ГОУ ВПО «ДОНЕЦКИЙ НАЦИОНАЛЬНЫЙ УНИВЕРСИТЕТ»

ФИЗИКО-ТЕХНИЧЕСКИЙ ФАКУЛЬТЕТ

Кафедра радиофизики и инфокоммуникационных технологий

УТВЕРЖДАЮ:
проректор по научно-методической
и учебной работе
_____ Е.И. Скафа
«__» _____ 2020 г.

РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ

«ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В ПРОФЕССИОНАЛЬНОЙ ДЕЯТЕЛЬНОСТИ»

Специальность:	45.05.01 Перевод и переводоведение
Специализация:	Специальный перевод (английский и немецкий языки)
Образовательная программа:	специалитет
Квалификация:	лингвист-переводчик
Форма обучения:	очная

Донецк 2020

УТВЕРЖДАЮ:
Декан физико-технического факультета
_____ С. А. Фоменко
«17» апреля 2020 г.
МП

Программа составлена на основании Федерального государственного образовательного стандарта высшего образования (ФГОС ВО) специальности 45.05.01 Перевод и переводоведение, утвержденного приказом Министерства образования и науки Российской Федерации от 17 октября 2016 г. N 1290 с изменениями и дополнениями от 13 июля 2017г.;
Порядка организации учебного процесса в образовательных организациях высшего профессионального образования Донецкой Народной Республики, утвержденного приказом Министерства образования и науки ДНР № 1171 от «10» ноября 2017 г.;
учебного плана и основной образовательной программы Специальный перевод (английский и немецкий языки) специальности 45.05.01 Перевод и переводоведение, разработанных в ГОУ ВПО «Донецкий национальный университет».

Разработчики:
Профессор кафедры РФ и ИКТ, д.т.н. _____ В.В. Данилов

Старший преподаватель кафедры РФ и ИКТ. _____ М.В. Бабичева

Программа учебной дисциплины утверждена на заседании кафедры радиофизики и инфокоммуникационных технологий
Протокол № 17 от «06» апреля 2020 г.

Заведующий кафедрой РФ и ИКТ _____ В.В. Данилов

Программа учебной дисциплины одобрена учебно-методической комиссией факультета иностранных языков

Протокол № 4 от «15» апреля 2020 г.
Председатель учебно-методической комиссии факультета _____ О.Л. Бессонова

1. ОБЛАСТЬ ПРИМЕНЕНИЯ И МЕСТО ДИСЦИПЛИНЫ В УЧЕБНОМ ПРОЦЕССЕ

Учебная дисциплина «Основы информационной безопасности в профессиональной деятельности» относится к базовой части первого блока. Трудоемкость освоения дисциплины составляет 2 зач.ед. или 72 час. Изучается в 7 семестре, по дисциплине предусмотрен зачет. Для успешного изучения данной учебной дисциплины необходимы знания, умения и навыки, сформированные в процессе:

- изучения программы общеобразовательной школы;

Освоение дисциплины обеспечивает формирование у студентов современных навыков профессиональной и безопасной работы с информационными системами и документами.

2. СТРУКТУРА ДИСЦИПЛИНЫ

Характеристика учебной дисциплины	
Специальность:	45.05.01 Перевод и переводоведение
Специализация	Специальный перевод (английский и немецкий языки)
Образовательная программа	специалитет
Квалификация	лингвист-переводчик
Количество содержательных модулей	2
Дисциплина базовой / вариативной части образовательной программы	Блок 1 «Дисциплины (модули)» Базовая часть
Формы контроля (МК, экзамен, зачет)	Модульный контроль, зачет
Показатели	очная форма обучения
Количество зачетных единиц (кредитов)	2
Год подготовки	4
Семестр	7
Количество часов	72
- лекционных	28
- практических, семинарских	–
- лабораторных	–
- самостоятельной работы	44
в т.ч. индивидуальное задание	–
Недельное количество часов,	5
в т.ч. аудиторных	2

3. ОПИСАНИЕ ДИСЦИПЛИНЫ

Цель – знакомство с понятиями национальной безопасности; видами безопасности; ИБ в системе национальной безопасности; основными понятиями, общеметодологическими принципами теории ИБ; анализом угроз ИБ, проблемами информационной войны; государственной информационной политикой; видами информации; методами и средствами обеспечения ИБ; методами нарушения конфеденциальности, целостности и доступности информации; причинами, видами, каналами утечки и искажения информации.

