

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
(МИНОБРНАУКИ РОССИИ)

Ю4: ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ
64836970683057 ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
ДОНБАССКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНИЧЕСКИЙ УНИВЕРСИ
(ФГБОУ ВО «ДонГТУ»)

Факультет	информационных технологий и автоматизации производственных процессов
Кафедра	интеллектуальных систем и информационной безопасности

УТВЕРЖДАЮ
И.о. проректора
по учебной работе

Д.В. Мулов

РАБОЧАЯ ПРОГРАММА ПРАКТИКИ

Технологическая
(наименование дисциплины)

10.05.03 Информационная безопасность автоматизированных систем
(код, наименование специальности)

Безопасность открытых информационных систем

(программа)

Квалификация специалист по защите информации
(бакалавр/специалист/магистр)

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

Алчевск, 2024

1 Цели и задачи технологической практики

Цели технологической практики. Повысить теоретический и практический уровень знаний будущих специалистов по обеспечению информационной безопасности автоматизированных систем, полученных в процессе обучения, на основе изучения работы предприятия, учреждения, организации, где они проходят практику, а также овладения производственными навыками и передовыми методами труда по специальности.

Задачи технологической практики:

- сбор, обработка, анализ и систематизация научно-технической информации, отечественного и зарубежного опыта по проблемам информационной безопасности автоматизированных систем;
- анализ безопасности информационных технологий, реализуемых в автоматизированных системах;
- сбор и анализ исходных данных для проектирования систем защиты информации;
- выполнение проектов по созданию программ, комплексов программ, программно-аппаратных средств, баз данных, компьютерных сетей для защищенных автоматизированных систем;
- контроль работоспособности и эффективности применяемых программно-аппаратных, криптографических и технических средств защиты информации;
- контроль реализации политики информационной безопасности;
- администрирование подсистем информационной безопасности автоматизированных систем;
- мониторинг информационной безопасности автоматизированных систем.

Технологическая практика направлена на формирование универсальных (УК-1, УК-3, УК-6, УК-8) общепрофессиональных (ОПК-2, ОПК-4, ОПК-9, ОПК-12) и профессиональных (ПК-1) компетенции выпускника.

2 Место технологической практики в структуре образовательной программы

Логико-структурный анализ дисциплины – «Технологическая практика» входит в обязательную часть БЛОКА 2 «Практика», подготовки обучающихся по специальности 10.05.03 – «Информационная безопасность автоматизированных систем» («Безопасность открытых информационных систем»).

Технологическая практика реализуется кафедрой интеллектуальных систем и информационной безопасности. Основывается на базе дисциплин: «Базы данных», «Основы информационной безопасности», «Архитектура вычислительных систем», «Сети и системы передачи информации».

В свою очередь компетенции, освоенные студентами в ходе прохождения технологической практики, могут быть использованы ими при изучении дисциплин: «Защита информации от утечки по техническим каналам», «Программно-аппаратные средства защиты информации».

Для прохождения практики необходимы компетенции, сформированные у обучающегося для решения универсальных, общепрофессиональных и профессиональных задач деятельности.

Технологическая практика является фундаментом для ориентации обучающихся в сфере алгоритмизации задач и создании программных продуктов.

Общая трудоемкость прохождения технологической практики составляет 6 зачетных единиц, 216 ак.ч. Программой технологической практики предусмотрена самостоятельная работа студента (216 ч.).

Технологическая практика проходит на 3 курсе после 6 семестра. Форма промежуточной аттестации – дифференцированный зачет.

Базой для прохождения технологической практики являются сторонние организации, основная деятельность которых предопределяет наличие объектов и видов профессиональной деятельности выпускников по данному направлению или на кафедрах и в лабораториях вуза, обладающих необходимым кадровым и научно-техническим потенциалом.

Практика осуществляется на основе договоров между Университетом и предприятиями, учреждениями, организациями, независимо от их организационно-правовых форм и форм собственности.

Практика проходит в течение четырех недель после экзаменационной сессии 6-го семестра (3 курс) у студентов очной формы обучения.

3 Перечень результатов обучения по технологической практике, соотнесённых с планируемыми результатами освоения образовательной программы

Процесс прохождения технологической практики направлен на формирование компетенций, представленных в таблице 1.

