МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ,
МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ КЫРГЫЗСКОЙ РЕСПУБЛИКИ

МОО ВПО Кыргызско-Российский Славянский университет им. Б.Н. Ельцина

УТВЕРЖДАЮ
декан факультета

_____
_____ 2024 г.

Информационная безопасность

рабочая программа дисциплины (модуля)

Закреплена за кафедрой **Сетей связи и систем коммуникаций**

Учебный план b11030230_23_4итисс.plx
Направление 11.03.02 - РФ, 690300 - КР Инфокоммуникационные технологии и системы связи
Профиль "Сети связи и системы коммутации"

Квалификация **бакалавр**

Форма обучения **очная**

Общая трудоемкость **3 ЗЕТ**

Часов по учебному плану 108
в том числе:
аудиторные занятия 36
самостоятельная работа 71,8

Виды контроля в семестрах:
зачеты с оценкой 8

Распределение часов дисциплины по семестрам

Семестр (<Курс>.<Семестр на курсе>)	**8 (4.2)**		Итого	
Недель	14			
Вид занятий	УП	РП	УП	РП
Лекции	18	18	18	18
Лабораторные	9	9	9	9
Практические	9	9	9	9
Контактная работа в период теоретического обучения	0,2	0,2	0,2	0,2
В том числе инт.	8	8	8	8
В том числе в форме практ.подготовки	18	18	18	18
Итого ауд.	36	36	36	36
Контактная работа	36,2	36,2	36,2	36,2
Сам. работа	71,8	71,8	71,8	71,8
Итого	108	108	108	108

Программу составил(и):
к.т.н., доцент, Джылышбаев М.Н.;к.т.н., Кудцев Е.В. _____

Рецензент(ы):
к.т.н., доцент, Нач. каф., Оконов М.О. _____

Рабочая программа дисциплины
Информационная безопасность

разработана в соответствии с ФГОС 3++:
Федеральный государственный образовательный стандарт высшего образования - бакалавриат по направлению подготовки 11.03.02 Инфокоммуникационные технологии и системы связи (приказ Минобрнауки России от 19.09.2017 г. № 930)

составлена на основании учебного плана:
Направление 11.03.02 - РФ, 690300 - КР Инфокоммуникационные технологии и системы связи
Профиль "Сети связи и системы коммутации"
утвержденного учёным советом вуза от 29.06.2021 протокол № 10.

Рабочая программа одобрена на заседании кафедры
Сетей связи и систем коммуникаций

Протокол от _ __23_____ 2021 г. № _1
Срок действия программы: 2021-2025 уч.г.
Зав. кафедрой к.т.н., доцент Оконов М. О.

1. ЦЕЛИ ОСВОЕНИЯ ДИСЦИПЛИНЫ	
1.1	Ознакомить студентов с актуальными вопросами интегральной безопастности личности, объекта и информации. Особое внимание уделено обеспечению информационной безопастности, основным реализационным составляющим интегральной безопастности: технологиям, средства и услугам безопастности. Дать представление об их возможностях, достоинствах и недостатках, познакомить с новыми эффективными интегральными технологиями обеспечения безопасности.

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ООП	
Цикл (раздел) ООП:	Б1.В
2.1	**Требования к предварительной подготовке обучающегося:**
2.1.1	Программное обеспечение инфокоммуникационных технологий
2.1.2	Информатика
2.1.3	Ведедние в инфокоммуникационные технологии и системы связи
2.1.4	Информатика (спец. главы)
2.1.5	Общая теория связи
2.1.6	Направляющие систем электросвязи
2.1.7	Теория телетрафики
2.1.8	Цифровая обработка сигналов
2.1.9	Цифровые системы передачи
2.2	**Дисциплины и практики, для которых освоение данной дисциплины (модуля) необходимо как предшествующее:**
2.2.1	Основы права в инфокоммуникациях
2.2.2	Проектирование и эксплуатация систем связи
2.2.3	Сети связи

3. КОМПЕТЕНЦИИ ОБУЧАЮЩЕГОСЯ, ФОРМИРУЕМЫЕ В РЕЗУЛЬТАТЕ ОСВОЕНИЯ ДИСЦИПЛИНЫ (МОДУЛЯ)	
ПК-8: Способен к администрированию средств обеспечения безопасности удаленного доступа, операционных систем и специализированных протоколов	
Знать:	
Уровень 1	Нормативно-правовые нормативно-технические и организационно-методические документы, регламентирующие проектную подготовку, внедрение и эксплуатацию систем связи (телекоммуникационных систем), строительство объектов связи
Уровень 2	Принципы построения технического задания при автоматизации проектирования средств и сетей связи и их элементов; структуру и основы подготовки технической и проектной документации
Уметь:	
Уровень 1	Выявлять и анализировать преимущества и недостатки вариантов проектных решений, оценивать риски, связанные с реализацией проекта
Владеть:	
Уровень 1	Навыками сбора исходных данных, необходимых для разработки проектной документации