Задачи:

1) получение представления о многообразии задач и методов защиты информации;
2) знакомство с основными разделами информационной безопасности;
3) овладение основными практическими методами предупреждения и отражения информационных угроз;
4) приобретение навыков самостоятельно анализировать каналы утечки информации и выбирать соответствующие средства защиты;

5) углубление навыков безопасного использования международной сети Internet, браузеров, операционных систем, приложений, связанных с документооборотом и ПК.

Требования к результатам освоения дисциплины. Процесс изучения дисциплины направлен на формирование элементов следующих компетенций в соответствии с ФГОС ВО РФ по специальности 45.05.01 Перевод и переводоведение и основной образовательной программы высшего профессионального образования специальности 45.05.01 Перевод и переводоведение. Специальный перевод (английский и немецкий языки)

а) ***общекультурных (ОК):***

– способностью использовать основы правовых знаний в различных сферах жизнедеятельности (ОК-3);

– способностью понимать социальную значимость своей будущей профессии, цели и смысл государственной службы, обладать высокой мотивацией к выполнению профессиональной деятельности в области защиты интересов личности, общества и государства, соблюдать нормы профессиональной этики (ОК-4);

– способностью логически верно, аргументированно и ясно строить устную и письменную речь на русском языке, в том числе по профессиональной тематике, публично представлять собственные и известные научные результаты, вести дискуссии (ОК-6);

– способностью к самоорганизации и самообразованию (ОК-7);

б) общепрофессиональных (ОПК):

– способностью работать с различными источниками информации, информационными ресурсами и технологиями, осуществлять поиск, хранение, обработку и анализ информации из разных источников и баз данных, представлять её в требуемом формате с использованием информационных, компьютерных и сетевых технологий, владеть стандартными методами компьютерного набора текста и его редактирования на русском и иностранном языке (ОПК-1);

– способностью соблюдать в профессиональной деятельности требования правовых актов в области информационной безопасности, защиты государственной тайны и иной информации ограниченного доступа, обеспечивать соблюдение режима секретности (ОПК-2);

– способностью самостоятельно осуществлять поиск профессиональной информации в печатных и электронных источниках, включая электронные базы данных (ОПК-5);

в) профессиональных (ПК):

– способностью применять методику ориентированного поиска информации в справочной, специальной литературе и компьютерных сетях (ПК-8);

– способностью к обобщению, критическому осмыслению, систематизации информации, анализу логики рассуждений и высказываний (ПК-15);

– способностью оценивать качество и содержание информации, выделять наиболее существенные факты и концепции, давать им собственную оценку и интерпретацию (ПК-16);

– способностью работать с материалами различных источников, осуществлять реферирование и аннотирование письменных текстов, составлять аналитические обзоры по заданным темам, находить, собирать и первично обобщать фактический материал, делая обоснованные выводы (ПК-17);

В результате изучения учебной дисциплины студент должен

знать:

терминологию в области информационной безопасности,

методы и средства обеспечения информационной безопасности,

методы нарушения конфиденциальности, целостности и доступности информации.

содержание основных понятий по правовому обеспечению информационной безопасности;

основы безопасности операционных систем;

основы безопасности вычислительных сетей;

основные технические средства и методы защиты информации;

основные программно-аппаратные средства обеспечения информационной безопасности.