Таблица 1 – Компетенции, обязательные к освоению

Содержание компетенции	Код компетенции	Код и наименование индикатора достижения компетенции
1	2	3
Способен осуществлять критический анализ проблемных ситуаций на основе системного подхода, вырабатывать стратегию действий	УК-1	УК-1.4 Формулирует проблему, собирает информацию о проблемной ситуации, оценивает имеющиеся ограничения по ее разрешению, выбирает стратегию и тактику действий
Способен организовывать и руководить работой команды, вырабатывая командную стратегию для достижения поставленной цели	УК-3	УК-3.1 Определяет стратегию организации и руководства работой команды для достижения поставленной цели
Способен определять и реализовывать приоритеты собственной деятельности и способы ее совершенствования на основе самооценки и образования в течение всей жизни	УК-6	УК-6.3 Управляет своей познавательной деятельностью и способами удовлетворения образовательных интересов и потребностей

Продолжение таблицы 1

1	2	3
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	УК-8.3 Демонстрирует способы оказания первой помощи в зависимости от вида неотложного состояния организма
Способен применять программные средства системного и прикладного назначения, в том числе отечественного производства, для решения задач профессиональной деятельности	ОПК-2	ОПК-2.1 Применяет программные средства системного назначения, в том числе отечественного производства, для решения задач профессиональной деятельности
Способен анализировать физическую сущность явлений и процессов, лежащих в основе функционирования микроэлектронной техники, применять основные физические законы и модели для решения задач профессиональной деятельности	ОПК-4	ОПК-4.2 Применяет основные физические законы и модели для решения задач профессиональной деятельности

Продолжение таблицы 1

1	2	3
Способен решать задачи профессиональной деятельности с учетом текущего состояния и тенденций развития информационных технологий, средств технической защиты информации, сетей и систем передачи информации	ОПК-9	ОПК-9.1 Решает задачи профессиональной деятельности с учетом текущего состояния и тенденций развития информационных технологий
Способен применять знания в области безопасности вычислительных сетей, операционных систем и баз данных при разработке автоматизированных систем	ОПК-12	ОПК-12.2 Применяет знания в области безопасности операционных систем при разработке автоматизированных систем
Способен разрабатывать системы защиты информации автоматизированных систем	ПК-1	ПК-1.1 Осуществляет формирование требований к защите информации автоматизированных систем

4 Объём и виды занятий по технологической практике

Общая трудоёмкость технологической практики составляет 6 зачётных единицы, 216 ак.ч.

Самостоятельная работа студента (СРС) включает проработку материалов методических указаний по проведению практики, выполнение индивидуального задания, самостоятельное изучение материала и подготовку к дифференцированному зачету.

При организации внеаудиторной самостоятельной работы по данной дисциплине используются формы и распределение бюджета времени на СРС для очной формы обучения в соответствии с таблицей 2.

Таблица 2 – Распределение бюджета времени на СРС

Вид учебной работы	Всего ак.ч.	Ак.ч. по семестрам
		6
Аудиторная работа, в том числе:	-	-
Лекции (Л)	-	-
Практические занятия (ПЗ)	-	-
Лабораторные работы (ЛР)	-	-
Курсовая работа/курсовой проект	-	-
Самостоятельная работа студентов (СРС), в том числе:	216	216
Ознакомление с программой технологической практики и согласование тем индивидуальных заданий	8	8
Инструктаж по технике безопасности и противопожарной профилактике	8	8
Экскурсии по цехам, производствам и подразделениям предприятия	16	16
Работа на производственных участках и подразделениях предприятия по сбору материалов для выполнения индивидуального задания	64	64
Сбор информации по литературным источникам, интернет-ресурсам и цеховой документации	32	32
Выполнение индивидуального задания	64	64
Оформление отчета по практике	18	18
Подготовка к экзамену (диф.зачету)	6	6
Промежуточная аттестация – диф.зачет (ДЗ)	ДЗ	ДЗ
Общая трудоёмкость дисциплины		
ак.ч.	216	216
з.е.	6	6

5 Место и время проведения технологической практики

Базой для прохождения технологической практики являются сторонние организации, основная деятельность которых предопределяет наличие объектов и видов профессиональной деятельности выпускников по данному направлению или на кафедрах и в лабораториях вуза, обладающих необходимым кадровым и научно-техническим потенциалом.

Практика осуществляется на основе договоров между Университетом и предприятиями, учреждениями, организациями, независимо от их организационно-правовых форм и форм собственности.

Практика проходит в течение четырех недель после экзаменационной сессии 6-го семестра (3 курс).

Базовые предприятия для проведения производственной практики:

- 1) ООО «Южный горно-металлургический комплекс» (Алчевский металлургический комбинат);
- 2) ООО «Южный горно-металлургический комплекс» (Енакиевский металлургический комбинат);
- 3) бюджетные организации федерального и муниципального уровня;
- 4) банки и финансовые организации.

