ГОСУДАРСТВЕННОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ПРОФЕССИОНАЛЬНОГО ОБРАЗОВАНИЯ «ДОНЕЦКИЙ НАЦИОНАЛЬНЫЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ»

УТВЕРЖДАЮ:
Проректор по научно-педагогической работе
_____ А.Б. Бирюков
(подпись)
«26» мая 20 20 года

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ
Б1.В4 Информационная безопасность в АСУ

Направление подготовки: 09.04.01 Информатика и вычислительная техника
(код и наименование направления / специальности)

Магистерская программа: Автоматизированные системы управления (АСУ)
(наименование профиля / магистерской программы / специализации)

Программа: Магистратура
(бакалавриат, магистратура, специалитет)

Форма обучения: Очная, заочная
(очная, заочная, очно-заочная)

Форма обучения:	Очная	Заочная
Семестр(ы)	2	2
Общая трудоёмкость в з.е./часах	4 / 144	4 / 144
Контактная работа (час.), в том числе:	72	18
лекции (час.)	34	6
лабораторные работы (час.)	34	6
практические (семинарские) занятия (час.)	-	-
Самостоятельная работа (час.), в том числе	40	96
курсовой проект (работа) (семестр/час.)	-	-
индивидуальное задание (кол./час.)	-	1/9
Контроль (экзамен, час./зачёт)	экзамен/36	экзамен/36

Донецк, 2020 г.

Рабочая программа дисциплины «Информационная безопасность в АСУ» составлена в соответствии с учебными планами по направлению подготовки 09.04.01 Информатика и вычислительная техника (магистерская программа - Автоматизированные системы управления) для 2020 года приёма по очной и заочной формам обучения.

Составители:

старший преподаватель кафедры
«Автоматизированные системы управления» _____ Теплова О. В.,
к.тех.н, доцент, зав. кафедры
«Автоматизированные системы управления» _____ Секирин А.И.

Рабочая программа **рассмотрена и принята** на заседании кафедры *«Автоматизированные системы управления».*

Протокол от 28 апреля 2020 года № 11

Заведующий кафедрой _____ Секирин А.И.
(подпись) (Ф.И.О.)

Рабочая программа **одобрена учебно-методической комиссией** ГОУВПО «ДОННТУ» по направлению подготовки 09.04.01 Информатика и вычислительная техника

Протокол от 21 мая 2020 года № 6

Председатель _____ А.Я. Аноприенко
(подпись) (Ф.И.О.)

Рабочая программа **продлена** для 20___ года приёма на заседании кафедры *«Автоматизированные системы управления».*

Протокол от «_____» _____20___ года № _____
Заведующий кафедрой _____ _____
(подпись) (Ф.И.О.)

Рабочая программа **продлена** для 20___ года приёма на заседании кафедры *«Автоматизированные системы управления».*

Протокол от «_____» _____20___ года № _____
Заведующий кафедрой _____ _____
(подпись) (Ф.И.О.)

Рабочая программа **продлена** для 20___ года приёма на заседании кафедры *«Автоматизированные системы управления».*

Протокол от «_____» _____20___ года № _____
Заведующий кафедрой _____ _____
(подпись) (Ф.И.О.)

1. ОБЪЕКТ, ЦЕЛЬ И ЗАДАЧИ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Дисциплина рассматривает принципы и технологии проектирования подсистем защиты информации в компьютерных системах и сетях; принципы построения политики безопасности предприятия.

Целью дисциплины является овладение методами и подходами обеспечения информационной безопасности в АСУ предприятия с использованием современных технологий и методов защиты информации.

В результате освоения дисциплины студент должен:

знать:

– процедуры критического анализа, методики анализа результатов исследования и разработки стратегий проведения исследований, организации процесса принятия решения;

– основные угрозы безопасности информации и модели нарушителя, основные меры по защите информации в автоматизированных системах, основные криптографические методы, алгоритмы, протоколы, используемые для защиты информации в автоматизированных системах, организационные меры по защите информации, средства и способы обеспечения безопасности информации, принципы построения систем защиты информации, особенности защиты информации в автоматизированных системах.