уметь:

правильно проводить анализ угроз информационной безопасности, выполнять основные этапы решения задач информационной безопасности, применять на практике основные общеметодологические принципы теории информационной безопасности;

отыскивать необходимые нормативные правовые акты и информационно-правовые нормы в системе действующего законодательства, в том числе с помощью систем правовой информации;

применять действующую законодательную базу в области информационной безопасности;

разрабатывать проекты нормативных материалов, регламентирующих работу по защите информации, а также положений, инструкций и других организационно-распорядительных документов;

***владеть*:**

способами комплексного обеспечения информационной безопасности на основе разработанных программ и методик, с обеспечением требований нормативных документов, регламентирующих режим соблюдения государственной тайны;

выполнять оперативное управление деятельностью организаций по комплексному обеспечению информационной безопасности конкретных автоматизированных систем;

4. СОДЕРЖАНИЕ ДИСЦИПЛИНЫ И ФОРМЫ ОРГАНИЗАЦИИ УЧЕБНОГО ПРОЦЕССА

Курс дисциплины «Основы информационной безопасности в профессиональной деятельности» предусматривает следующие *формы организации учебного процесса*:

1) лекции,

2) самостоятельная работа студента.

Материал излагается с использованием объяснительно-иллюстративных, эвристических и исследовательских методов преподавания. При проведении лекций для обсуждения материала используются мультимедийные презентации. При чтении лекций по всем разделам программы теоретический материал иллюстрируется большим количеством примеров, что позволяет сделать изложение наглядным и продемонстрировать обучаемым приемы решения поставленных задач.

В учебном процессе применяются активные и интерактивные формы проведения занятий (разбор конкретных ситуаций, дискуссия, полемика), внеаудиторная самостоятельная работа, балльно-рейтинговая система оценки успеваемости, личностно-ориентированное обучение, проблемное обучение, блочно-модульное обучение.

Самостоятельная работа студентов предусматривает выполнение индивидуальных заданий, подготовку к самлсьлятельным занятиям, изучение учебной, научной и методической литературы, составление конспектов.

Используются следующие методы контроля:

1) устный контроль (экспресс-опрос на лекциях);
2) проверка конспектов;
3) проверка самостоятельных работ;
4) доклад, на выбранную тему;

Порядковый номер и тема	**Краткое содержание темы**
Содержательный модуль 1	
Тема 1. Понятие и структура информационной безопасности.	Основные понятия информационной безопасности. Правовые основы ИБ и законодательство ДНР об информации. Информация, информационная система, владелец информации. Виды информации. Конфиденциальная информация, государственная тайна. Нормативные документы РФ по ИБ. Конфеденциальность, целостность, доступность.
Тема 2. Основы криптографии	Историческая справка, примитивные шифры. Шифр xor, Цезаря, Винежера. Симметричные и ассиметричные методы. Суть ассимметричного шифрования. Алгоритм RSA и Эль-Гамаля. Симметричное шифрование. Гаммирование. Квантовая криптография.
Тема 3. Авторизация и аутентификация	Авторизация, аутентификация и идентификация. Системы аутентификации. Парольная защита. Метода взлома пароля. Хеширование. Электронные методы аутентификации. Биометрические методы аутентификации. Распространенность методов аутентификации.
Тема 4. Защита в компьютерных сетях	Уязвимости компьютерных сетей. Основные виды атак при передаче информации. Снифферы. Ответвления трафика. Анализ электромагнитных излучений. Атаки на канальном и сетевом уровне. Спуфинг. Виды сканирования. DOS и DDOS атаки. Подмена IP адреса. Меры противодействия атакам. Виртуальные сети.
Содержательный модуль 2	
Тема 5. Вирусы и антивирусы	История создания вирусов. Классификация вирусов. Загрузочные, файловые, макросы, скрипт-вирусы. Вирусы для Linux, Android, iOSm Трояны, черви, собственно вирусы. Хакеры. Платные и бесплатные антивирусы. Возможности антивирусного ПО.
Тема 6. Техническая защита информации	Каналы утечки информации. Радиозакладки. Пассивные, активные и полуактивные РЗ. Детектирование радиозакладок. Нелинейные локаторы.Акустические и лазерные микрофоны. Утечка по виброканалу. Стетоскопы. Генераторы шума, скремблеры, постановщики помех.IP шифраторы и токены. Электронные замки.
Тема 7. Модели управления доступом	Различные модели управления доступом. Составляющие модели управления доступом. Мандатная модель доступа. Разграничение доступа. Разработка и эксплуатация защищенных автоматизированных систем. Планирование, организация и контроль выполнения работ и мероприятий по защите персональных данных;
Тема 8. Организация мероприятий по защите информации.	Методы и уровни защиты конфиденциальности, целостности и доступности информации. Причины, виды, каналы утечки и искажения информации. Основные направления обеспечения информационной безопасности объектов информационной сферы государства в условиях информационной войны.