Место проведения практики в текущем учебном году определяется учебным планом и наличием договора с базовым предприятием.

6 Содержание технологической практики

Содержание практики и форма отчетности приведены в таблице 3.

Таблица 3 – Содержание практики и форма отчетности

№ п/п	Разделы (этапы) практики	Виды работы, на практике включая самостоятельную работу студентов	Формы текущего контроля
1.	Подготовительный , организационный этап	Распределение студентов по рабочим местам	Допуск к практике
		Ознакомление с распорядком рабочего дня и местом работы	
		Инструктаж по технике безопасности и противопожарной профилактике	
		Получение индивидуального задания	
2.	Основной этап	Экскурсии по цехам, производствам и подразделениям предприятия	Подразделы отчета по практике
		Работа на производственных участках и подразделениях предприятия по сбору материалов для выполнения индивидуального задания	
		Сбор информации по литературным источникам, интернет-ресурсам и цеховой документации	
		Выполнение индивидуального задания	
3.	Заключительный этап	Подготовка и оформление заключительного отчета о практике	Предоставл ение отчета
		Защита отчета	Защита отчета

Освоение компетенций при прохождении технологической практики осуществляется в три этапа:

- работа на производственных участках и подразделениях предприятия по сбору материалов для выполнения индивидуального задания;
- сбор информации по литературным источникам, интернет-ресурсам и цеховой документации;
- выполнение индивидуального задания.

Обучающийся должен ознакомиться:

- с технологическим процессом производства;
- с программным и техническим обеспечением, имеющимся на предприятии.

Обучающийся должен изучить:

- организацию производства и технику безопасности на предприятии;
- технологический процесс производства;

– закрепить навыки оформления отчетной документации в соответствии с требованиями действующих стандартов, а также навыки пользования технической и справочной литературой.

При прохождении технологической практики предусматривается использование в учебном процессе активных и интерактивных форм проведения занятий с обсуждением индивидуальных заданий и путей их выполнения. Текущий контроль осуществляется в виде кратких отчетов по этапам практики.

После окончания технологической практики в сроки, установленные кафедрой, каждый обучающийся представляет отчет по практике руководителю и защищает его.

По содержанию работы, оформлению отчёта, ответам руководитель устанавливает глубину знаний обучающегося по данной работе, степень самостоятельности в выполнении индивидуального задания и принимает решение о дифференцированной оценке прохождения практики. Оценка проставляется в зачётную книжку обучающегося и в ведомость.

Невыполнение обучающимся требований к прохождению технологической практики в сроки, установленные учебным планом, рассматривается как академическая задолженность.

Организация практики

В начале практики студенты проходят инструктаж по правилам техники безопасности на кафедре и промышленном предприятии и получают общее представление о предприятии в целом.

Более детальное ознакомление студентов с производством происходит в подразделениях предприятия путем наблюдения их работы в определенной технологической последовательности.

Последовательность пребывания в цехах и распределение времени практики устанавливается графиком практики для каждой группы в отдельности.

Основными объектами наблюдения в каждом из цехов являются:

- технологический процесс;
- организация производства и техника безопасности на предприятии;
- программное и техническое обеспечение, имеющимся на предприятии.

Во время прохождения практики на предприятии руководители практики от завода и университета, проводят консультации и экскурсии, на которых сообщаются основные сведения, необходимые для составления отчета. Посещение консультаций и участие в экскурсии для студентов обязательны. Темы этапов практики и их краткое содержание должны быть

отражены в соответствующем разделе дневника по практике.

В процессе практики студенты ведут дневники, в которые вносятся записи, эскизы, схемы и т.д., отражающие вышеперечисленные вопросы. На основании этих материалов и учебных пособий составляется отчет по практике.

Отчет по практике составляется каждым студентом самостоятельно. В отчет заносятся результаты личных наблюдений студентов на производстве и основные данные, сообщенные студентам на консультациях и во время экскурсий.

После прохождения общего инструктажа по технике безопасности, получения пропусков на предприятие и распределения по подразделениям предприятия в отделе подготовки кадров, студенты закрепляются за руководителями практики от предприятия. Рекомендует руководителей сотрудник бюро организации производства цеха, а утверждает начальник цеха или старший мастер смены.

