

Министерство науки и высшего образования
Российской Федерации

Федеральное государственное бюджетное
образовательное учреждение высшего образования
«Донецкий государственный университет»

Физико-технический факультет
Кафедра радиофизики



РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

**ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В
ПРОФЕССИОНАЛЬНОЙ ДЕЯТЕЛЬНОСТИ**

Укрупненная группа направлений подготовки	45.00.00 Языкознание и литературоведение
Программа высшего образования	Программа специалитета
Специальность	45.05.01 Перевод и переводоведение
Специализация	Специальный перевод (английский и немецкий языки)
Квалификация	Лингвист-переводчик
Форма обучения	Очная

Рабочая программа адаптирована для лиц
с ограниченными возможностями здоровья и инвалидов

Донецк 2024

Рабочая программа дисциплины **«Основы информационной безопасности в профессиональной деятельности»** для обучающихся по специальности 45.05.01 Перевод и переводоведение, специализации «Специальный перевод (английский и немецкий языки)», составлена на основании Федерального государственного образовательного стандарта высшего образования – магистратура по направлению подготовки 45.05.01 Перевод и переводоведение, утвержденного приказом Министерства образования и науки Российской Федерации от 12 августа 2020 г. № 989 (с изм. и доп.), Порядка организации и осуществления образовательной деятельности по образовательным программам высшего образования – программам бакалавриата, программам специалитета, программам магистратуры, утвержденного приказом Министерства науки и высшего образования Российской Федерации от 06 апреля 2021 г. № 245 (с изм. и доп.), в соответствии с учебным планом, утвержденным Ученым советом ФГБОУ ВО «ДонГУ» для набора 2024 года.

Разработчик:

К.т.н., доцент кафедры РФ и ИКТ



М.В.Бабичева

Рабочая программа утверждена на заседании радиофизики и инфокоммуникационных технологий.

Протокол от 26.03.2024 г. № 16

Заведующий кафедрой



В.В.Данилов

СОГЛАСОВАНО:

И. о. декана факультета иностранных
языков
28.03.2024 г.



Е. И. Петрищева

Учебно-методическая комиссия факультета иностранных языков

Протокол от 27.03.2024 г. № 4.

Председатель



О. Л. Бессонова

Руководитель основной профессиональной
образовательной программы,
д-р филол. наук, доц.
26.03.2024 г.



В. А. Дроздов

1. МЕСТО ДИСЦИПЛИНЫ / ПРАКТИКИ / КУРСОВОЙ РАБОТЫ / ГОСУДАРСТВЕННОЙ ИТОГОВОЙ АТТЕСТАЦИИ В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

1.1. Требования к предварительной подготовке обучающихся, предшествующие и сопутствующие дисциплины, на которых основывается изучение данной:
Для изучения данной учебной дисциплины необходимы знания и умения, формируемые в процессе изучения программы общеобразовательной школы и курсов, связанных с информационными технологиями.

1.2. Знания и умения, полученные в ходе изучения дисциплины «Основы информационной безопасности в профессиональной деятельности» обеспечивает формирование у студентов современных навыков профессиональной и безопасной работы с информационными системами и документами.

2. ОПИСАНИЕ ДИСЦИПЛИНЫ / ПРАКТИКИ / КУРСОВОЙ РАБОТЫ / ГОСУДАРСТВЕННОЙ ИТОГОВОЙ АТТЕСТАЦИИ

2.1. Общая характеристика

Наименование показателя	Значение показателя
Название образовательной программы	45.05.01 Перевод и переводоведение
Шифр и название в соответствии с учебным планом	Б1.Б.М3 Основы информационной безопасности в профессиональной деятельности
Часть образовательной программы	Базовая часть Модуль профессионально-ориентированных дисциплин
Количество зачетных единиц / всего часов	2/ 72

2.2. Распределение часов по периодам обучения

Форма обучения	курс	семестр	Общее количество часов					Форма контроля
			лекционных	лабораторных	практических	самостоятельной работы	всего	
Очная	3	5	34	—	-	38	72	зачет

3. ЦЕЛИ ДИСЦИПЛИНЫ

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 конфиденциальности, целостности и доступности информации; причинами, видами, каналами утечки и искажения информации.

