МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ
ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ
ВЫСШЕГО ОБРАЗОВАНИЯ

"БРАТСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ"

УТВЕРЖДАЮ

Проректор по учебной работе

_____ Е.И.Луковникова

18 февраля 2021 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

ФТД.В.02 Основы информационной безопасности сетей и систем

Закреплена за кафедрой **Управления в технических системах**

Учебный план bs270304_21_УТС.plx
27.03.04 Управление в технических системах

Квалификация **Бакалавр**

Форма обучения **заочная**

Общая трудоемкость **3 ЗЕТ**

Виды контроля на курсах:
Зачет 3

Распределение часов дисциплины по курсам

Курс	3		Итого	
Вид занятий	УП	РП		
Лекции	2	2	2	2
Лабораторные	2	2	2	2
Практические	2	2	2	2
В том числе инт.	4	4	4	4
Итого ауд.	6	6	6	6
Контактная работа	6	6	6	6
Сам. работа	98	98	98	98
Часы на контроль	4	4	4	4
Итого	108	108	108	108

Программу составил(и):
б.с., ст.пр., Ульянов А.Д. _____

Рабочая программа дисциплины

Основы информационной безопасности сетей и систем

разработана в соответствии с ФГОС:

Федеральный государственный образовательный стандарт высшего образования - бакалавриат по направлению подготовки 27.03.04 Управление в технических системах (приказ Минобрнауки России от 31.07.2020 г. № 871)

составлена на основании учебного плана:

27.03.04 Управление в технических системах
утвержденного приказом ректора от 01.03.2021 протокол № 80.

Рабочая программа одобрена на заседании кафедры

Управления в технических системах

Протокол от 09 апреля 2021 г. № 9

Срок действия программы: 2021-2025 уч.г.

Зав. кафедрой Игнатьев И.В. _____

Председатель МКФ
старший преподаватель Латушкина С.В. _____ №8 20 апреля 2021 г.

Ответственный за реализацию ОПОП _____ Игнатьев И.В.
(подпись) (ФИО)

Директор библиотеки _____ _____
(подпись) (ФИО)

№ регистрации 1761
(методический отдел)

1. ЦЕЛИ ОСВОЕНИЯ ДИСЦИПЛИНЫ	
1.1	Формирование у обучаемых знаний в области основ информационной безопасности и навыков практического обеспечения защиты информации и безопасного использования про граммных и аппаратных средств в сетях и системах связи.

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ООП	
Цикл (раздел) ООП:	ФТД.В.02
2.1	**Требования к предварительной подготовке обучающегося:**
2.1.1	Информатика
2.1.2	Программирование и основы алгоритмизации
2.1.3	Информационные сети и телекоммуникации
2.2	**Дисциплины и практики, для которых освоение данной дисциплины (модуля) необходимо как предшествующее:**
2.2.1	Производственная (преддипломная) практика
2.2.2	Моделирование систем управления

3. КОМПЕТЕНЦИИ ОБУЧАЮЩЕГОСЯ, ФОРМИРУЕМЫЕ В РЕЗУЛЬТАТЕ ОСВОЕНИЯ ДИСЦИПЛИНЫ (МОДУЛЯ)	
ПК-1: Способен к подготовке необходимых данных и составление технических заданий на проектирование АСУП	
Индикатор 1	ПК-1.5 Разрабатывает технические задания на проектирование АСУП в соответствии с требованиями информационной безопасности

В результате освоения дисциплины обучающийся должен

3.1	**Знать:**
3.1.1	Основы цифровой вычислительной техники, структуры и функционирование локальных вычислительных сетей и глобальной сети Интернет.
3.2	**Уметь:**
3.2.1	Оценивать основные проблемы, связанные с эксплуатацией и внедрением новой телекоммуникационной техники.
3.3	**Владеть:**
3.3.1	Навыками отладки с использованием соответствующих отладочных средств программного обеспечения сигнальных процессов и микроконтроллеров.

4. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

Код занятия	Вид занятия	Наименование разделов и тем	Семестр / Курс	Часов	Компетен-ции	Литература	Инте ракт.	Примечание
	Раздел	**Раздел 1. Введение в информационную безопасность**						
1.1	Лек	Понятие информационной безопасности	3	0,5	ПК-1	Л1.1 Л1.2Л2.1 Л2.2 Э1	0	ПК-1.5
1.2	Ср	Основные составляющие информационной безопасности	3	2	ПК-1	Л1.1 Л1.2Л2.1 Л2.2 Э1	0	ПК-1.5
1.3	Ср	Важность и сложность проблемы информационной безопасности	3	1	ПК-1	Л1.1 Л1.2Л2.1 Л2.2 Э1	0	ПК-1.5
1.4	Ср	Основные определения и критерии классификации угроз	3	2	ПК-1	Л1.1 Л1.2Л2.1 Л2.2 Э1	0	ПК-1.5
1.5	Ср	Некоторые примеры угроз доступности	3	1	ПК-1	Л1.1 Л1.2Л2.1 Л2.2 Э1	0	ПК-1.5

1.6	Ср	Вредоносное программное обеспечение	3	2	ПК-1	Л1.1 Л1.2Л2.1 Л2.2 Э1	0	ПК-1.5
1.7	Ср	Основные угрозы целостности	3	1	ПК-1	Л1.1 Л1.2Л2.1 Л2.2 Э1	0	ПК-1.5
1.8	Ср	Основные угрозы конфиденциальности	3	2	ПК-1	Л1.1 Л1.2Л2.1 Л2.2 Э1	0	ПК-1.5
1.9	Ср	Подготовка к зачету	3	20	ПК-1	Л1.1 Л1.2Л2.1 Л2.2 Э1	0	ПК-1.5
1.10	Зачёт		3	2	ПК-1	Л1.1 Л1.2Л2.1 Л2.2 Э1	0	ПК-1.5
	Раздел	**Раздел 2. Уровни информационной безопасности**						
2.1	Лек	Законодательный уровень информационной безопасности	3	0,5	ПК-1	Л1.1 Л1.2Л2.1 Л2.2 Э1	0	ПК-1.5
2.2	Ср	Обзор российского законодательства в области информационной безопасности	3	2	ПК-1	Л1.1 Л1.2Л2.1 Л2.2 Э1	0	ПК-1.5
2.3	Ср	Обзор зарубежного законодательства в области информационной безопасности	3	1	ПК-1	Л1.1 Л1.2Л2.1 Л2.2 Э1	0	ПК-1.5
2.4	Ср	Административный уровень информационной безопасности	3	1	ПК-1	Л1.1 Л1.2Л2.1 Л2.2 Э1	0	ПК-1.5
2.5	Ср	Политика безопасности	3	1	ПК-1	Л1.1 Л1.2Л2.1 Л2.2 Э1	0	ПК-1.5
2.6	Ср	Программа безопасности	3	1	ПК-1	Л1.1 Л1.2Л2.1 Л2.2 Э1	0	ПК-1.5
2.7	Ср	Синхронизация программы безопасности с жизненным циклом систем	3	1	ПК-1	Л1.1 Л1.2Л2.1 Л2.2 Э1	0	ПК-1.5
2.8	Ср	Процедурный уровень информационной безопасности	3	1	ПК-1	Л1.1 Л1.2Л2.1 Л2.2 Э1	0	ПК-1.5
2.9	Ср	Управление персоналом	3	1	ПК-1	Л1.1 Л1.2Л2.1 Л2.2 Э1	0	ПК-1.5
2.10	Ср	Физическая защита	3	1	ПК-1	Л1.1 Л1.2Л2.1 Л2.2 Э1	0	ПК-1.5

