияния дополнительных атрибутов

Цель работы

Изучение механизмов изменения идентификаторов, применения SetUID- и Sticky-битов. Получение практических навыков работы в консоли с дополнительными атрибутами. Рассмотрение работы механизма смены идентификатора процессов пользователей, а также влияние бита Sticky на запись и удаление файлов.

Лабораторная работа № 6. Мандатное разграничение прав в Linux

Цели работы

Развить навыки администрирования ОС Linux. Получить первое практическое знакомство с технологией SELinux. Проверить работу SELinx на практике совместно с вебсервером Apache.

Лабораторная работа № 7. Элементы криптографии. Однократное гаммирование

Цель работы

Освоить на практике применение режима однократного гаммирования.

Лабораторная работа № 8. Элементы криптографии. Шифрование (кодирование) различных исходных текстов одним ключом

Цель работы

Освоить на практике применение режима однократного гаммирования на примере кодирования различных исходных текстов одним ключом.

Методические указания и шкала оценок

Порядок выполнения лабораторной работы заключается в следующем:

- Ознакомиться с разделами методических указаний к лабораторной работе.
- Выполнить задания лабораторной работы.
- Подготовить отчёт.

В качестве ответа на лабораторную работу в ТУИС необходимо загрузить:

1. Ссылку на скринкаст с выполнением лабораторной работы (на *youtube*).
2. Ссылку на скринкаст с презентацией лабораторной работы (на *youtube*).
3. Ссылку на репозиторий на *Github*.
4. Следует загрузить отдельными файлами (не общим архивом):
   - отчёт в `markdown`;
   - отчёт в `docx` (сделанный из markdown);
   - отчёт в `pdf` (сделанный из markdown);
   - архив с исходными материалами `markdown` (текстовые файлы, скриншоты и т. д.);
   - презентацию в `pdf` (сделанная из `markdown`);
   - презентацию в `markdown`.

Критерии оценки

Технические элементы отчёта лабораторной работы

- Скринкаст выполнения лабораторной работы
  - Ссылка на скринкаст выполнения лабораторной работы
  - Элементы скринкаста
    - Изображение рабочего стола с записью процесса выполнения лабораторной работы
    - Изображение выполняющего лабораторную работу с камеры компьютера (обычно в углу экрана)
    - Комментарии голосом, записанные в процессе выполнения лабораторной работы
- Отчёт о выполнении лабораторной работы
  - Форматы отчёта
    - `DOCX` (Для Лабораторных работ №1 и №2)
    - `Markdown` (Для Лабораторных работ №3 - №15)
    - `PDF` (полученный из `Markdown`) (Для Лабораторных работ №3 - №15)
    - `DOCX` (полученный из `Markdown`) (Для Лабораторных работ №3 - №15)
  - Структура отчёта
    - данные о работе (тема, дисциплина), ФИО автора и преподавателя;
    - цели и задачи;

        - объект и предмет исследования;
        - условные обозначения и термины;
        - список иллюстраций и таблиц;
        - теоретические вводные данные;
        - техническое оснащение и выбранные методы проведения работы;
        - полученные результаты;
        - анализ результатов;
        - заключение и выводы.
- Библиографическая информация
- Презентация по лабораторной работе
    - Размер презентации — 5-10 слайдов
    - Структура презентации
        - Представление выступающего (Who is this guy)
        - Прагматика выполнения лабораторной работы (Зачем)
        - Цель выполнения лабораторной работы
        - Задачи выполнения лабораторной работы
        - Результаты выполнения лабораторной работы
- Скринкаст презентации лабораторной работы

Соглашения об именовании

При выполнении работ следует придерживаться следующих правил именования: - пользователь внутри виртуальной машины должен иметь имя, совпадающее с учётной записью студента, выполняющего лабораторную работу. - Имя хоста вашей виртуальной машины должно совпадать с учётной записью студента, выполняющего лабораторную работу. - Имя виртуальной машины должно совпадать с учётной записью студента, выполняющего лабораторную работу. - В дисплейных классах вы можете посмотреть имя вашей учётной записи, набрав в терминале команду: id -un. - При установке на своей технике необходимо использовать имя вашей учётной записи дисплейных классов (Транслитерированные первые буквы имени и отчества, плюс транслитерированная фамилия). Например, если студента зовут Остап Сулейманович Бендер, то его учётная запись имеет вид osbender. - Идентификатор пользователя должен быть ясно различим на скриншотах в отчётах.

Технические критерии выполнения лабораторной работы

Критерий	0	1	2
Скринкаст	Отсутствует скринкаст + голос выполнения работы	Скринкаст + голос без фиксирования вебкамерой	Скринкаст + голос с фиксированием вебкамерой
Отчёт (*)	Нет отчёта в markdown	Есть отчёт в markdown (только текст)	Есть отчёт в markdown и архив с материалами (изображения)
Форматы (*)	Нет отчётов в других форматах	Отчёт в `docx` (из markdown)	Отчёт в `docx` и в `pdf` (из markdown)
Структура	Не соответствует структуре отчёта	Частично соответствует структуре отчёта	Полностью соответствует структуре отчёта
Подписи	Скриншоты не подписаны	Не все скриншоты подписаны	Все скриншоты подписаны
Ссылки	На скриншоты нет	Не на все скриншо-	На все скриншоты

Критерий	0	1	2
	ссылок	ты есть ссылки	есть ссылки
Полнота	Не все этапы работы описаны	Все этапы работы описаны	Все этапы работы описаны + подробное теоретическое введение
Библиография	Нет библиографии	Есть библиография, но ссылки не проставлены	Есть библиография с проставленными ссылками в тексте
Презентация	Презентация работы отсутствует	Есть презентация работы	Есть презентация работы и скринкаст
Оформление	Презентация сделана не в Markdown	Презентация сделана в Markdown	Markdown + научный стиль
Git	Работа не выложена на git	Работа выложена на хостинг git	Github + общепринятые коммиты + семантические версии + changelog

Содержательная часть работы

Критерий	0	1	2
Корректность выполнения	Выполнено не верно	Незначительные ошибки	Выполнено без ошибок
Анализ результатов	Не выполнен	Выполнен не в полном объёме	Выполнен в полном объёме
Запись выполнения работы	Запись отсутствует	Запись неполная или не всё пояснено	Запись полная, пояснения полные

Критерии выполнения соглашения об именовании лабораторной работы

Критерий	0	5	10
Именование	Отсутствует именование	Не везде выполнено соглашение об именовании	Везде выполнено соглашение об именовании