В обязанности руководителя практики от предприятия входит:

- проведение инструктажа по технике безопасности в данном подразделении;
- проведение экскурсии по основным и вспомогательным подразделениям;
- консультирование по вопросам технологии производства в подразделении и применяемому основному и вспомогательному программному и техническому обеспечению производства;
- организация прохождения практики в отдельных подразделениях предприятия;
- помощь в сборе материалов для выполнения индивидуального задания и составления отчета по практике;
- участие в принятии зачета по практике.

После прохождения инструктажа по технике безопасности в цеху и экскурсий студенты начинают изучать основное и вспомогательное программное и техническое обеспечение производства.

Руководитель практики от предприятия договаривается со старшим на участке (мастерами или бригадирами) о кураторстве практики на каждом участке длительностью 1-3 смены.

Кураторство состоит из проведения инструктажа по технике безопасности на рабочем месте (участке), пояснение особенностей технологии и устройства оборудования, оказание помощи в сборе материалов для отчета и индивидуального задания. Желательно прохождение практики в виде стажировки, когда студент наблюдает выполнение всех обязанностей

своим куратором на данном участке, начиная и заканчивая сменно-встречными собраниями.

На протяжении всей практики каждый студент обязан вести дневник практики, куда он должен заносить всю информацию о выполнении за день работы и сборе материалов.

В последнюю неделю практики студенты заканчивают сбор материалов, при необходимости обращаясь в библиотеку предприятия, его архивы и патентное бюро и составляют отчет. В конце недели они получают отзыв о своей работе со стороны руководителя практики от предприятия (в дневнике практики) и сдают дифференцированный зачет руководителю от университета (может присутствовать руководитель от предприятия).

Отчетность обучающегося о результатах технологической практики

По ходу выполнения программы практики обучающиеся пишут отчет, который защищают по окончании практики.

По окончании практики обучающийся защищает отчет и получает дифференцированный зачет. Защита отчета производится на кафедре, на последней неделе в специально отведенные дни (1-2 дня), предусмотренные в графике прохождения практики, но не позднее 10 дней после начала следующего за практикой учебного семестра.

Для сдачи зачета по практике обучающийся должен иметь следующие документы:

- письменный отчет, оформленный в соответствии с требованиями действующих стандартов на оформление отчетов;
- дневник практики;
- отзыв руководителя практики от предприятия, заверенный печатью (в дневнике практики).

Проявление обучающимся недобросовестного отношения к практике, нарушение дисциплины, невыполнение программы практики, получение неудовлетворительной оценки при защите отчета влечет за собой оставление обучающегося на повторный курс или отчисление из университета.

Итоги технологической практики обсуждаются на заседании кафедры, советах факультета и университета.

Требования к оформлению отчета по практике

Оформление отчета является итоговым этапом прохождения технологической практики. В отчете должны быть отражены все мероприятия, предусмотренные в графике прохождения практики.

Исходными данными для составления отчета должны быть: дневник практики, сведения, полученные при выполнении отдельных пунктов программы практики, а также сведения, полученные на лекциях и

практических занятиях.

Описание программного обеспечения и аппаратных средств должно сопровождаться иллюстрациями в виде эскизов и справочными данными.

Отчет выполняется в виде пояснительной записки, которая должна иметь следующую структуру:

- титульный лист (образец выдается кафедрой);
- реферат;
- содержание;
- введение;
- основная часть (разделы, посвященные отдельным этапам практики);
- заключение;
- приложения (при необходимости).

Объем пояснительной записки должен составлять не менее 40-50 страниц в виде текста, иллюстраций, таблиц или их сочетаний. Пояснительная записка выполняется на одной стороне листов белой бумаги формата А4 (210×297 мм), разрешается использовать печатающие устройства ЭВМ, при этом высота букв и цифр должна быть размером 14, а на странице должно быть размещено не более 40 строк. Допускается использование листов формата А3 (297×420 мм) для приложений, если это необходимо. В пояснительную записку помещается систематизированный, аккуратно оформленный материал.

При оформлении пояснительной записки отчета необходимо руководствоваться требованиями действующих стандартов, а также рекомендациями кафедры.

Оформление отчета производится поэтапно по мере накопления материала в свободное время от других занятий, определенных программой практики.

7 Фонд оценочных средств для проведения текущего контроля успеваемости и промежуточной аттестации студентов по технологической практике

7.1 Критерии оценивания

В соответствии с Положением о кредитно-модульной системе организации образовательного процесса ФГБОУ ВО «ДонГТУ» (https://www.dstu.education/images/structure/license_certificate/polog_kred_modul.pdf) при оценивании сформированности компетенций по дисциплине используется 100-балльная шкала.