уметь:

– принимать конкретные решения для повышения эффективности процедур анализа проблем, принятия решений и разработки стратегий;

– анализировать программные, архитектурно-технические и схемотехнические решения компонентов автоматизированных систем с целью выявления потенциальных уязвимостей безопасности информации, выбирать меры защиты информации, определять структуру системы защиты информации автоматизированной системы, разрабатывать технические задания на создание подсистем безопасности информации автоматизированных систем.

владеть:

– методами установления причинно-следственных связей и определения наиболее значимых среди них; методиками постановки цели и определения способов ее достижения; методиками разработки стратегий действий при проблемных ситуациях;

– навыками проведения анализа структурных и функциональных схем защищенных автоматизированных систем с целью выявления потенциальных информационных уязвимостей автоматизированных систем, выявления основных угроз безопасности информации в автоматизированных системах; методами разработки модели угроз безопасности информации и модели нарушителя, моделей АС и подсистем безопасности АС, навыками разработки предложений по совершенствованию системой управления безопасностью информации.

Перечисленные результаты обучения являются основой для формирования следующих компетенций: **ПК-4, УК-1:**

– способен осуществлять критический анализ проблемных ситуаций на

основе системного подхода, вырабатывать стратегию действий **(УК-1)**;

– способен разрабатывать системы защиты информации автоматизированных систем **(ПК-4).**

2. МЕСТО ДИСЦИПЛИНЫ В ОСНОВНОЙ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЕ

Дисциплина относится к части, формируемой участниками образовательных отношений, Блока 1 «Дисциплины (модули)» учебного плана.

Базируется на знаниях и умениях, которые студент приобрел при освоении предшествующих дисциплин программы бакалавриата.

Знания и умения, приобретенные при освоении данной дисциплины, реализуются студентом при прохождении преддипломной практики, прохождении государственной итоговой аттестации.

3. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

3.1 Распределение учебных часов по темам дисциплины и видам занятий

Наименование тем (содержательных модулей)	Количество часов (очная/заочная форма)				
	Всего	В том числе			
		Лекции	Практ. (Семин.)	Лабор.	СР
Тема 1. Основы информационной безопасности.	4/4	2/1			2/3
Тема 2. Анализ угроз информационной безопасности	4/4	2/1			2/3
Тема 3. Системы защиты информации	18/18	6/1		4/2	8/15
Тема 4. Обеспечение безопасности операционных систем.	28/28	6/1		14/2	8/25
Тема 5. Многоуровневая защита корпоративных сетей.	42/33	14/1		16/2	12/30
Тема 6. Облачные вычисления и их безопасность.	12/12	4/1			8/11
Индивидуальное задание	0/9				0/9
Итого по видам занятий		34/6		34/6	40/96
Контроль	36/36				
Итого:	144/144				

Формирование компетенций в результате освоения тем дисциплины

Компетенции	Темы дисциплины, нацеленные на выработку компетенции
УК-1	Тема 2,3,5,6
ПК-4	Тема 1,2,3,4,5

3.2. Лекции

Тема 1. Основы информационной безопасности.

Содержание темы 1:

Лекция 1: Основные понятия информационной безопасности. Регламентирующие документы в области информационной безопасности.

Литература к теме 1: [1,3]

Тема 2. Анализ угроз информационной безопасности.

Содержание темы 2:

Лекция 2: Классификация угроз информационным системам. Тенденции развития ИТ-угроз в современном мире.

Литература к теме 2: [1,3]

Тема 3. Системы защиты информации.

Содержание темы 3:

*Лекция 3:*Классификация систем защиты информации по различным критериям.

Лекция 4: Особенности обеспечения информационной безопасности в распределенных информационных системах и центрах обработки информации, анализ угроз корпоративных сетей.

Лекция 5: Допустимые и целесообразные средства защиты информации для систем различных категорий.

Литература к теме 3: [1,2,3]

Тема 4. Обеспечение безопасности операционных систем.