В результате освоения дисциплины обучающийся должен

3.1	**Знать:**
3.1.1	-технологии и топологии телекоммуникационных сетей.
3.1.2	-современные угрозы и каналы утечки информации.
3.1.3	-современные методы и средства обеспечения информационной безопасности.
3.1.4	-современные методы и средства обеспечения безопасности объектов.
3.2	**Уметь:**
3.2.1	-новые технологии информационной безопасности.
3.2.2	-новые технологии безопасности объектов.
3.3	**Владеть:**
3.3.1	-нанотехнологии и проксимити-технологии.
3.3.2	-рынок технических средств и услуг обеспечения безопасности.

4. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)								
Код занятия	**Наименование разделов и тем /вид занятия/**	**Семестр / Курс**	**Часов**	**Компетен-ции**	**Литература**	**Инте ракт.**	**Пр. подг.**	**Примечание**
	Раздел 1. Современые угрозы и каналы утечки информации							
1.1	Современные угрозы и каналы утечки информации. Особенности современных каналов утечки и несанкционированного доступа к информации. /Лек/	8	1	ПК-8	Л1.1 Л1.2 Л1.3Л2.1 Л2.2Л3.1 Э1	1		Лекция-беседа
1.2	Защита информации в сетях связи. Технические средства и методы защиты /Лаб/	8	1	ПК-8	Л1.2 Л1.3Л2.1 Л2.2Л3.1 Э1		1	Разбор примеров
1.3	Радиомониторинг безопасности /Ср/	8	2	ПК-8	Л1.1 Л1.2 Л1.3Л2.1 Л2.2Л3.1 Э1			
1.4	Аппаратная реализация современных методов несанкционированного доступа к информации /Лек/	8	1	ПК-8	Л1.2 Л1.3Л2.1 Л2.2 Л2.3Л3.1 Э1	1		Лекция-беседа
1.5	Система безопасности "ОПАС" /Ср/	8	2	ПК-8	Л1.2 Л1.3Л2.1 Л2.2 Л2.3Л3.1 Э1			
1.6	Современные угрозы информации в информационно - вычислительных и телекоммуникационных сетях /Лек/	8	1	ПК-8	Л1.2 Л1.3Л2.1 Л2.2 Л2.3Л3.1 Э1	1		Лекция-беседа
1.7	Аппаратура контроля линии связи. Анализатор ССТА- 1000, нелинейный детектор ВИЗИР-НЧ /Лаб/	8	1	ПК-8	Л1.2 Л1.3Л2.1 Л2.2Л3.1 Э1		1	Разбор примеров
1.8	Сравнительный анализ методов воздействия и противодействия в сетях INTER.NET. Какие существуют современные угрозы информации в телекоммуникационных сетях /Пр/	8	1	ПК-8	Л1.1 Л1.2 Л1.3Л2.1 Л2.2Л3.1 Э1		1	Разбор примеров
1.9	Технологии защиты систем безопасности от электромагнитного излучения /Ср/	8	2	ПК-8	Л1.2 Л1.3Л2.1 Л2.2Л3.1 Э1			
1.10	Современные методы и средства обеспечения информационной безопасности: основные понятия концепции безопасности АСОИ (Автоматическая система обработки информации) Методы и средства обеспечения безопасности /Лек/	8	1	ПК-8	Л1.2 Л1.3Л2.1 Л2.2 Л2.3Л3.1 Э1	1		Лекция - беседа