**4. КОМПЕТЕНЦИИ ОБУЧАЮЩЕГОСЯ, ФОРМИРУЕМЫЕ В РЕЗУЛЬТАТЕ
ОСВОЕНИЯ КОМПОНЕНТА ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ, ИХ ИНДИКАТОРЫ
И ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОБУЧЕНИЯ**

Компетенции	Индикаторы	Результаты обучения
УК-8. Способен создавать и поддерживать в повседневной жизни и в профессиональной деятельности безопасные условия жизнедеятельности для сохранения природной среды, обеспечения устойчивого развития общества, в том числе при угрозе и возникновении чрезвычайных ситуаций и военных конфликтов.	УК-8.1 Способен создавать и поддерживать в повседневной жизни и в профессиональной деятельности безопасные условия жизнедеятельности для среды, обеспечения устойчивого развития общества	Знает основы безопасности жизнедеятельности
		Умеет, создавать безопасные условия реализации профессиональной деятельности.
		Имеет практический опыт поддержания безопасных условий жизнедеятельности.
ОПК-4 Способен работать с электронными словарями, различными источниками информации, осуществлять поиск, хранение, обработку и анализ информации, представлять ее в требуемом формате с использованием информационных, компьютерных и сетевых технологий.	ОПК-4.1. Владеет навыками оперативного получения, обработки и управления информацией с учетом применения компьютерных технологий.	Умеет оказать первую помощь в чрезвычайных ситуациях, создавать безопасные условия реализации профессиональной деятельности.
		Имеет практический опыт поддержания безопасных условий жизнедеятельности.
		Умеет выбирать оптимальные способы работы с учетом применения компьютерных технологий.

5. ПРОГРАММА ДИСЦИПЛИНЫ

Название темы	Краткое содержание темы (вопросы темы)
1. Основные понятия и составляющие информационной безопасности	1. Основные понятия информационной безопасности. 2. Правовые основы ИБ и законодательство ДНР об информации. 3. Информация, информационная система, владелец информации. 4. Виды информации. 5. Конфиденциальная информация, государственная тайна. 6. Нормативные документы РФ по ИБ. 7. Конфиденциальность, целостность, доступность.
2. Структура файлов и hex-редактор.	1. Понятие файла. Hex-редактор, структура и предназначение. 2. Форматы файлов. Структура некоторых текстовых и графических файлов. 3. Сигнатуры файлов.

	4. Определение формата файла в различных ОС.
3. Криптография и криптоанализ	<ol style="list-style-type: none"> 1. Историческая справка, примитивные шифры. 2. Шифр хог, Цезаря, Винежера. 3. Симметричные и ассиметричные методы. 4. Суть ассиметричного шифрования. 5. Алгоритм RSA и Эль-Гамала. 6. Симметричное шифрование. 7. Гаммирование. Квантовая криптография.
4. Хеш-функции	<ol style="list-style-type: none"> 1. Понятие хеш-функции. 2. Криптографические и не криптографические хеш-функции. 3. Свойства хеш-функции. CRC –суммы. 4. Хеш-функции MD5 и SHA1. 5. Коллизии хеш-функций. 6. Криптоанализ хеш-функций.
5. Аутентификация по паролю	<ol style="list-style-type: none"> 1. Авторизация, аутентификация и идентификация. 2. Системы аутентификации. Парольная защита. 3. Уязвимости парольной защиты. 4. Методы хранения пароля. 5. Определение криптостойкости пароля. 6. Формула Шеннона. Метода взлома пароля. 7. Программы для взлома пароля. 7. Организация безопасной парольной защиты.
6. Другие методы аутентификации	<ol style="list-style-type: none"> 1. Электронные методы аутентификации. 2. Аппаратная аутентификация. 3. Биометрические методы аутентификации. 4. Аутентификация по отпечатку пальца, аутентификация по лицу. 5. Распространенность методов аутентификации. 6. Уязвимости биометрической аутентификации. 8. Федеральная аутентификация.
7. Вирусы	<ol style="list-style-type: none"> 1. История создания вирусов. 2. Классификация вирусов. 3. Загрузочные, файловые, макросы, скрипт-вирусы. 4. Вирусы для Linux, Android, iOSm 5. Трояны, черви, собственно вирусы. 9. Хакеры.
8. Антивирусы	<ol style="list-style-type: none"> 1. Принцип работы антивирусных программ. 2. Сигнатуры вирусов. 3. Возможности антивирусного ПО. 4. Написание антивирусной программы. 5. Платные и бесплатные антивирусы. 6. Международные рейтинги антивирусных программ. 7. Обзор наиболее популярных антивирусных программ.
9. Web- безопасность.	<ol style="list-style-type: none"> 1. Основные понятия web. HTML, CSS и JS. 2. Цели злоумышленников, атакующих сайты. 3. Куки и их роль в безопасности сайтов. 4. Атаки на сайты. XSS, CSRF, SQL-инъекции и методы защиты от них. 5. Программы для анализа сайтов на уязвимости. 6. Уязвимости методов аутентификации. 7. Уязвимости прикладного уровня.