Содержание темы 3:

Лекция 6: Проблемы обеспечения безопасности операционных систем. Угрозы безопасности операционных систем.

Лекция 7: Понятие защищенной ОС. Архитектура подсистемы защиты операционной системы. Основные функции подсистемы защиты ОС.

Лекция 8: Идентификация, аутентификация и авторизация субъектов доступа. Разграничение доступа к объектам ОС. Аудит.

Литература к теме 4: [2,3,5]

Тема 5. Многоуровневая защита корпоративных информационных систем

Содержание темы 5:

Лекция 9: Принципы построения многоуровневой защиты корпоративной информации.

Лекция 10: Корпоративная информационная система (КИС) с традиционной структурой.

Лекция 11: Многоуровневый подход к обеспечению информационной безопасности корпоративных информационных систем.

Лекция 12: Подсистемы информационной безопасности традиционных корпоративных информационных систем.

Лекция 13: Управление средствами обеспечения информационной безопасности, задачи управления информационной безопасностью.

Лекция 14: Разновидности архитектуры управления безопасностью корпоративных информационных систем.

Лекция 15: Функционирование системы управления информационной безопасностью корпоративных информационных систем, аудит и мониторинг безопасности корпоративных информационных систем.

Литература к теме 5: [2,3,4,5]

Тема 6. Облачные вычисления и их безопасность.

Содержание темы 6:

Лекция 16: Системы «облачных» вычислений. Основные проблемы безопасности облачных вычислений.

Лекция 17: Безопасность облачных вычислений. Средства защиты в виртуальных средах. Выбор провайдера облачных услуг.

Литература к теме 4: [4,5]

3.3. Лабораторные работы

№ п/п	Тема работы	Объем, час.	Литература
1	Реализация дискреционной модели политики безопасности.	4	[1,2,6,8]
2	Количественная оценка стойкости парольной защиты.	2	[2,3,6,8]
3	Защита программ и данных. Привязка к аппаратному обеспечению. Использование реестра.	4	[4,5,6,8]
4	Средства и методы ограничения доступа к файлам.	4	[3,4,6,8]
5	Восстановление данных.	4	[1,3,6,8]
6	Нагрузочное тестирование web-сервера.	4	[2,4,6,8]
7	Особенности организации DDoS и защита от них.	4	[2,3,6,8]
8	Борьба со спамом.	4	[1,2,6,8]
9	Управление информационной безопасностью и событиями безопасности.	4	[1,5,6,8]
Итого		34	

3.4. Самостоятельная работа студента

№ п/п	Виды самостоятельной работы студента	Объем, час. очн/заочн
1	Изучение лекционного материала	22/75
2	Подготовка к практическим занятиям	-
3	Подготовка к лабораторным работам	18/12
4	Выполнение курсового проекта	-
5	Выполнение курсовой работы	-
6	Выполнение индивидуального задания	0 / 9
ИТОГО:		40/96

3.6. Курсовой проект (работа), индивидуальное задание

Курсовой проект (работа) по дисциплине учебным планом не предусмотрен.

Для студентов заочной формы обучения во 2-м семестре предусмотрено выполнение контрольной работы по форме **индивидуального задания**.

Тематика работы связана с многоуровневой защитой корпоративных сетей.

Выполняется в соответствии с [7].

В результате выполнения работы студент должен:

– знать средства и способы обеспечения безопасности информации, принципы построения систем защиты информации;

– уметь выбирать меры защиты информации, определять структуру системы защиты информации;

– владеть навыками проведения анализа структурных и функциональных схем защищенных автоматизированных систем, навыками проектирования и моделирования сетей в автоматизированных средах.

Объем учебной нагрузки при выполнении контрольной работы – 9 часов.

Рекомендуемый объем пояснительной записки по контрольной работе – не более 12 страниц формата А4 (210×297 мм).