Перечень компетенций по технологической практике и способы оценивания знаний приведены в таблице 4.

Таблица 4 – Перечень компетенций по технологической практике и способы оценивания знаний

Код и наименование компетенции	Способ оценивания	Оценочное средство
УК-1, УК-3, УК-6, УК-8, ОПК-2, ОПК-4, ОПК-9, ОПК-12, ПК-1	Дифференцированный зачет	Защита отчета по практике

В шестом семестре (очная форма обучения) после экзаменационной сессии обучающиеся проходят технологическую практику и в итоге могут получить от 60 до 100 баллов (диф. зачет). Обучающиеся, которые выполнили график самостоятельной работы и защитили отчет по практике получают зачетную оценку по дисциплине в этом семестре. Если оценка не удовлетворяет обучающегося, он имеет право после исправления замечаний повторно защитить работу (отчет по практике).

Подводя итоги прохождения технологической практики, можно использовать следующие критерии (показатели) оценки ответов:

- достаточные знания в объеме изучаемой и разрабатываемой темы;
- использование научной терминологии, стилистически грамотное, логически правильное изложение ответа на вопросы, умение делать выводы;
- владение инструментарием изучаемой темы, умение его использовать в решении учебных и профессиональных задач;
- способность самостоятельно применять типовые решения в рамках учебной программы;

- усвоение основной литературы, рекомендованной учебной программой для изучаемой темы;
- умение ориентироваться в базовых теориях, концепциях и направлениях по изучаемой теме и давать им сравнительную оценку;
- полнота и конкретность ответа;
- последовательность и логика изложения;
- уровень выполнения и оформления пояснительной записки по практике.

При проведении аттестации обучающихся важно всегда помнить, что систематичность, объективность, аргументированность – главные принципы, на которых основаны контроль и оценка их знаний.

Шкала оценивания знаний при проведении промежуточной аттестации приведена в таблице 5.

Таблица 5 – Шкала оценивания знаний

Сумма баллов за все виды учебной деятельности	Оценка по национальной шкале зачёт/экзамен
0-59	Не зачтено/неудовлетворительно
60-73	Зачтено/удовлетворительно
74-89	Зачтено/хорошо
90-100	Зачтено/отлично

Для текущего контроля успеваемости обучающихся при прохождении практики, проводятся консультационно-практические занятия, на которых руководитель практики от университета контролирует ход выполнения ее программы и написания отчета.

7.2 Примерный перечень вопросов, выносимых на защиту отчета по технологической практике

- 1) Что такое информация, информационная безопасность, защита информации, конфиденциальная информация?
- 2) Как классифицируется информация?
- 3) Что такое утечка информации?
- 4) Каким образом классифицируются каналы утечки информации?
- 5) В чем состоит актуальность проблем информационной безопасности?
- 6) Каковы правовые понятия в области защиты информации?

- 7) Какие методы защиты информации, использовавшиеся в древнее время и в Средние века Вам известны?
- 8) В чем, на Ваш взгляд, заключаются основные трудности обеспечения информационной безопасности в настоящее время?
- 9) В каких направлениях идет развитие теории информационной безопасности в настоящее время?
- 10) С чем связан возросший интерес к проблемам защиты информации?
- 11) Каков вклад российских ученых в теорию информационной безопасности?
- 12) Что такое конфиденциальность, целостность, доступность?
- 13) Что такое информационная система? Телекоммуникационная система? Автоматизированная система?
- 14) Каковы основные принципы построения систем защиты информации?
- 15) Что такое комплексный подход к обеспечению информационной безопасности?
- 16) Каковы основные задачи защиты информации?
- 17) Каковы основные средства реализации комплексной системы защиты информации?
- 18) Что такое морально-этические средства защиты информации?
- 19) Что такое центры информационной безопасности и какова их роль в развитии теории и практики защиты информации?
- 20) Перечислите основные носители информации, особенности их использования и защиты.
- 21) Какими свойствами определяется ценность информации?
- 22) Что понимается под информационными ресурсами?
- 23) Какие существуют виды тайны?
- 24) Какое назначение имеет перечень конфиденциальных сведений предприятия?
- 25) Что не разрешается относить к информации ограниченного доступа?
- 26) Каково место информационной безопасности в системе национальной безопасности Российской Федерации?
- 27) Какова структура государственной системы защиты информации?
- 28) Кто несет ответственность за нарушение режима защиты информации?