10. Защита информации в компьютерных сетях.	<ol style="list-style-type: none"> 1. Уязвимости компьютерных сетей. 2. Основные виды атак при передаче информации. 3. Снифферы. Ответвления трафика. 4. Анализ электромагнитных излучений. 5. Атаки на канальном и сетевом уровне. 6. Спуфинг. Виды сканирования. 7. DOS и DDOS атаки. 8. Подмена IP адреса. 9. Меры противодействия атакам.
11. Техническая защита информации	<ol style="list-style-type: none"> 1. Классификация каналов технической разведки. 2. Краткая характеристика каждого канала. 3. Возможности различных видов технической разведки. Историческая справка. 4. Параметрический канал утечки, исторические примеры. 5. Демаскирующие признаки объектов наблюдения и сигналов. 6. Опасные сигналы и их источники.
12. Защита документов	<ol style="list-style-type: none"> 1. Методы подделки документов. 2. Методы подделки цифровых документов. 3. Методы определения подлинности документов. 4. Получение дополнительной информации из EXIF. 5. Методы ELA и PCA и их ограничения. 6. Методы защиты документов.
13. Электронно-цифровая подпись	<ol style="list-style-type: none"> 1. Понятие электронно-цифровой подписи. 2. История развития ЭЦП. 3. Основные схемы ЭЦП. 4. Построение ЭЦП. Протокол подписания документа. 5. Центры сертификации. 6. Удостоверяющие центры. 7. Криптостойкость схем ЭЦП.
14. Методы стеганографии	<ol style="list-style-type: none"> 1. Стеганография, как средство защиты файлов. 2. Цифровые водяные знаки. 3. Слияние файлов, LSB. 4. Соккрытие информации в аудио и видео файлах. 5. Методы обнаружения скрытых сообщений.
15. Методы социальной инженерии.	<ol style="list-style-type: none"> 1. История развития социальной инженерии. 2. Человек, как самое уязвимое звено любой системы. 3. Психологические основы социальной инженерии. 4. Методы социальной инженерии..
16. Заключительное занятие.	Обобщение пройденного материала
17. Доклады студентов	Доклады студентов.

6. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

6.1. Форма обучения – очная, курс – 3, семестр – 5

Наименования разделов и тем	Количество часов				
	Лекц.	Лабор	Практ.	СРС+К	Всего
		.			

Основные понятия и составляющие информационной безопасности	2			3	5
Структура файлов и hex-редактор.	2			3	5
Криптография и криптоанализ	2			3	5
Хеш-функции	2			3	5
Аутентификация по паролю	2			3	5
Другие методы аутентификации	2			3	5
Вирусы	2			2	4
Антивирусы	2			2	4
Web- безопасность.	2			2	4
Защита информации в компьютерных сетях.	2			2	4
Техническая защита информации	2			2	4
Защита документов	2			2	4
Электронно-цифровая подпись	2			2	4
Методы стеганографии.	2			2	4
Методы социальной инженерии.	2			2	4
Заключительное занятие.	2			2	4
Доклады студентов	2				
ИТОГО ЗА СЕМЕСТР / ЗА КУРС / ПО КОМПОНЕНТУ ОПОП	34			35,8+2,2	72
ИТОГО ПО КОМПОНЕНТУ ОПОП	34			38	72

7. ОЦЕНОЧНЫЕ МАТЕРИАЛЫ (СРЕДСТВА) ДЛЯ ТЕКУЩЕГО КОНТРОЛЯ УСПЕВАЕМОСТИ, ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ

7.1. Контрольные вопросы

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 хог.
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.