Тематический план

	Количество часов					
	Очная форма обучения					
	всего	в т.ч.				
		лекции	практические	лабораторные	самостоятель-ная работа	индивидуальная работа
Тема 1.	**9**	4			5	
Тема 2.	**9**	4			5	
Тема 3.	**10**	4			6	
Тема 4.	**10**	4			6	
Итого по содержательному модулю 1	**38**	**16**			**22**	
Тема 5.	**9**	4			5	
Тема 6.	**9**	4			5	
Тема 7.	**8**	2			6	
Тема 8.	**8**	2			6	
Итого по содержательному модулю 2	**34**	**12**			**22**	
Всего по курсу	**72**	**28**			**44**	

5. МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ ДЛЯ ПРОВЕДЕНИЯ ЛЕКЦИОННЫХ, ПРАКТИЧЕСКИХ И ЛАБОРАТОРНЫХ ЗАНЯТИЙ

Темы лекционных занятий

№ п/п	***Название темы***	***Количество часов***
1	Основные понятия и составляющие информационной безопасности	2
2	Защита файлов и папок	2
3	Криптография и криптоанализ	2
4	Хеш-функции и их применение в информационной безопасности	2
5	Аутентификация по паролю	2
6	Уязвимости компьютерных сетей	2
7	Web- безопасность	2
8	Вирусы	2
9	Антивирусы	2
10	Технические средства защиты информации	2
11	Защита документов	2
12	Электронно-цифровая подпись	2
13	Методы социальной инженерии	2
14	Модели управления доступом	2
	ВСЕГО	**28**

6. МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ ПО ОРГАНИЗАЦИИ САМОСТОЯТЕЛЬНОЙ РАБОТЫ СТУДЕНТОВ

Самостоятельная работа студентов по курсу «Основы информационной безопасности в профессиональной деятельности» предусматривает:

– систематическое ведение конспекта лекций и повседневную проработку лекционного материала;

– изучение дополнительной литературы и интернет-источников, в т.ч. рекомендуемых этой программой;

– изучение необходимого инструментария;

– подготовку и защиту докладов по выбранным темам.

Темы для докладов студенты выбирают из списка или предлагают свои, связанные с обеспечением информационной безопасности.

Список предлагаемых тем, для докладов:

1. История криптографии
2. Квантовая криптография
3. XSS – атаки.
4. Поисковик Shodan
5. Форензика.
6. Стеганография.
7. Технология tor.
8. DOS и DDOS атаки
9. Фишинговые сайты
10. Видеонаблюдение
11. Google Hacking
12. Безопасность интернета вещей
13. Honey Pots.
14. Как работает интернет. HTML, CSS, Java Script.
15. Куки.
16. Хакеры.
17. Угрозы, исходящие от ботов.