- 29) Каковы функции руководителей предприятий при организации защиты информации?
- 30) Каковы основные функции ФСТЭК?
- 31) Какие основные положения Доктрины информационной безопасности приняты в РФ?
- 32) Для каких систем (приведите примеры) наибольшую опасность представляет нарушение целостности информации?
- 33) В каких системах на первом месте стоит обеспечение доступности информации?
- 34) В чем различие понятий «нарушение конфиденциальности информации», «несанкционированный доступ к информации», «утечка информации»?
- 35) В чем отличие терминов «НСД» и «Нарушение конфиденциальности информации»?
- 36) Каким образом следует выбирать меры защиты конфиденциальности информации?
- 37) В чем разница между понятиями идентификации и аутентификации пользователя?
- 38) Какой из способов аутентификации Вы считаете наиболее эффективным? Почему?
- 39) Какие основные методы контроля доступа используются в известных вам информационных системах? В чем их достоинства и недостатки?
- 40) Почему аутентификация с использованием пароля считается в настоящее время ненадежной?
- 41) Каковы методы аутентификации с использованием предметов заданного типа?
- 42) Поясните, что понимается под понятием – совершенный шифр?
- 43) Почему большинство современных шифрограмм могут быть однозначно дешифрованы?
- 44) Каким образом государство регулирует использование средств криптозащиты?
- 45) Каковы способы контроля целостности потока сообщений?
- 46) Какие существуют способы контроля целостности сообщений при взаимном доверии сторон?
- 47) Как контролировать целостность сообщений при высоком уровне помех в каналах связи?
- 48) Как организован обмен документами, заверенными цифровой подписью?

- 49) В чем отличие и сходство обычной и цифровой подписей?
- 50) Какими принципами нужно руководствоваться для сохранения целостности данных при их обработке?
- 51) Почему проблемы контроля целостности данных относятся к проблемам информационной безопасности?
- 52) Что означает контроль целостности данных на уровне содержания?
- 53) Как обеспечить целостность данных при их хранении?
- 54) Что такое надежность и чем отличается надежность аппаратуры от надежности программного обеспечения?
- 55) Следует ли различать защиту от случайных угроз и от действий злоумышленника при обеспечении беспрепятственного доступа к информации?
- 56) Как защитить программное обеспечение от изучения логики его работы?
- 57) Как изменяется надежность аппаратуры с течением времени?
- 58) Каковы способы повышения надежности аппаратуры и линий связи?
- 59) Что из себя представляет матрица доступа?
- 60) Что из себя представляет граф доступа?
- 61) Что такое политика безопасности, кто ее разрабатывает и где она применяется?
- 62) Приведите классификацию моделей разграничения доступа. Какова их роль в теории информационной безопасности?
- 63) Каковы основные достоинства и недостатки дискреционных моделей?
- 64) Что такое монитор безопасности и какие требования к нему предъявляются?
- 65) Перечислите основные положения субъектно-объектного подхода к разграничению доступа? В чем достоинства и недостатки такого подхода?
- 66) В чем суть мандатной политики разграничения доступа?
- 67) Каковы основные достоинства и недостатки мандатной политики?
- 68) Что такое скрытые каналы утечки информации и как их обнаружить?
- 69) Почему ролевая политика получила большое распространение?
- 70) В чем суть моделей группового доступа?
- 71) Что такое информационная невыводимость и информационное невмешательство?

- 72) Как и зачем строятся многоуровневые схемы разграничения доступа?
- 73) Чем отличаются понятия «информационная война» и «информационное противоборство»?
- 74) Какие виды информационных войн Вы можете выделить?
- 75) Можно ли рассматривать рекламу как средство ведения информационной борьбы?
- 76) Что такое информационное оружие?
- 77) Какие виды оружия применяются в ходе ведения информационной войны?
- 78) Каковы цели информационной войны?
- 79) Каковы средства и методы защиты от информационно-технического оружия?
- 80) Каковы особенности информационно-психологической войны?
- 81) Что такое аттестация объекта автоматизации?
- 82) Что такое сертификация средств защиты информации?
- 83) Что такое лицензирование деятельности в области защиты информации?
- 84) Что представляет из себя риск-ориентированный подход при обеспечении информационной безопасности?
- 85) Какие технические каналы утечки информации Вы знаете?
- 86) Какие криптографические методы обработки информации используются в области информационной безопасности?
- 87) Что такое симметричная система шифрования, ее достоинства и недостатки?
- 88) Что такое асимметричная система шифрования, ее достоинства и недостатки?
- 89) Какие известны основные принципы построения систем защиты информации?
- 90) Какие известны подсистемы обеспечения информационной безопасности?
- 91) Что такое центр мониторинга и управления безопасностью?
- 92) Перечислите основополагающие документы по информационной безопасности.
- 93) Что подразумевает понятие государственной тайны?
- 94) Основные задачи информационной безопасности в соответствии с Концепцией национальной безопасности РФ.