4 Фонд оценочных средств

4.1 Критерии и шкалы для интегрированной оценки уровня сформированности компетенций

Составляющая компетенции – полнота знаний:

- нулевой уровень: неверные, не аргументированные, с множеством грубых ошибок ответы на вопросы / ответы на два вопроса из трех полностью отсутствуют. Уровень знаний ниже минимальных требований;
- минимальный уровень: даны не полные, не точные и неаргументированные ответы на вопросы. Уровень знаний ниже минимальных требований. Допущено много грубых ошибок;
- пороговый уровень: даны недостаточно полные, точные и аргументированные ответы на вопросы. Плохо знает термины, определения и понятия; основные закономерности, соотношения, принципы. Допущено много негрубых ошибок;
- средний уровень: даны достаточно полные, точные и аргументированные ответы на вопросы. В целом знает термины, определения и понятия; основные закономерности, соотношения, принципы. Допущено несколько негрубых ошибок;
- продвинутый уровень: даны полные, точные и аргументированные ответы на вопросы. Знает термины, определения и понятия; основные закономерности, соотношения, принципы. Допущено несколько негрубых ошибок;
- высокий уровень: даны полные, точные и аргументированные ответы на вопросы. Знает термины, определения и понятия; основные закономерности, соотношения, принципы. Допущено несколько неточностей.

Составляющая компетенции – умения:

- нулевой уровень: полное отсутствие понимания сути методики решения задачи, допущено множество грубейших ошибок / задания не выполнены вообще;
- минимальный уровень: слабое понимание сути методики решения задачи, допущены грубые ошибки. Решения не обоснованы. Не умеет использовать нормативно-техническую литературу. Не ориентируется в специальной научной литературе, нормативно-правовых актах;
- пороговый уровень: достаточное понимание сути методики решения задачи, допущены ошибки. Решения не всегда обоснованы. Умеет использовать нормативно-техническую литературу. Слабо ориентируется в специальной научной литературе, нормативно-правовых актах;
- средний уровень: в целом понимает суть методики решения задачи, допущены ошибки. Решения не всегда обоснованы. Умеет использовать нормативно-техническую и специальную научную литературу, нормативно-правовые акты;
- продвинутый уровень: в целом понимает суть методики решения задачи, но допущены неточности. Способен обосновать принятое решение. Умеет использовать нормативно-техническую и специальную научную литературу, нормативно-правовые акты;

- высокий уровень: понимает суть методики решения задачи. Способен обосновать принятое решение. Умеет использовать нормативно-техническую и специальную научную литературу, передовой зарубежный опыт, нормативно-правовые акты.

Составляющая компетенции – владение навыками:

- нулевой уровень: не продемонстрировал навыки выполнения профессиональных задач. Испытывает существенные трудности при выполнении отдельных заданий;
- минимальный уровень: не продемонстрировал навыки выполнения профессиональных задач. Испытывает существенные трудности при выполнении отдельных заданий;
- пороговый уровень: владеет опытом готовности к профессиональной деятельности и профессиональному самосовершенствованию на пороговом уровне. Трудовые действия выполняет медленно и некачественно;
- средний уровень: владеет средним опытом готовности к профессиональной деятельности и профессиональному самосовершенствованию. Трудовые действия выполняет на среднем уровне по быстроте и качеству;
- продвинутый уровень: владеет опытом и достаточно выраженной личностной готовности к профессиональной деятельности и профессиональному самосовершенствованию. Быстро и качественно выполняет трудовые действия;
- высокий уровень: владеет опытом и выраженностью личностной готовности к профессиональной деятельности и профессиональному самосовершенствованию. Быстро и качественно выполняет трудовые действия.

Обобщенная оценка сформированности компетенций:

- нулевой уровень: компетенции не сформированы;
- минимальный уровень: значительное количество компетенций не сформировано;
- пороговый уровень: все компетенции сформированы, но большинство на пороговом уровне;
- средний уровень: все компетенции сформированы на среднем уровне;
- продвинутый уровень: все компетенции сформированы на среднем или высоком уровне;
- высокий уровень: все компетенции сформированы на высоком уровне.