Организация самостоятельной работы студентов

№ п/п	***Название темы***	***Количество часов***
1	Законодательно-правовые основы информационной безопасности.	5
2	Криптография и криптоанализ.	5
3	Авторизация и аутентификация.	6
4	Защита в компьютерных сетях.	6
5	Вирусы и антивирусы.	5
6	Техническая защита информации.	5
7	Модели управления доступом.	6
8	Организация мероприятий по защите информации.	6
	ВСЕГО	**44**

7. ИНДИВИДУАЛЬНЫЕ ЗАДАНИЯ

Индивидуальные задания учебным планом не предусмотрены

8. КОНТРОЛЬНЫЕ ВОПРОСЫ К ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ

1. Что такое информация? Свойства информации. Информационные технологии.
2. Составляющие информационной безопасности.
3. Правовые основы защиты информации.
4. Информация с точки зрения возможности ее распространения.
5. Какая информация относится к конфиденциальной?
6. Какая информация относится к государственной тайне?
7. Три категории стандартной модели безопасности.
8. Уровни защиты информации.
9. Что такое криптография и криптоанализ?
10. Шифр Цезаря и частотный анализ.
11. Шифр xor.
12. Симметричные и асимметричные криптосистемы.
13. Симметричные шифры. Примеры.
14. Симметричные шифры. Достоинства и недостатки.
15. Принцип ассиметричного шифрования.
16. Асимметричные шифры. Примеры.
17. Асимметричные шифры. Достоинства и недостатки.
18. Квантовая криптография.
19. Два основных алгоритма квантовой криптографии.
20. Что такое авторизация, аутентификация и идентификация? Что такое хэш и зачем он нужен?
21. Какие хеш-функции вы знаете?
22. Для чего используются хеш-функции?
23. Чем отличаются криптографические хеш-функции от некриптографических?
24. Что такое коллизия хеш-функции?
25. Что такое парадокс дней рождения и как он связан со взломом хешей?
26. Методы взлома хеш-функций.
27. Что такое «радужные таблицы»?
28. Какие виды паролей существуют?
29. Что такое динамические пароли?
30. Аппаратная и программная защита флешки.
31. Программы для защиты паролем папок, файлов и носителей информации.
32. Что такое «правильный пароль» и как его запомнить?
33. Методы взлома паролей.
34. Что такое «радужные таблицы»?
35. Системы аутентификации и идентификации. Классификация.
36. Используемый фактор аутентификации. Приоритет использования. Степень автоматизации.
37. Недостатки парольной аутентификации.
38. Аппаратная аутентификация, ее виды, достоинства и недостатки.
39. Биометрическая аутентификация.
40. Достоинства и недостатки аутентификации по отпечаткам пальцев.
41. Аутентификация по геометрии лица 2 вида.
42. Аутентификация по голосу.

43. Биометрические технологии будущего.
44. Распространенность методов биометрической аутентификации.
45. Что такое компьютерный вирус? Классификация вирусов.
46. Три этапа развития написания и распространения вирусов.
47. Классификация вирусов по среде обитания.
48. Пути проникновения вирусов.
49. Основные признаки появления вируса.
50. Загрузочные вирусы.
51. Файловые вирусы.
52. Макро-вирусы.
53. Скрипт-вирусы.
54. Классификация вирусов по операционным системам.

9. ОБРАЗЕЦ МОДУЛЬНОГО КОНТРОЛЯ

ГОУ ВПО «ДОНЕЦКИЙ НАЦИОНАЛЬНЫЙ УНИВЕРСИТЕТ»
Факультет иностранных языков

Специальность: 45.05.01 Перевод и переводоведение
Специализация: Специальный перевод (английский и немецкий языки)
Программа подготовки: ***специалитет***
Семестр 7
Учебная дисциплина Основы информационной безопасности в профессиональной деятельности

МОДУЛЬНАЯ КОНТРОЛЬНАЯ РАБОТА

ВАРИАНТ №1

1. Что такое информация? Свойства информации. Информационные технологии.
2. Что такое криптография и криптоанализ?
3. Чем отличаются криптографические хеш-функции от некриптографических?
4. Аппаратная аутентификация, ее виды, достоинства и недостатки.
5. Что такое компьютерный вирус? Классификация вирусов.

Утверждено на заседании кафедры радиофизики и инфокоммуникационных технологий, протокол № ___ от «__» _____ 20__ г.