95) Дайте характеристику Федерального закона от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации».

96) Какая ответственность в Уголовном кодексе РФ предусмотрена за создание, использование и распространение вредоносных компьютерных программ?

97) Назовите 5 – 6 из 11 существующих функциональных требований стандарта ГОСТ Р ИСО/МЭК 15408-1-2012.

98) Для чего служит профиль защиты, согласно стандарту ГОСТ Р ИСО/МЭК 15408-1-2012?

99) Что прописано в Доктрине информационной безопасности РФ?

100) Чем отличаются функциональные требования от требований доверия, согласно стандарту ГОСТ Р ИСО/МЭК 15408-1-2012?

101) Что предполагает информационное обеспечение любой компании в целом?

102) Что такое макровирус?

103) Какие типы файлов заражают макровирусы?

104) Как просмотреть код макровируса?

105) Как восстановить файл, зараженный макровирусом?

106) Что такое компьютерный вирус?

107) Какими свойствами обладают компьютерные вирусы?

108) Повысится ли устойчивость компьютера к воздействию вируса, если установить два антивирусных продукта одновременно?

109) Каковы внешние проявления наличия вируса в компьютере?

110) Какие программы-доктора вы знаете?

111) Какие вирусы называются резидентными, и в чем особенность таких вирусов?

112) Дать характеристику вируса-невидимки.

113) Что представляет «полная изоляция» вируса?

114) Характеристика сетевых вирусов.

115) Чем опасны файлово-загрузочные вирусы?

116) Что такое логическая бомба?

117) Что такое электронно-цифровая подпись?

118) Для чего используется механизм электронной цифровой подписи?

119) Алгоритмы электронно-цифровой подписи.

120) Какой метод шифрования использует электронная цифровая подпись?

121) Виды цифровой подписи.

- 122) Что такое реестр ОС Windows 10?
- 123) Поясните особенности «троянских программ».
- 124) Почему профилактика «троянских программ» связана с системным реестром?
- 125) Какие разделы и ключи реестра являются потенциальными местами запуска «троянских программ»?
- 126) Что такое аутентификация и идентификация?
- 127) Для чего применяются эти механизмы?
- 128) Что можно настроить с помощью вкладки «Локальные политики безопасности»?
- 129) Что понимают под техническими каналами утечки информации?
- 130) Для чего служат средства перехвата информации?
- 131) На какие виды делятся технические каналы утечки информации?
- 132) Что относится к электромагнитным каналам утечки информации?
- 133) Какова природа возникновения электрических каналов?
- 134) Какой канал утечки информации называют параметрическим?
- 135) Дайте описание вибрационных каналов утечки информации
- 136) Какая информация называется речевой?
- 137) Что является средой распространения речевых сигналов в акустических каналах утечки информации?
- 138) Что является средой распространения речевых сигналов в виброакустических каналах?
- 139) Покажите связь между уровнем развития общества и технологиями защиты информации.
- 140) В каких направлениях идет развитие теории информационной безопасности в настоящее время?
- 141) Каков вклад российских ученых в теорию информационной безопасности?
- 142) С чем связан возросший интерес к проблемам защиты информации?
- 143) Каковы отличия формального и неформального подходов к проблемам защиты информации?
- 144) В чем, на Ваш взгляд, заключаются основные трудности обеспечения информационной безопасности в настоящее время?
- 145) Что такое информационная система? Телекоммуникационная система? Автоматизированная система?
- 146) Каковы правовые понятия в области защиты информации?
- 147) Что такое защита информации? Информационная безопасность?

148) Охарактеризуйте понятия, связанные с организацией защиты информации.

149) Каковы основные принципы построения систем защиты информации?

150) Что такое комплексный подход к обеспечению информационной безопасности?

151) Каковы основные задачи защиты информации?

152) Какова взаимосвязь различных средств защиты информации? Есть ли среди них приоритетные?

153) Каковы основные средства реализации комплексной системы защиты информации?

154) Что такое морально-этические средства защиты информации?

155) Докажите необходимость сочетания различных средств защиты информации.

156) Приведите примеры формальных и неформальных средств защиты?

157) Что такое центры информационной безопасности и какова их роль в развитии теории и практики защиты информации?

158) Что такое информация и каковы уровни ее представления?