1.11	Рекомендации по защите систем безопасности от силового деструктивного воздействия /Ср/	8	3,8	ПК-8	Л1.2 Л1.3Л2.1 Л2.2 Л2.3Л3.1 Э1			
1.12	Анализ типовых мер безопасности. Методы и средства защиты не санкционированного доступа. Современный подход к обеспечению сетевой защиты информации. Современные технологические средства сетевой защиты компьютерной информации /Лек/	8	1	ПК-8	Л1.2 Л1.3Л2.1 Л2.2Л3.1 Э1	1		Лекция-беседа
1.13	Многофункциональные устройства индивидуальной защиты телефонных линий /Лаб/	8	1	ПК-8	Л1.2 Л1.3Л2.1 Л2.2Л3.1 Э1		1	Разбор примеров
1.14	Современные методы и средства обеспечения информационной безопасности в каналах ИВС и телекоммуникациях /Пр/	8	1	ПК-8	Л1.2 Л1.3Л2.1 Л2.2Л3.1 Э1		1	Разбор примеров
1.15	Промышленный шпионаж /Ср/	8	6	ПК-8	Л1.2 Л1.3Л2.1 Л2.2 Л2.3Л3.1 Э1			
1.16	Компоненты, которые подвержены угрозе. Основные компоненты угроз. Типы угроз. Основные пути несанкционированного получения информации /Лек/	8	1	ПК-8	Л1.2 Л1.3Л2.1 Л2.2 Л2.3Л3.1 Э1			
1.17	Рекомендации по защите систем безопасности от силового деструктивного воздействия /Ср/	8	6	ПК-8	Л1.2 Л1.3Л2.1 Л2.2Л3.1 Э1			
1.18	Система защиты телекоммуникационных сетей /Лек/	8	1	ПК-8	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3Л3.1 Э1	1		Лекция - беседа
1.19	Устройства уничтожения закладок BUGROASTER, КОБРА /Лаб/	8	1	ПК-8	Л1.1 Л1.2 Л1.3Л2.1 Л2.2Л3.1 Э1		1	Разбор примеров
1.20	Криптографические средства защиты /Пр/	8	1	ПК-8	Л1.2 Л1.3Л2.1 Л2.2Л3.1 Э1		1	Разбор примеров
1.21	Перехват информации в линиях связи /Ср/	8	6	ПК-8	Л1.2 Л1.3Л2.1 Л2.2 Л2.3Л3.1 Э1			
1.22	Система FS Communication System. Сдвоенный канал связи типа V.24/RS 232 и X.21. Программа управления защитой данных SE-5795 /Лек/	8	1	ПК-8	Л1.1 Л1.2 Л1.3Л2.1 Л2.2Л3.1 Э1	1		Лекция - беседа

1.23	Нормативно-правовая база защиты информации /Ср/	8	2	ПК-8	Л1.2 Л1.3Л2.1 Л2.2Л3.1 Э1			
	Раздел 2. Методы и средства обеспечения безопасности объектов							
2.1	Технические возможности реализации интегральной защиты в компьютерной телефонии. Системы: «Калейдоскоп плюс», «МАГ», интегральное терминальное устройство «Индекс» /Лек/	8	1	ПК-8	Л1.2 Л1.3Л2.1 Л2.2Л3.1 Э1			
2.2	Средства создания акустических маскирующих помех /Лаб/	8	1	ПК-8	Л1.2 Л1.3Л2.1 Л2.2Л3.1 Э1		1	Разбор примеров
2.3	Комплексная защита объекта. Технические средства физической защиты /Пр/	8	1	ПК-8	Л1.2 Л1.3Л2.1 Л2.2Л3.1 Э1		1	Разбор примеров
2.4	Программа управления защитой данных 8E-5795 /Ср/	8	6	ПК-8	Л1.2 Л1.3Л2.1 Л2.2Л3.1 Э1			
2.5	Датчики для обеспечения физической защиты. Новые технологии информационной безопасности. Обзор стенографических программ /Лек/	8	1	ПК-8	Л1.2 Л1.3Л2.1 Л2.2Л3.1 Э1			
2.6	Системы защиты телекоммуникационных сетей /Ср/	8	6	ПК-8	Л1.2 Л1.3Л2.1 Л2.2Л3.1 Э1			
2.7	Алгоритмы шифрования DES (Data Encryption Standard). Метод Clipper. Криптографические программные средства PGP. Российский стандарт ТОСТ 28147-89 /Лек/	8	1	ПК-8	Л1.2 Л1.3Л2.1 Л2.2Л3.1 Э1			
2.8	Основные пути несанкционированного получения информации /Ср/	8	6	ПК-8	Л1.2 Л1.3Л2.1 Л2.2Л3.1 Э1			
2.9	Современные методы и средства обеспечения безопасности объектов /Пр/	8	1	ПК-8	Л1.2 Л1.3Л2.1 Л2.2Л3.1 Э1		1	Разбор примеров
2.10	Технические средства пространственного и линейного зашумления /Лаб/	8	1	ПК-8	Л1.2 Л1.3Л2.1 Л2.2Л3.1 Э1		1	Разбор примеров
2.11	Мероприятия от несанкционированного доступа. Программы обеспечения Watchdog 4.1. Методы криптографической защиты /Лек/	8	1	ПК-8	Л1.2 Л1.3Л2.1 Л2.2Л3.1 Э1			
2.12	/КрТО/	8	0,2	ПК-8	Л1.2 Л1.3Л2.1 Л2.2Л3.1 Э1			