2.11	Ср	Поддержание работоспособности	3	1	ПК-1	Л1.1 Л1.2Л2.1 Л2.2 Э1	0	ПК-1.5
2.12	Ср	Реагирование на нарушения режима безопасности	3	1	ПК-1	Л1.1 Л1.2Л2.1 Л2.2 Э1	0	ПК-1.5
2.13	Ср	Планирование восстановительных работ	3	1	ПК-1	Л1.1 Л1.2Л2.1 Л2.2 Э1	0	ПК-1.5
2.14	Ср	Подготовка к зачету	3	20	ПК-1	Л1.1 Л1.2Л2.1 Л2.2 Э1	0	ПК-1.5
2.15	Зачёт		3	1	ПК-1	Л1.1 Л1.2Л2.1 Л2.2 Э1	0	ПК-1.5
	Раздел	**Раздел 3. Основные программно-технические меры информационной безопасности сетей и систем**						
3.1	Лек	Основные понятия программно-технического уровня информационной безопасности	3	1	ПК-1	Л1.1 Л1.2Л2.1 Л2.2 Э1	0	ПК-1.5
3.2	Ср	Особенности современных информационных систем, существенные с точки зрения безопасности	3	1	ПК-1	Л1.1 Л1.2Л2.1 Л2.2 Э1	0	ПК-1.5
3.3	Ср	Идентификация и аутентификация	3	1	ПК-1	Л1.1 Л1.2Л2.1 Л2.2 Э1	0	ПК-1.5
3.4	Ср	Архитектурная безопасность	3	1	ПК-1	Л1.1 Л1.2Л2.1 Л2.2 Э1	0	ПК-1.5
3.5	Ср	Управление доступом	3	1	ПК-1	Л1.1 Л1.2Л2.1 Л2.2 Э1	0	ПК-1.5
3.6	Ср	Протоколирование и аудит	3	1	ПК-1	Л1.1 Л1.2Л2.1 Л2.2 Э1	0	ПК-1.5
3.7	Ср	Активный аудит	3	1	ПК-1	Л1.1 Л1.2Л2.1 Л2.2 Э1	0	ПК-1.5
3.8	Ср	Шифрование	3	1	ПК-1	Л1.1 Л1.2Л2.1 Л2.2 Э1	0	ПК-1.5
3.9	Ср	Контроль целостности	3	1	ПК-1	Л1.1 Л1.2Л2.1 Л2.2 Э1	0	ПК-1.5
3.10	Ср	Экранирование	3	1	ПК-1	Л1.1 Л1.2Л2.1 Л2.2 Э1	0	ПК-1.5

3.11	Ср	Анализ защищенности	3	1	ПК-1	Л1.1 Л1.2Л2.1 Л2.2 Э1	0	ПК-1.5
3.12	Ср	Обеспечение высокой доступности	3	1	ПК-1	Л1.1 Л1.2Л2.1 Л2.2 Э1	0	ПК-1.5
3.13	Ср	Основы мер обеспечения высокой доступности	3	1	ПК-1	Л1.1 Л1.2Л2.1 Л2.2 Э1	0	ПК-1.5
3.14	Ср	Отказоустойчивость и зона риска	3	1	ПК-1	Л1.1 Л1.2Л2.1 Л2.2 Э1	0	ПК-1.5
3.15	Ср	Программное обеспечение промежуточного слоя	3	0,5	ПК-1	Л1.1 Л1.2Л2.1 Л2.2 Э1	0	ПК-1.5
3.16	Ср	Обеспечение обслуживаемости	3	0,5	ПК-1	Л1.1 Л1.2Л2.1 Л2.2 Э1	0	ПК-1.5
3.17	Лаб	Программирование арифметических алгоритмов	3	1	ПК-1	Л1.1 Л1.2Л2.1 Л2.2 Э1	1	Работа в малых группах,ПК-1.5
3.18	Лаб	Программирование алгебраических алгоритмов	3	1	ПК-1	Л1.1 Л1.2Л2.1 Л2.2 Э1	1	Работа в малых группах, ПК-1.5
3.19	Пр	Криптографические методы защиты	3	1	ПК-1	Л1.1 Л1.2Л2.1 Л2.2 Э1	1	Работа в малых группах, ПК-1.5
3.20	Пр	Шифрование методом IDEA	3	1	ПК-1	Л1.1 Л1.2Л2.1 Л2.2 Э1	1	Работа в малых группах, ПК-1.5
3.21	Ср	Подготовка к зачету	3	20	ПК-1	Л1.1 Л1.2Л2.1 Л2.2 Э1	0	ПК-1.5
3.22	Зачёт		3	1	ПК-1	Л1.1 Л1.2Л2.1 Л2.2 Э1	0	ПК-1.5