Заведующий кафедрой В.В. Данилов
Преподаватель М.В, Фоменко

Критерии оценивания модульного контроля

Номер задания	***Количество баллов***
1	10
2	10
3	10
4	10
5	10
Всего	***50***

10. ОБРАЗЕЦ ЭКЗАМЕНАЦИОННОГО БИЛЕТА

Экзамен программой не предусмотрен

11. ОБРАЗЕЦ ТЕСТОВОГО ЗАДАНИЯ

Тестовые задания программой не предусмотрены

12. КРИТЕРИИ ОЦЕНИВАНИЯ

По курсу предполагается проведение промежуточной аттестации в виде модульного контроля и заслушивания самостоятельно подготовленного доклада на выбранную тему.

Текущий контроль успеваемости осуществляется на лекционных занятиях: в виде опроса теоретического материла.

Промежуточный контроль осуществляется проведением контрольной работы по отдельным разделам дисциплины, изученным студентом.

Формы и виды самостоятельной работы студентов при освоении дисциплины «Основы информационной безопасности в профессиональной деятельности»:

- чтение основной и дополнительной литературы;
- работа с библиотечным каталогом, самостоятельный подбор необходимой литературы;
- поиск необходимой информации в сети Интернет;
- конспектирование источников;
- подготовка к модульному контрольному занятию;
- подготовка докладов и презентаций.

Промежуточная аттестация является одним из основных механизмов оценки качества подготовки обучающихся и формой контроля их учебной работы. Предметом оценивания на промежуточной аттестации является уровень сформированности компетенций в рамках учебной дисциплины.

Распределение баллов, которые могут получить студенты в процессе изучения дисциплины

Организационно-учебная работа студента	**СРС**			**Всего**
	Индивидуальная работа	**Модульный контроль**	**Индивидуальная творческая работа**	
Max **10** баллов	max **20** баллов	max **50** баллов	max **20** баллов	**100** баллов
Экспресс-опрос на лекциях и активность на самостоятельных занятиях; проверка конспектов	Подготовка презентации и доклада на выбранную тему	Выполнение модульной контрольной работы	Защита подготовленного доклада и обсуждение затронутых проблем	

Шкала соответствия баллов государственной шкале

Оценка по шкале ECTS	Оценка по 100-балльной шкале	Оценка по государственной шкале (экзамен, дифференцированный зачет)	Оценка по государственной шкале (зачет)
A	90-100	5 (отлично)	зачтено
B	80-89	4 (хорошо)	зачтено
C	75-79	4 (хорошо)	зачтено
D	70-74	3 (удовлетворительно)	зачтено
E	60-69	3 (удовлетворительно)	зачтено
FX	35-59	2 (неудовлетворительно) с возможностью повторной сдачи	не зачтено
F	0-34	2 (неудовлетворительно) с возможностью повторной сдачи при условии обязательного набора дополнительных баллов	не зачтено

13. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ УЧЕБНОГО ПРОЦЕССА

Для проведения лекционных занятий, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации по дисциплине «Основы информационной безопасности в профессиональной деятельности», а также для самостоятельной работы обучающихся могут быть использованы следующие аудитории, имеющие необходимое материально-техническое обеспечение:

– учебная аудитория (ауд. № 1203: г. Донецк, пр. Гурова, 6), укомплектованная учебной мебелью на 53 посадочных места, комплектом рабочего места преподавателя, доской магнитно-маркерной – 1 шт., мультимедийным проектором – 1 шт., ноутбуком – 1 шт., принтером – 1 шт., телевизором – 1 шт.

Для самостоятельной работы обучающиеся могут также использовать следующие помещения ДОННУ:

–зал электронной информации (ауд. № 104-а: г. Донецк, пр. Гурова, 6) с комплектом учебной мебели на 40 посадочных мест, компьютером в комплекте (14 шт.).