	Раздел 3. Технологии информационной безопасности. Обзор современных технических средств.							
3.1	Классификация носителей информации. Проксимити - технологии в системах обеспечения безопасности объектов /Лек/	8	1	ПК-8	Л1.2 Л1.3Л2.1 Л2.2Л3.1 Э1			
3.2	Еенераторы шума в акустическом диапазоне WNG-023, SP-21B,ЕНОМ-3, ЕШ-1000, ТУМАН-1 /Лаб/	8	1	ПК-8	Л1.1 Л1.2 Л1.3Л2.1 Л2.2Л3.1 Э1		1	Разбор примеров
3.3	Оценка скрытности по критерию ХИ квадрат. Оценка скрытности переходов в потоке НЗБ (наименее 6-7 2 значимые биты). Оценка скрытности по группированию серии в потоке НЗБ /Пр/	8	1	ПК-8	Л1.1 Л1.2 Л1.3Л2.1 Л2.2Л3.1 Э1		1	Разбор примеров
3.4	Мероприятия от несанкционированного доступа /Ср/	8	6	ПК-8	Л1.2 Л1.3Л2.1 Л2.2Л3.1 Э1			
3.5	Нормативно-правовая база защиты информации /Лек/	8	1	ПК-8	Л1.2 Л1.3Л2.1 Л2.2Л3.1 Э1			
3.6	Новая эффективная технология защиты /Лек/	8	1	ПК-8	Л1.2 Л1.3Л2.1 Л2.2 Л2.3Л3.1 Э1			
3.7	Средства создания маскирующих помех в сетях электропитания. NG-201, СПЕРНИК /Лаб/	8	1	ПК-8	Л1.1 Л1.2 Л1.3Л2.1 Л2.2Л3.1 Э1		1	Разбор примеров
3.8	Технические возможности реализации интегральной защиты компьютерной телефонии. Технологии пассивной защиты от утечки информации /Пр/	8	1	ПК-8	Л1.1 Л1.2 Л1.3Л2.1 Л2.2Л3.1 Э1		1	Разбор примеров
3.9	Методы криптографической защиты /Ср/	8	6	ПК-8	Л1.1 Л1.2 Л1.3Л2.1 Л2.2Л3.1 Э1			
3.10	Рекомендации по защите систем безопасности от силового деструктивного воздействия /Лек/	8	1	ПК-8	Л1.1 Л1.2 Л1.3Л2.1 Л2.2Л3.1 Э1			
3.11	Технические средства защиты информации /Ср/	8	6	ПК-8	Л1.1 Л1.2 Л1.3Л2.1 Л2.2Л3.1 Э1			
3.12	Системы защиты телекоммуникационных сетей /Лек/	8	1	ПК-8	Л1.1 Л1.2 Л1.3Л2.1 Л2.2Л3.1 Э1			

3.13	Многофункциональные устройства защиты СОНАТ А-ДУ, ЕРОМ-ЗИ-4 /Лаб/	8	1	ПК-8	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3Л3.1 Э1		1	Разбор примеров
3.14	Современные средства компьютерной телефонии /Пр/	8	2	ПК-8	Л1.2 Л1.3Л2.1 Л2.2 Л2.3Л3.1 Э1		2	Разбор примеров
3.15	Защита от несанкционированной аудиозаписи. Защита информации в компьютерных сетях /Ср/	8	6	ПК-8	Л1.2 Л1.3Л2.1 Л2.2Л3.1 Э1			
3.16	Программа управления защитой данных 8Е-5795 /Лек/	8	1	ПК-8	Л1.2 Л1.3Л2.1 Л2.2Л3.1 Э1	1		Лекция - беседа

5. ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

5.1. Контрольные вопросы и задания

Вопрос уровня ЗНАТЬ к зачёту:

1. Особенности современных каналов утечки и несанкционированного доступа к информации.
2. Причины возникновения электрических каналов утечки.
3. Сравнительные характеристики пассивных средств получения информации.
4. Сравнительные характеристики активных средств получения информации.
5. Классификация программных закладок используемых и INTERNET.
6. Концепция безопасности АСОИ. (Автоматическая система обработки информации).

Вопрос уровня УМЕТЬ к зачёту:

7. Технические средства обнаружения угроз безопасности.
8. Современные угрозы информации в телекоммуникационных сетях.
9. Технические средства обнаружения угроз безопасности.
10. Современные методы и средства обеспечения информационной безопасности.
11. Модель системы безопасности.
12. Средства обеспечения.

Вопрос уровня ВЛАДЕТЬ к зачёту:

13. Типы угроз.
14. Системы защиты телекоммуникационных сетей.
15. Методы криптографической защиты.
16. Технические средства и методы защиты.
17. Защита информации от ВЧ - навязывания.
18. Защита в проводных каналах.
19. Оценка уровня скрытости по критерию ХИ квадрат.
20. Оценка скрытности по количеству переходов в потоке НЗБ (Наименее значимые биты).