5. ОБРАЗОВАТЕЛЬНЫЕ ТЕХНОЛОГИИ

Традиционная (репродуктивная) технология (преподаватель знакомит обучающихся с порядком выполнения задания, наблюдает за выполнением и при необходимости корректирует работу обучающихся)

Образовательные технологии с использованием активных методов обучения (лекция – беседа, лекция – дискуссия, проблемная лекция, лекция-визуализация, лекция с заранее запланированными ошибками, лекция – пресс-конференция, лекция с разбором конкретных ситуаций, лекция-консультация, занятия с применением затрудняющих условий, методы группового решения творческих задач, метод развивающейся кооперации)

Технология компьютерного обучения(использование в учебном процессе компьютерных технологий и предоставляемых ими возможностях (электронные библиотеки, онлайн тесты, практические задания и т.д.))

6. ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

6.1. Контрольные вопросы и задания

Контрольные вопросы:

1. В чем главный принцип стенографии?
2. В каких «контейнерах» может быть спрятано зашифрованное сообщение?
3. Привести примеры стеганографии древних времён.
4. Дать определение аналитическим преобразованиям.
5. В каких случаях могут быть использованы аналитические преобразования?
6. К какой информации этот вид шифрования может быть применим?
7. Принцип действия метода шифрования Джиффорда?
8. Для каких целей использовался данный метода шифрования?
9. В каком году он был взломан?.
10. Что является входной информацией для шифра RC6?
11. Сколько нужно циклов шифрования для достаточной степени сокрытия информации?
12. На сколько блоков делиться входная информация?
13. Что является входной информацией для шифра IDEA?
14. Сколько нужно циклов шифрования для достаточной степени сокрытия информации?
15. На сколько блоков делиться входная информация?
16. Что такое шифрование?
17. Чем отличается открытый ключ от закрытого?
18. Дать определение стеганографии.

6.2. Темы письменных работ

учебным планом не предусмотренно

6.3. Фонд оценочных средств

Вопросы к зачету:

Раздел 1. Введение в информационную безопасность

1. Понятие и основные составляющие информационной безопасности.
2. Важность и сложность проблемы информационной безопасности.
3. Основные определения и критерии классификации угроз.
4. Наиболее распространенные угрозы доступности.
5. Вредоносное программное обеспечение.
6. Угрозы целостности.
7. Угрозы конфиденциальности.

Раздел 2. Уровни информационной безопасности

8. Что такое законодательный уровень информационной безопасности и почему он важен.
9. Обзор российского законодательства в области информационной безопасности.
10. Обзор зарубежного законодательства в области информационной безопасности.
11. Политика безопасности.
12. Программа безопасности.
13. Синхронизация программы безопасности с жизненным циклом инфокоммуникационных систем.
14. Управление рисками.
15. Основные классы мер процедурного уровня.
16. Управление персоналом.
17. Физическая защита.
18. Поддержание работоспособности.
19. Реагирование на нарушения режима безопасности.
20. Планирование восстановительных работ.

Раздел 3. Основные программно-технические меры информационной безопасности сетей и систем

21. Основные понятия программно-технического уровня информационной безопасности.
22. Особенности современных информационных систем, существенные с точки зрения безопасности.
23. Архитектурная безопасность.
24. Основные понятия об идентификации и аутентификации.
25. Парольная аутентификация.
26. Идентификация/ аутентификация с помощью биометрических данных.
27. Управление доступом.
28. Ролевое управление доступом.
29. Основные понятия протоколирования и аудита.
30. Активный аудит.
31. Симметричное и ассиметричное шифрование.
32. Контроль целостности: хэш-функции и электронно-цифровая подпись.
33. Экранирование: основные понятия и архитектурные аспекты.
34. Классификация межсетевых экранов.
35. Анализ защищенности.
36. Основные понятия доступности.
37. Основы мер обеспечения высокой доступности.
38. Отказоустойчивость и зона риска.
39. Обеспечение обслуживаемости.