4.2 Вопросы к экзамену

1. Основные понятия и определения информационной безопасности.
2. Виды и источники угроз безопасности информации.
3. Классификация угроз информационной безопасности.
4. Регламентирующие документы Российской Федерации в области информационной безопасности.
5. Критерии оценки безопасности КС. «Оранжевая книга».
6. Механизмы и сервисы безопасности.
7. Формирование политики безопасности организации.
8. Основные принципы формирования пользовательских паролей.
9. Идентификация пользователей (назначение и способы реализации).
10. Аутентификация пользователей (назначение и способы реализации).

11. Авторизации пользователей (назначение и способы реализации).
12. Объекты защиты информации в сети.
13. Угрозы безопасности в Internet. Классификация сетевых атак.
14. Методы защиты информации в сети Internet.
15. Использование межсетевых экранов для обеспечения информационной безопасности в Internet. Классификация межсетевых экранов. Схемы подключения межсетевых экранов.
16. Частные виртуальные сети (VPN). Классификация VPN.
17. Комплексная защита информационных систем.
18. Управление доступом. Избирательное управление доступом.
19. Управление доступом. Полномочное (мандатное) управление доступом.
20. Организация защиты программного обеспечения от исследования.
21. Оценка стойкости парольной системы
22. Средства безопасности ОС семейства Windows
23. Средства безопасности ОС семейства Unix
24. Безопасность облачных вычислений

4.3 Пример экзаменационного билета

ГОУВПО «Донецкий национальный технический университет»

Уровень высшего профессионального образования *магистратура*

Направление подготовки (специальность): *09.04.01 Информатика и вычислительная техника*

Магистерская программа *Автоматизированные системы управления (АСУ)*
Семестр: 2
Учебная дисциплина: Информационная безопасность в АСУ

БИЛЕТ № 1

1. Классификация угроз информационной безопасности.
2. Управление доступом. Избирательное управление доступом
3. Программа взломщик паролей проверяет 70 паролей в секунду. Подобрать минимальную длину пароля, чтобы вероятность подбора паролей на протяжении недели непрерывной работы программы взломщика была больше 10^{-9}.

Утверждено на заседании кафедры «Автоматизированные системы управления»

Протокол № от
Зав. кафедрой А.И. Секирин

Экзаменатор А.И. Секирин

4.4 Критерии оценивания

В каждом билете содержится два теоретических вопроса и одна задача. Заданиям присваиваются следующие весовые коэффициенты: 0,3; 0,25 и 0,45. Сумма весовых коэффициентов равна единице.

Ответ на каждое задание оценивается по 100-бальной шкале.

В случае теоретического задания оценка «100» ставится в случае полного раскрытия вопроса без каких-либо неточностей. Баллы снимаются, если в ответе упущены какие-либо второстепенные моменты (до 10 баллов), допущены несущественные неточности (до 10 баллов), допущены существенные неточности при правильном ответе в целом (до 25 баллов), при недостаточном представлении материалов (баллы снимаются как процент недостающего материала с учетом его значимости).

В случае задачи оценка «100» ставится при представлении полного решения с правильным ходом и точным ответом, при верном указании единиц измерения и выполненном анализе результатов (если требуется). Баллы снимаются в случае: если в решении есть неточности, не повлиявшие на результат (до 15 баллов), неверно указаны или не указаны единицы измерения (до 15 баллов), допущены отдельные неточности в ходе решения, не исказившие ход решения в целом (до 25 баллов), неточность численных результатов (до 15 баллов), ошибки в анализе результатов (до 20 баллов).

Итоговая оценка за экзамен рассчитывается как сумма произведений оценок за каждое задание на их весовой коэффициент.

Полученная оценка по 100-балльной шкале определяет оценку по национальной шкале и шкале ESTS.