5.2. Темы курсовых работ (проектов)

Курсовые работы, курсовые проекты в учебном плане не предусмотрены.

5.3. Фонд оценочных средств

Темы рефератов:

1. Назначение технического устройства Спринт.
2. Назначение технического устройства BUGROASTER.
3. Назначение технического устройства СОПЕРНИК.
4. Алгоритм шифрования DEC.
5. Инфракрасные датчики контроля пространства.
6. Назначение технического устройства КОБРА.
7. Средства обеспечения безопасности.
8. Назначение технического устройства ГШ-1000.
9. Метод шифрования информации по технологии Clipper.
10. Назначение технического устройства СМОГ.

5.4. Перечень видов оценочных средств

Контрольные вопросы;
Задание лабораторных занятий;

Задание практических занятий;
Задание самостоятельных работ (рефераты).

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

6.1. Рекомендуемая литература

6.1.1. Основная литература

	Авторы, составители	Заглавие	Издательство, год
Л1.1	А.А. Малюк, В.С. Горбатов, В.И. Королев и др.	Введение в информационную безопасность: Учебное пособие для вузов	Москва .: Горячая линия-Телеком 2013
Л1.2	Мельников В.П., Клейменов С.А., Клейменов С.А., Петраков А.М.	Информационная безопасность и защита информации: Учебное пособие для студентов высших учебных заведений	М.: Издательский центр "Академия" 2008
Л1.3	Блинов А.М.	Информационная безопасность. Ч. 1.: Учебное пособие	СПб.: Изд-во СПбГУЭФ 2010

6.1.2. Дополнительная литература

	Авторы, составители	Заглавие	Издательство, год
Л2.1	Мельников В.П., Клейменов С.А., Клейменов С.А., Петраков А.М.	Информационная безопасность и защита информации: Учебное пособие для студентов высших учебных заведений	М.: Издательский центр "Академия" 20082012
Л2.2	Макаренко С.И.	Информационная безопасность: Учебное пособие для студентов вузов	Ставрополь: СФ МГГУ им. М.А. Шолохова 2009
Л2.3	Горбатов Малюк, Королев В.С., Горбатова В.С.	Введение в информационную безопасность: Учебное пособие для вузов	М.: Горячая линия- Телеком 2013

6.1.3. Методические разработки

	Авторы, составители	Заглавие	Издательство, год
Л3.1	Шаньгин, В. Ф.	Информационная безопасность компьютерных систем и сетей: учеб. Пособие	М.: ИД «ФОРУМ»: ИНФРА-М, 2012

6.2. Перечень ресурсов информационно-телекоммуникационной сети "Интернет"

Э1	Информационная безопасность	http://center-yf.ru/data/stat/informacionn

6.3. Перечень информационных и образовательных технологий

6.3.1 Компетентностно-ориентированные образовательные технологии

6.3.1.1	Традиционные образовательные технологии – технологии, ориентированные прежде всего на сообщение знаний и способов действий, передаваемых учащимся в готовом виде и предназначенных для воспроизводящего усвоения. Предполагают, что педагог является единственным инициативно действующим лицом учебного процесса. К ним могут быть отнесены лекции, семинары, лабораторные работы репродуктивного типа и т.д.
6.3.1.2	Инновационные образовательные технологии – занятия в интерактивной форме, которые формируют системное мышления и способность генерировать идеи при решении различных творческих задач. К формам интерактивных лекций, применяемых в рамках дисциплины, относятся: лекция-беседа, лекция-дискуссия, лекция с разбором конкретных ситуаций.
6.3.1.3	Лекция-беседа, или «диалог с аудиторией», является наиболее распространенной и сравнительно простой формой вовлечения студентов в учебный процесс. Эта лекция предполагает непосредственный контакт преподавателя с аудиторией. Преимущество лекции-беседы состоит в том, что она позволяет привлекать внимание слушателей к наиболее важным вопросам темы, определять содержание и темп изложения учебного материала с учетом особенностей обучаемых.
6.3.1.4	Лекция-дискуссия. В отличие от лекции-беседы здесь преподаватель при изложении лекционного материала не только использует ответы слушателей на свои вопросы, но и организует свободный обмен мнениями в интервалах между логическими разделами.
6.3.1.5	Дискуссия – это взаимодействие преподавателя и учащегося, свободный обмен мнениями, идеями и взглядами по исследуемому вопросу. Это оживляет учебный процесс, активизирует познавательную деятельность аудитории и, что очень важно, позволяет преподавателю управлять коллективным мнением группы, использовать в целях убеждения, преодоления негативных установок и ошибочных мнений некоторых обучаемых.
6.3.1.6	По ходу лекции-дискуссии преподаватель приводит отдельные примеры в виде ситуаций или кратко сформулированных проблем и предлагает студентам коротко обсудить, затем краткий анализ, выводы и лекция продолжается.