6.4. Перечень видов оценочных средств
Отчеты по лабораторным работам, вопросы к зачету

7. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

7.1. Рекомендуемая литература

7.1.1. Основная литература

	Авторы,	Заглавие	Издательство,	Кол-во	Эл. адрес
Л1.1	Иванов М.Ю.	Информационные технологии: методы криптографии: учебное пособие	Братск: БрГУ, 2010	1	http://ecat.brstu.ru/catalog/Учебные%20и%20учебно-методические%20пособия/Информатика%20-%20Вычислительная%20техника%20-%20Программирование/Иванов%20М.Ю.%20Информационные%20технологии.Методы%20криптографии.2010.pdf
Л1.2	Нестеров С.А.	Основы информационной безопасности: учебное пособие	Санкт-Петербург: Издательство Политехническо го университета, 2014	1	http://biblioclub.ru/index.php?page=book&id=363040

7.1.2. Дополнительная литература

	Авторы,	Заглавие	Издательство,	Кол-во	Эл. адрес
Л2.1	Девянин П.Н.	Модели безопасности компьютерных систем. Управление доступом и информационными потоками: учебное пособие	Москва: Горячая линия-Телеком, 2012	5	
Л2.2	Малюк А.А., Пазизин С.В., Погожин Н.С.	Введение в защиту информации в автоматизированных системах: учебное пособие	Москва: Горячая линия-Телеком, 2011	5	

7.2. Перечень ресурсов информационно-телекоммуникационной сети "Интернет"

Э1	Издательство "Лань" электронно-библиотечная система	http://e.lanbook.com

7.3.1 Перечень программного обеспечения

7.3.1.1	Microsoft Windows Professional 7 Russian Upgrade Academic OPEN No Level
7.3.1.2	Microsoft Office 2007 Russian Academic OPEN No Level
7.3.1.3	Microsoft Office Professional Plus 2010 Russian Academic OPEN 1 license No Level
7.3.1.4	Microsoft Windows (Win Pro 10)+

7.3.2 Перечень информационных справочных систем

7.3.2.1	Национальная электронная библиотека НЭБ
7.3.2.2	Университетская информационная система РОССИЯ (УИС РОССИЯ)
7.3.2.3	
7.3.2.4	Научная электронная библиотека eLIBRARY.RU
7.3.2.5	Информационная система "Единое окно доступа к образовательным ресурсам"
7.3.2.6	Электронная библиотека БрГУ
7.3.2.7	Электронный каталог библиотеки БрГУ
7.3.2.8	«Университетская библиотека online»
7.3.2.9	Издательство "Лань" электронно-библиотечная система

8. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

1230	Лаборатория УТС	Учебная мебель Лабораторный комплекс «Локальные сети ЭВМ» .Телевизор LG 47.

9. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ (МОДУЛЯ)

Материал лекции учитывается при подготовке к лабораторным занятиям.
Для освоения обучающимися дисциплины и достижения запланированных результатов обучения. Учебным планом предусмотрены лекции, лабораторные работы, практические занятия, самостоятельная работа студента, подготовка и сдача зачета. В условиях рейтинговой системы контроля результаты текущего оценивания студента используются как показатель его текущего рейтинга.

Текущий контроль успеваемости осуществляется в течение семестра, в ходе повседневной учебной работы. Данный вид контроля стимулирует у обучающегося стремление к систематической самостоятельной работе по изучения дисциплины. Обучающийся, пользуясь рабочей программой, основной и дополнительной литературой, сам организует процесс изучения дисциплины.
Самостоятельная работа способствует сознательному усвоению, углублению и расширению теоретических знаний; форматирует необходимые профессиональные умения и навыки и совершенствует имеющиеся; происходит более глубокое осмысление методов научного и творческого познания конкретной дисциплины.
Основными формами такой работы являются:
- конспектирование лекций и прочитанного источника;
- проработка материалов прослушанной лекции;
- самостоятельное изучение программных вопросов, указанных преподавателем на лекциях и выполнение домашних заданий;
- обзор и обобщение литературы по интересующему вопросу;
- подготовка к лабораторным занятиям, практическим занятиям и зачету.