7.2. Примерные темы индивидуальных заданий (доклад с презентацией)

1. История криптографии.
2. Современная криптография
3. Квантовая криптография
4. Атаки на сайты.
4. XSS -атаки.
5. SQL-атаки.
6. Методы взлома wi-fi.
7. Современная стеганография.
8. Поисковик Shodan.
9. Форензика.
10. Стеганография.
11. Google Hacking
12. DOS и DDOS атаки.
13. Honey Pots.
14. Аутентификация на сайтах.
15. Куки.
16. Хакеры. Субкультура хакеров.
17. Боты. Угрозы, исходящие от ботов.
18. Системы аутентификации.
19. Электронно-цифровая подпись.
20. Фишинговые сайты.
21. Вирусные атаки.
22. Прослушивающие устройства.
23. Скремблеры.
24. Направленные микрофоны.
25. Спуфинг.
26. Эвристический анализ для антивирусов.
27. Сниферы.

28. Охранные системы.
29. Видеонаблюдение.
30. Безопасность интернета вещей.
31. Методы криптоанализа.
32. Кейлоггеры.
33. Методы социальной инженерии.
34. Антивирусные программы. Есть ли смысл?
35. Взлом мобильных телефонов.
36. Применение нейронных сетей в информационной безопасности.

В случае ведения учебного процесса с использованием электронного обучения и дистанционных образовательных технологий, содержание билета может отличаться от приведенного.

8. РАСПРЕДЕЛЕНИЕ БАЛЛОВ, КОТОРЫЕ ПОЛУЧАЮТ ОБУЧАЮЩИЕСЯ

Общая оценка знаний обучающихся по дисциплине проводится по 100-балльной шкале исходя из максимума, приведенного в таблице ниже. Организационно-учебная работа в аудитории оценивается на основе таких критериев как посещаемость занятий, своевременное и качественное выполнение индивидуального задания, активность во время проведения лекционных и практических занятий (участие в обсуждении текущего и пройденного материала, решение задач и т.п.).

Номера разделов	Виды работ	Максимальное количество баллов
тема 1-17	Текущий контроль	20
	Индивидуальное задание	30
ИТОГО		50
Зачет		50
Общий итог за семестр		100

Соответствие баллов оценке

Количество баллов из 100	ECTS	Оценка по пятибалльной шкале	
		Экзамен, дифференцированный зачет	Зачет
90-100	A	отлично	зачтено
80-89	B	хорошо	зачтено
75-79	C		зачтено
70-74	D	удовлетворительно	зачтено
60-69	E		зачтено
35-59	FX	неудовлетворительно	не зачтено
0-34	F		не зачтено

9. ОБЕСПЕЧЕНИЕ ОБРАЗОВАТЕЛЬНОГО ПРОЦЕССА ДЛЯ ЛИЦ С ОГРАНИЧЕННЫМИ ВОЗМОЖНОСТЯМИ ЗДОРОВЬЯ И ИНВАЛИДОВ

В ходе реализации дисциплины используются следующие дополнительные методы обучения, текущего контроля успеваемости и промежуточной аттестации обучающихся в зависимости от их индивидуальных особенностей:

- 1) для слепых и слабовидящих:
 - лекции оформляются в виде электронного документа, доступного с помощью компьютера со специализированным программным обеспечением;
 - для выполнения задания при необходимости предоставляется увеличивающее устройство; возможно также использование собственных увеличивающих устройств;
 - письменные задания оформляются увеличенным шрифтом.
- 2) для глухих и слабослышащих:
 - лекции оформляются в виде электронного документа;
 - письменные задания выполняются на компьютере в письменной форме;
 - экзамен проводится в письменной форме на компьютере; возможно проведение в форме тестирования.
- 3) для лиц с нарушениями опорно-двигательного аппарата:
 - лекции оформляются в виде электронного документа, доступного с помощью компьютера со специализированным программным обеспечением;
 - письменные задания выполняются на компьютере;
 - экзамен и зачёт проводятся в устной форме или выполняются в письменной форме на компьютере.

При необходимости предусматривается увеличение времени для подготовки ответа.

Процедура проведения промежуточной аттестации для обучающихся устанавливается с учётом их индивидуальных психофизических особенностей. Промежуточная аттестация может проводиться в несколько этапов.

Проведение процедуры оценивания результатов обучения допускается с использованием дистанционных образовательных технологий.

Обеспечивается доступ к информационным и библиографическим ресурсам в сети Интернет для каждого обучающегося в формах, адаптированных к ограничениям их здоровья и восприятия информации:

- 1) для слепых и слабовидящих:
 - в печатной форме увеличенным шрифтом;
 - в форме электронного документа;
- 2) для глухих и слабослышащих:
 - в печатной форме;
 - в форме электронного документа.
- 3) для обучающихся с нарушениями опорно-двигательного аппарата:
 - в печатной форме;
 - в форме электронного документа.

10. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ УЧЕБНОГО ПРОЦЕССА

Учебные занятия проводятся в Главном корпусе ДонГУ (г. Донецк, пр. Гурова, 6). Для проведения лабораторных занятий требуется аудитория, оборудованная меловой или маркерной доской, мультимедийный проектор и экран, ноутбук, комплект учебной мебели для студентов, рабочее место преподавателя, выход в Интернет – проводной или с использованием Wi-Fi.

Для самостоятельной работы используются текстовые и электронные ресурсы Научной библиотеки университета и других электронных библиотечных баз данных, учебно-методическое обеспечение, представленное в учебно-методическом кабинете Главного корпуса (ауд.405).

Обучающиеся имеют возможность использовать учебные материалы по дисциплине, размещенные на платформе Moodle Центра дистанционного образования ФГБОУ ВО «ДонГУ». При изучении дисциплины применяются электронное обучение и дистанционные образовательные технологии.

С использованием ресурсов платформы дистанционного образования осуществляется текущий контроль знаний обучающихся на основе тестирования и проверки результатов самостоятельной работы.

11. РЕКОМЕНДУЕМАЯ ЛИТЕРАТУРА

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.
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.
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. 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.

Дополнительная литература

5. Рассел, Ч. Microsoft Windows Server 2008 : справочник администратора / Ч. Рассел, Ш. Кроуфорд. – Москва : ЭКОМ Паблишерз, 2009. - 1321 с
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
7. Безопасность компьютерных сетей на основе Windows NT / В. С. Люцарев, К. В. Ермаков, Е. Б. Рудный, И. В. Ермаков. - М.: Рус. ред. TOO Channel Trading, 1998. – 304 с. + Электр. оптич. диск (CD-ROM)

ИНФОРМАЦИОННЫЕ РЕСУРСЫ

1. Интернет-Основы информационной безопасности . – URL: <http://www.intergu.ru/> – Режим доступа: свободный. – Текст : электронный
2. Классификация механизмов аутентификации пользователей и их обзор . – URL: <https://habr.com/ru/post/177551/>– Режим доступа: свободный. – Текст : электронный
3. SQL инъекции. Проверка, взлом, защита . – URL: <https://habr.com/ru/post/130826/>– Режим доступа: свободный. – Текст : электронный
4. XSS глазами злоумышленника. – URL: <https://habr.com/ru/post/66057/>
5. Stealthphone: Защита микрофона мобильного телефона от несанкционированного включения . – URL: <https://habr.com/ru/company/ancort/blog/160215/>– Режим доступа: свободный. – Текст : электронный
6. Основные параметры передатчиков и приемников . – URL: <https://radiokot.ru/start/analog/bugs/02/>– Режим доступа: свободный. – Текст : электронный
7. Научная электронная библиотека elibrary.ru : информ.-аналит. портал / ООО Научная электронная библиотека. – Москва : ООО Науч. электрон. б-ка, сор. 2000–2022. – URL: <https://elibrary.ru> (дата обращения: 01.01.2023). – Режим доступа: для зарегистрир. пользователей. – Текст : электронный.

8. Электронный каталог Научной библиотеки Донецкого государственного университета. – Донецк : НБ ДонГУ, 1999– . – URL: <http://catalog.donnu.education> (дата обращения: 01.01.2023). – Текст : электронный;

9. Техническая библиотека URL: <http://techlibrary.ru/> (дата обращения: 31.03.2023). – Режим доступа: свободный. – Текст : электронный;

10. Научные журналы ФГБОУ ВО «ДонГУ» URL: <http://donnu.ru/science/journals> (дата обращения: 31.03.2023). – Режим доступа: свободный. – Текст : электронный.

ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ

1. Windows 7 PRO (корпоративная лицензия ДонГУ № 46484614)
2. Microsoft Office (корпоративная лицензия ДонГУ № 46472919)
3. Microsoft Visual Studio (лицензия программы Dream Spark для высших учебных заведений)
4. Антивирус Касперского, Adobe Acrobat Reader, xPDF (лицензии GPL, Apache, BSD для свободного программного обеспечения).
5. Kali Linux (свободно распространяемое ПО).
6. Wireshark (свободно распространяемое ПО).
7. NEO hex-редактор (свободно распространяемое ПО).