6.3.1.7	Лекция с разбором конкретных ситуаций. Данная лекция по форме похожа на лекцию-дискуссию, однако, на обсуждение преподаватель ставит не вопросы, а конкретную ситуацию. Поэтому изложение ее должно быть очень кратким, но содержать достаточную информацию для оценки характерного явления и обсуждения. Слушатели анализируют и обсуждают эти микроситуации и обсуждают их сообща, всей аудиторией.
6.3.1.8	К формам интерактивных семинаров и практических занятий, применяемых в рамках дисциплины, относятся: творческие задания.
6.3.2 Перечень информационных справочных систем и программного обеспечения	
6.3.2.1	http://center-yf.ru/data/stat/informacionnaya-bezopasnost.php - Информационная безопасность

7. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)	
7.1	В качестве материально-технического обеспечения дисциплины могут быть использованы:
7.2	
7.3	• Лекционная аудитория с видеопроектором с беспроводной сетью управления через ноутбук с подключением локальную сеть кафедры ССиСК и в Интернет. При этом имеется возможность проведения лекций на основе разработанных презентаций и учебно-методических материалов в сети кафедры ССиСК и в Интернете.
7.4	• Лаборатория компьютерных технологий с 10-ю ПК подключенных в локальную сеть кафедры и в Интернет.
7.5	• Лаборатория Цифровых систем коммутации и Цифровых систем передачи. В данных лабораториях имеются 19 многофункциональных стендов:
7.6	- 6 стендов по цифровым системам коммутации, включенных в единную сеть;
7.7	- 3 стенда по Цифровым системам передачи;
7.8	- 2 стенда по Схемотехнике ТК устройств;
7.9	- 1 стенд по Электропитанию ТК устройств;
7.10	- 3 стенда по Направляющим системам передач;
7.11	- 4 стенда по АЦП и ЦАП.
7.12	• Измерения и диагностика на данных стендах проводятся с помощью 15 электронных осциллографов АКИИП совместно 15 ПК.
7.13	Кроме того для проведения исследований и учебных занятий имеются генераторы сигналов (4 шт), указатели уровня (4 шт), аналоговые осцилографы (4 шт), Лабораторный блок питания (2 шт), Мультиметры (4 шт) и т.п..

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

8.1.Порядок и условия изучения и контроля знаний по дисциплине «Информационная безопастность»

Изучение дисциплины студентами осуществляется в форме лекций и лабораторных занятий, выполнения заданий самостоятельных работ и контроля знаний.

Текущий контроль

Текущий контроль осуществляется в течение семестра при опросе на лекционных и лабораторных занятиях, при выполнении лабораторных работ, в виде опроса теоретического материалах, и при контроле самостоятельной работы.

Учебный материал разбит на разделы. Проверка освоения студентами материала каждого раздела осуществляется на рубежных контролях - при подготовке и выступлении с докладами, при подготовке и защите рефератов, при выполнении контрольных работ.

Баллы по каждому виду контроля отражены в технологической карте дисциплины. Результаты текущего контроля, рубежного контроля и самостоятельной работы студентов учитываются при оценке итоговой успеваемости студентов.

Средства оценки текущей успеваемости основаны на % вкладе в выполнение различных форм обучения, в сумме составляющем 100%.

Для получения зачета по дисциплине сумма баллов, полученная студентом по результатам прохождения текущего и рубежного контроля (контрольных точек), должна быть 60 и более баллов.

Система перевода 100 бальной оценки к пятибалльной.

85 – 100 баллов отлично
70 – 84 баллов хорошо
60 – 69 баллов удовлетворительно
Меньше 60 баллов неудовлетворительно

Технологическая карта дисциплины "Информационная безопастность" приведена в ПРИЛОЖЕНИИ

Программа дисциплины предусматривает теоретическое обучение, лабораторные занятия и самостоятельную работу. Теоретическое обучение осуществляется в форме лекционных занятий в аудиториях со специальными техническими средствами (видеопроектор, компьютеры с беспроводным подключением в локальную сеть и в Интернет и др.), позволяющих проводить занятия с наглядными материалами, с возможностью просмотра необходимого материала через локальную сеть кафедры, университета и через Интернет. Имеется возможность проведения лекций на основе презентаций. Некоторые занятия могут проводится в интерактивной форме, например, в виде «разбора ситуаций», когда по итогам пройденного материала, заранее ставится конкретная задача, студенты готовятся по данной тематике и на занятиях