4.5 Пример текущего опроса на лабораторных занятиях

1. Что понимается под политикой безопасности в компьютерной системе?
2. В чем заключается модель дискреционной политики безопасности в компьютерной системе?
3. Что понимается под матрицей доступа в дискреционной политике безопасности? Что хранится в данной матрице?
4. Какие действия производятся над матрицей доступа в том случае, когда один субъект передает другому субъекту свои права доступа к объекту компьютерной системы?
5. Чем определяется стойкость подсистемы идентификации и аутентификации?
6. Перечислить минимальные требования к выбору пароля.
7. Перечислить минимальные требования к подсистеме парольной аутентификации.
8. Как определить вероятность подбора пароля злоумышленником в течение срока его действия?
9. Выбором каких параметров можно повлиять на уменьшение вероятности подбора пароля злоумышленником при заданной скорости подбора пароля злоумышленником и заданном сроке действия пароля?

Текущий контроль знаний студентов производится по результатам выполнения и защиты лабораторных работ. Защита работ включает ответы на контрольные вопросы по теме лабораторной работе, заданные преподавателем, или выполнение дополнительного индивидуального задания к лабораторной работе.

Промежуточная аттестация по результатам освоения дисциплины в семестре проводится в форме семестрового экзамена в соответствии с «Положением об организации учебного процесса в Донецком национальном техническом университете», утвержденном приказом ДонНТУ от 02.05.2018 г. №337-14. К экзамену допускаются студенты, выполнившие в полном объеме все работы, предусмотренные учебным планом.

Для определения уровня знаний студентов преподаватель руководствуется критериями оценки знаний, являющимися составляющей учебно-методического комплекса дисциплины.

5 РЕКОМЕНДУЕМАЯ ЛИТЕРАТУРА

I. Основная литература

1. Шаньгин В.Ф. Защита информации в компьютерных системах и сетях [Электронный ресурс] : учебное пособие для студентов технических вузов / В. Ф. Шаньгин ; В.Ф. Шаньгин ; гл. ред. Д.А. Мовчан. - 74 Мб. - Москва : ДМК Пресс, 2012. - 1 файл. - Систем. требования: Acrobat Reader. http://ed.donntu.org/books/cd5782.pdf

2. Мельников В.П. Защита информации [Электронный ресурс] : учебник для подготовки бакалавров по направлению 230100 "Информатика и вычислительная техника" / В. П. Мельников, А. И. Куприянов, А. Г. Схиртладзе ; В.П. Мельников, А.И. Куприянов, А.Г. Схиртладзе ; под ред. В.П. Мельникова. - 76 Мб. - Москва : ИЦ "Академия", 2014. - 1 файл. - (Высшее образование. Бакалавриат). - Систем. требования: ZIP-архиватор. http://ed.donntu.org/books/18/cd8182.zip

II. Дополнительная литература

3. Варфоломеев А.А. Основы информационной безопасности [Электронный ресурс] : учебное пособие для вузов / А. А. Варфоломеев ; А.А. Варфоломеев ; Приоритетн. нац. проект "Образование", РУДН. - 2 Мб. - Москва : РУДН, 2008. - 1 файл. - Систем. требования: Acrobat Reader. http://ed.donntu.org/books/cd4852.pdf

4. Шаньгин В.Ф. Комплексная защита информации в корпоративных системах [Электронный ресурс] : учебное пособие для вузов / В. Ф. Шаньгин ; В.Ф. Шаньгин. - 76 Мб. - М. : ФОРУМ : ИНФРА-М, 2010. - 1 файл. - (Высшее образование). - Систем. требования: Acrobat Reader. http://ed.donntu.org/books/cd3724.pdf

5. Шаньгин, В.Ф. Информационная безопасность компьютерных систем и сетей [Электронный ресурс] / В. Ф. Шаньгин. - 5 Мб. - 2011. - 1 файл. - Систем.

требования: Acrobat Reader. - ISBN 978-5-8199-0331-5. - ISBN 978-5-16-003132-3. http://ed.donntu.org/books/17/cd6560.pdf

6 УЧЕБНО-МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Учебно-методические издания, разработанные в ДонНТУ:

6. Методические указания для выполнения лабораторных работ по дисциплине "Информационная безопасность в АСУ" [Электронный ресурс] / сост.: О.В. Теплова, В.В. Пряхин – Донецк, ДонНТУ. 2020. – 1 файл. – Систем. требования: Acrobat Reader. (доступ через личный кабинет студента).