14. РЕКОМЕНДОВАННАЯ ЛИТЕРАТУРА

№ п/п	Наименование	Кол-во экземпляров в библиотеке ДонНУ	Наличие электронной версии в ЭБС
	Основная литература		
1.	Теоретические основы компьютерной безопасности : Учеб. пособие для вузов по специальности "Компьютерная безопасность и др. / П. Н. Девянин, О. О. Михальский, Д. И. Правиков и др. – М. : Радио и связь, 2000. - 192 с	14	
2.	Корт, С. С. Теоретические основы защиты информации : Учеб. пособие для студентов вузов, обучающихся по группе спец. в обл. информ. безопасности / С. С. Корт. - М. : Гелиос АРВ, 2004. – 233 с.	13	
3.	Защита программного обеспечения / [Д. Гроувер, Р. Сатер, Дж. Фипс и др.] ; под ред. Д. Гроувера ; пер. с англ. В. Г. Потемкина и др. ; под ред. В. Г.	12	

	Потемкина. – Москва : Мир, 1992. - 286 с.		
4.	Завгородний, В. И. Комплексная защита информации в компьютерных системах : Учеб. пособие для студентов вузов / В. И. Завгородний. – М. : Логос, 2001. - 264 с.	11	
Дополнительная литература			
5.	Рассел, Ч. Microsoft Windows Server 2008 : справочник администратора / Ч. Рассел, Ш. Кроуфорд. – Москва : ЭКОМ Паблишерз, 2009. - 1321 с	14	
6.	Программно-аппаратные средства обеспечения информационной безопасности : Защита программ. и данных / П.Ю. Белкин, О.О. Михальский, А.С. Першаков и др. – М. : Радио и связь, 2000. - 169 с	4	
7.	Безопасность компьютерных сетей на основе Windows NT / В. С. Люцарев, К. В. Ермаков, Е. Б. Рудный, И. В. Ермаков. - М. : Рус. ред. ТОО Channel Trading, 1998. – 304 с. + Электр. оптич. диск (CD-ROM)	1	

15. ИНФОРМАЦИОННЫЕ РЕСУРСЫ

1. http://library.donnu.ru/ – сайт библиотеки ДонНУ;
2. http://elibrary.ru/ – научная электронная библиотека;
3. http://scholar.google.com/ – электронно-библиотечная поисковая система «Академия Google»;
4. http://window.edu.ru – Каталог образовательных Internet-ресурсов;

16. ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ

1. Windows 7 PRO (корпоративная лицензия ДОННУ № 46484614).
2. Microsoft Office (корпоративная лицензия ДОННУ № 46472919).
3. Microsoft Visual Studio (лицензия программы DreamSpark для высших учебных заведений).
4. Лицензии GPL, Apache, BSD для свободного программного обеспечения: Adobe Acrobat Reader, Антивирус Касперского.

17. ИСПОЛЬЗОВАНИЕ ЭЛЕКТРОННОГО ОБУЧЕНИЯ И ДИСТАНЦИОННЫХ ОБРАЗОВАТЕЛЬНЫХ ТЕХНОЛОГИЙ

При реализации программы дисциплины могут использоваться следующие виды электронного взаимодействия преподаватель-студент:

– размещение учебных и учебно-методических пособий в ЭБС для использования студентами при подготовке к занятиям;

– размещение учебных материалов в облачном хранилище для использования студентами при подготовке к занятиям;

рассылка по электронной почте материалов и заданий для выполнения, проверка выполненных заданий.

Рабочая программа рассмотрена и переутверждена на заседании кафедры радиофизики и инфокоммуникационных технологий с изменениями (без изменений) на 2021 год.

Протокол № ___ от «_____» _____ 20__ __ г.

Заведующий кафедрой РФ и ИКТ _____ В.В. Данилов

Рабочая программа рассмотрена и переутверждена на заседании кафедры радиофизики и инфокоммуникационных технологий с изменениями (без изменений) на 2022 год.

Протокол № ___ от «_____» _____ 20__ __ г.

Заведующий кафедрой РФ и ИКТ _____ В.В. Данилов