делается разбор ситуации.
Лабораторные занятия будут проводится на многофункциональных стендах по элементной базе систем связи и по "Схемотехника" с использованием измерительных и вспомогательных средств (мультиметры, амперметры, вольтметры, осциллографы, источники питания, электропаяльники и принадлежностик нему и др.). Студенты при подготовке к самостоятельной работе могут пользоватся компьютерным классом подключенным в локальную сеть кафедры ССиСК и в Интернет. и в компьютерном классе, позволяющих проводить занятия с наглядными материалами, с возможностью просмотра необходимого материала через локальную сеть кафедры, университета и через Интернет.
Самостоятельная работа включает в себя изучение вопросов теоретического курса, не рассматриваемых на лекциях (вследствие ограничения времени, отводимого на лекционные занятия), повторение теоретического материала, рассматриваемого в ходе лекционных занятий, с целью закрепления полученных знаний, а также изучение теоретических сведений в ходе подготовки к лабораторным занятиям, математическую обработку результатов лабораторных исследований, их оформление и защиту.
Целью самостоятельной работы студентов является самостоятельное изучение части вопросов теоретического курса.
Рекомендации по организации самостоятельной работы студента
1. Советы по планированию и организации времени, необходимого для изучения дисциплины. Рекомендуется следующим образом организовать время, необходимое для изучения дисциплины:
Изучение конспекта лекции в тот же день, после лекции – 10-15 минут.
Изучение конспекта лекции за день перед следующей лекцией – 10-15 минут.
Изучение теоретического материала по учебнику и конспекту – 1 час в неделю.
Подготовка к практическому занятию – 2 час.
Всего в неделю – 3 часа 30 минут.
2. Описание последовательности действий студента
Для понимания материала и качественного его усвоения рекомендуется такая последовательность действий:
1. После прослушивания лекции и окончания учебных занятий, при подготовке к занятиям следующего дня, нужно сначала просмотреть и обдумать текст лекции, прослушанной сегодня (10-15 минут).
2. При подготовке к лекции следующего дня, нужно просмотреть текст предыдущей лекции, подумать о том, какая может быть тема следующей лекции (10-15 минут).
3. В течение недели выбрать время (1-час) для работы с рекомендуемой литературой в библиотеке.
4. При подготовке к практическим занятиям следующего дня, необходимо сначала прочитать основные понятия и подходы по теме домашнего задания. При выполнении упражнения или задачи нужно сначала понять, что требуется в задаче, какой теоретический материал нужно использовать, наметить план решения задачи.
3. Рекомендации по использованию материалов учебно-методического комплекса. Рекомендуется использовать методические указания по курсу, текст лекций преподавателя.
4. Рекомендации по работе с литературой. Теоретический материал курса становится более понятным, когда дополнительно к прослушиванию лекции и изучению конспекта, изучаются и книги. Легче освоить курс, придерживаясь одного учебника и конспекта. Рекомендуется, кроме «заучивания» материала, добиться состояния понимания изучаемой темы дисциплины. С этой целью рекомендуется после изучения очередного параграфа выполнить несколько простых упражнений на данную тему. Кроме того, очень полезно мысленно задать себе следующие вопросы (и попробовать ответить на них): о чем этот параграф?, какие новые понятия введены, каков их смысл?, что даст это на практике?
Полезно просмотреть весь материал курса, представить основную идею содержания дисциплины – цели, задачи, где используется на практике Инфокоммуникационных технологий.
При разработке конкретных тем представить логическую последовательность и место данного материала в общем содержании дисциплины.
5. Советы по подготовке к рубежному и промежуточному контролям. Дополнительно к изучению конспектов лекции необходимо пользоваться учебником. Кроме «заучивания» материала, очень важно добиться состояния понимания изучаемых тем дисциплины. С этой целью рекомендуется после изучения очередного параграфа выполнить несколько упражнений на данную тему. Кроме того, очень полезно мысленно задать себе следующие вопросы (и попробовать ответить на них): о чем этот параграф?, какие новые понятия введены, каков их смысл?, что даст это на практике?.
При подготовке к промежуточному контролю нужно изучить теорию: определения всех понятий и подходы к оцениванию до состояния понимания материала и самостоятельно решить несколько типовых задач из каждой темы. При решении задач всегда необходимо уметь качественно интерпретировать итог решения.
6. Указания по организации работы с контрольно-измерительными материалами, по выполнению домашних заданий. При выполнении домашних заданий необходимо сначала прочитать основные понятия и подходы по теме задания. При выполнении упражнения или задачи нужно сначала понять, что требуется в задаче, какой теоретический материал нужно использовать, наметить план решения задачи, а затем приступить к расчетам и сделать качественный вывод.