7. Методические указания для выполнения контрольной работы по дисциплине "Информационная безопасность в АСУ" [Электронный ресурс] / сост.: О.В. Теплова, В.В. Пряхин – Донецк, ДонНТУ. 2020. – 1 файл. – Систем. требования: Acrobat Reader. (доступ через личный кабинет студента).

8. Методические указания к организации самостоятельной работы [Электронный ресурс]: для студентов уровня профессионального образования «бакалавр» и «магистр» направлений подготовки : 09.04.01 «Информатика и вычислительная техника», 09.04.02 «Информационные системы и технологии» всех форм обучения / ГОУВПО «ДОННТУ», каф. Автоматизированных систем управления; сост.: С.Ю. Землянская, В.А. Светличная, А.И. Воронова, Е.А. Шуватова. – Электрон. дан. (1 файл: 667 Кб). – Донецк : ДОННТУ, 2020. – Систем. требования: Acrobat Reader. (доступ через личный кабинет студента).

Периодические издания и образовательные ресурсы:

8. Научные труды ДонНТУ. Серия: Информатика, кибернетика и вычислительная техника (2008-2014). http://ea.donntu.org:8080/jspui/handle/123456789/68
9. Информатика и кибернетика (2015-2020). http://infcyb.donntu.org/

7 МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

7.1 Лекционные занятия:

– *учебная аудитория №8.712*: учебный корпус 8 для проведения занятий лекционного типа, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации, мультимедийное оборудование: компьютер, операционная система Windows 7 Professional x86/64 (академическая подписка DreamSparkPremium), LibreOffice 4.3.2.2, Google Slides (бесплатная версия), мультимедийный проектор, экран; специализированная мебель: доска аудиторная, парты.

– *комплект электронных презентаций.*

7.2 Лабораторные работы:

– *компьютерная аудитория №8.603:* учебный корпус 8 для проведения лабораторных занятий, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации, (мультимедийное оборудование: компьютер Intel Pentium CPU G2020, операционная система Windows 7 Professional x86/64 (академическая подписка DreamSparkPremium, LibreOffice 4.3.2.2, Google Slides (бесплатная версия), Matlab, Microsoft Visual Studio Express, Google Chrome, Enterprise Architect Trial Edition, Cisco Packet Tracer 6.3, Wireshark, Adobe Flash Professional (Бесплатная пробная версия), GNS3, FreeCommander, HWiNFO, yEd Graph Editor, fxSolver, SCADA TRACE MODE, OpenOffice, Java, Eclipse, NetBeans, 7-zip, мультимедийная сеть; специализированная мебель: доска аудиторная, парты. Занятия проводятся в компьютерном классе, оснащенном:

- компьютеры с выходом в сеть (8 шт.);
- Wi-Fi роутер;
- пакеты программного обеспечения общего назначения (текстовые редакторы, графические редакторы, языки программирования высокого уровня).

7.3 Самостоятельная работа:

Помещения для самостоятельной работы с возможностью подключения к сети "Интернет" и обеспечением доступа в электронную информационно-образовательную среду организации: читальные залы, учебные корпуса 2,3 (Компьютерная техника с возможностью подключения к сети «Интернет» и обеспечением доступа в электронную информационно-образовательную среду (ЭИОС ДОННТУ) и электронно-библиотечную систему (ЭБС IPRbooks), а также возможностью индивидуального неограниченного доступа обучающихся в ЭБС и ЭИОС посредством Wi-Fi с персональных мобильных устройств. ОС- Microsoft Windows 7, OpenOffice 2.0.3 – общественная лицензия MPL 2.0/ Grub loader for ALT Linux - лицензия GNU LGPL v3/ Mozilla Firefox - лицензия MPL2.0, Moodle (Modular Object-Oriented Dynamic Learning Environment) - лицензия GNU GPLect-OrientedDynamicLearning Environment, лицензия GNUGPL).