Подготовка доклада к занятию.
Основные этапы подготовки доклада:
- выбор темы;
- консультация преподавателя;
- подготовка плана доклада;
- работа с источниками и литературой, сбор материала;
- написание текста доклада;
- оформление рукописи и предоставление ее преподавателю до начала доклада, что определяет готовность студента к выступлению;
- выступление с докладом, ответы на вопросы.

Тематика доклада предлагается преподавателем в ФОС.

Рекомендации по написанию реферата.

1. Тема реферата выбирается в соответствии с Вашими интересами и не обязательно должна соответствовать приведенному ниже примерному перечню. Важно, чтобы в реферате: во-первых, были освещены как естественнонаучные, так и социальные стороны проблемы; а во-вторых, представлены как общетеоретические положения, так и конкретные примеры. Особенно приветствуется использование конкретных примеров из реальной практики, связанная с физическими прцессами в элементах электроники.

2. Реферат должен основываться на проработке нескольких дополнительных к основной литературе источников. Как правило, это специальные учебники и учебные пособия по электронике и физическим основам электроники. Рекомендуется использовать также в качестве дополнительной литературы научно-популярные журналы: "Радиолоцман", "Радио", "Радиоаматор", "Наука и жизнь", "Сети и Телекоммуникации", "Телекоммуникации" и др.

3. План реферата должен быть авторским. В нем проявляется подход автора, его мнение, анализ проблемы.

4. Все приводимые в реферате факты и заимствованные соображения должны сопровождаться ссылками на источник информации. Например: ... Нас заинтересовало снижение рождаемости, зарегистрированное в последнее время в России (Население России, 2008)... или ... Установлено, что в крупных городах, таких как Москва, уровень загрязнения воздуха в некоторые часы может превышать предельно допустимые концентрации в 10 и более раз (Лихачева, Смирнова, 2006) ...

5. Недопустимо просто скомпоновать реферат из кусков заимствованного текста. Все цитаты должны быть представлены в кавычках с указанием в скобках источника и страницы, например: "Проанализировав качества каналов связи, в работе А.Л.Воронина, было установлено, что наиболее подходящим для качественной передачи информации, является оптические каналы связи." (Воронин А.Л., 1995, с.39). Отсутствие кавычек и ссылок означает плагиат и, в соответствии с установившейся научной этикой, считается грубым нарушением авторских прав.

6. Реферат оформляется в виде текста на листах стандартного формата (А-4). Начинается с титульного листа, в котором указывается название вуза, учебной дисциплины, тема реферата, фамилия и инициалы студента, номер академической группы или название кафедры, год и географическое место местонахождения вуза. Затем следует оглавление с указанием страниц разделов. Сам текст реферата желательно подразделить на разделы: главы, подглавы и озаглавить их. Приветствуется использование в реферате количественных данных и иллюстраций (графики, таблицы, диаграммы, рисунки).

7. Завершают реферат разделы "Заключение" и "Список использованной литературы". В заключении представлены основные выводы, ясно сформулированные в тезисной форме и, обычно, пронумерованные.

8. Список литературы должен быть составлен в полном соответствие с действующим стандартом (правилами), включая особую расстановку знаков препинания. Для этого достаточно использовать в качестве примера любую книгу изданную крупными научными издательствами: "Сети и Телекоммуникация", "Радио", "Радиолоцман", "Радиоаматор" и др. Или приведенный выше список литературы. В общем случае наиболее часто используемый в нашей стране порядок библиографических ссылок следующий:

Автор И.О. Название книги. Место издания: Издательство, Год издания. Общее число страниц в книге.

Автор И.О. Название статьи // Название журнала. Год издания. Том__. № __. Страницы от __ до ___.

Автор И.О. Название статьи / Название сборника. Место издания: Издательство, Год издания. Страницы от __ до ___.

ЛИСТ РЕГИСТРАЦИИ ИЗМЕНЕНИЙ
к рабочей программе дисциплины (модуля)

Информационная безопасность

наименование дисциплины

№ п/п	Основание внесения изменения	Раздел/ пункт	Содержание изменения
1.	№357-П от 24 июня 2026- О преобразовании Естественно-технического факультета и Факультета архитектуры дизайна и строительства в Политехнический институт КРСУ	Титульный лист. Пункт Разработано	Заменить слова «Разработано Кафедра Сети связи и системы коммуникации» словами «Разработано: Высшая школа Цифровых технологий»
2.			
3.			
4.			
5.			