159) Перечислите основные носители информации, особенности их использования и защиты.

160) Какими свойствами определяется ценность информации?

161) Какие критерии оценки ценности информации Вы можете предложить?

162) Приведите примеры различной зависимости ценности информации от времени.

163) Что понимается под информационными ресурсами?

164) Что не разрешается относить к информации ограниченного доступа?

165) Что понимается под конфиденциальной информацией?

166) Какие существуют виды тайны?

167) Какое назначение имеет перечень конфиденциальных сведений предприятия?

168) Каково место информационной безопасности в системе

169) национальной безопасности Российской Федерации?

170) Сформулируйте основные положения Доктрины информационной безопасности РФ.

171) Каковы основные цели защиты информации?

172) Каковы основные задачи в области информационной безопасности?

173) Какова структура государственной системы защиты информации?

174) Кто несет ответственность за нарушение режима защиты информации?

175) Каковы функции руководителей предприятий при организации защиты информации?

176) Каковы основные функции ФСТЭК?

8. Учебно-методическое и информационное обеспечение технологической практики

8.1 Рекомендуемая литература

Основная литература

1. Сычев Ю.Н. Защита информации и информационная безопасность : учебное пособие для студентов высших учебных заведений, обучающихся по направлению подготовки 10.03.01 "Информационная безопасность" (квалификация (степень) "бакалавр") / Ю.Н. Сычев . — Москва : ИНФРА-М, 2023 . — 199 с.: ил. + табл. — 15 экз.

Дополнительная литература

1. Гродзенский Я.С. Информационная безопасность: учебное пособие / Я.С. Гродзенский. - Москва: Проспект, 2021. - 142 с. Режим доступа: <https://knigogid.ru/books/1582163-informacionnaya-bezopasnost-nacionalnye-standarty-rossiyskoy-federacii/toread/fragment> (Дата обращения - 26.08.24).

Перечень ресурсов информационно-телекоммуникационной сети

8.2 Базы данных, электронно-библиотечные системы, информационно-справочные и поисковые системы

1. Научная библиотека ДонГТУ : официальный сайт.— Алчевск. — URL: library.dstu.education.— Текст : электронный.

2. Научно-техническая библиотека БГТУ им. Шухова : официальный сайт. — Белгород. — URL: <http://ntb.bstu.ru/jirbis2/>.— Текст : электронный.

3. Консультант студента : электронно-библиотечная система.— Москва. — URL: <http://www.studentlibrary.ru/cgi-bin/mb4x>.— Текст : электронный.

4. Университетская библиотека онлайн : электронно-библиотечная система.— URL: http://biblioclub.ru/index.php?page=main_ub_red.— Текст : электронный.

6. Сайт кафедры ИСИБ <http://scs.dstu.education>

Материально-техническое обеспечение представлено в таблице 6.

Таблица 6 – Материально-техническое обеспечение

Наименование оборудованных учебных кабинетов	Адрес (местоположение) учебных кабинетов
Специальные помещения: Аудитории для проведения лекций: <i>Мультимедийная аудитория. (60 посадочных мест),</i> оборудованная специализированной (учебной) мебелью (парта трехместная – 18 шт., парта двухместная – 6 шт, стол– 1 шт., доска аудиторная– 1 шт.), учебное ПК (монитор + системный блок), мультимедийная стойка с оборудованием – 1 шт., широкоформатный экран. <i>Компьютерные классы (22 посадочных места),</i> оборудованный учебной мебелью, компьютерами с неограниченным доступом к сети Интернет, включая доступ к ЭБС: ПК– 12 шт.; Доска – 1 шт.	ауд. <u>207</u> корп. <u>4</u> ауд. <u>211</u> корп. <u>4</u>

Лист согласования рабочей программы дисциплины

Разработал:

ст. преподаватель кафедры интеллектуальных системи информационной безопасности

(должность)


(подпись)Р.Н.Погорелов

Ф.И.О.)

(должность)

(подпись)

Ф.И.О.)

(должность)

(подпись)

Ф.И.О.)

И.о. заведующего кафедрой


(подпись)Е.Е.Бизянов

Ф.И.О.)

Протокол № 1 заседания кафедры ИСИБ от 27.08.2024 г

И.о. декана факультета


(подпись)В.В. Дьячкова

Ф.И.О.)

Согласовано:

Председатель методической
комиссии по специальности
10.05.03 Информационная безопасность
автоматизированных систем
(подпись)Е.Е. Бизянов

Ф.И.О.)

Начальник учебно-методического центра


(подпись)О.А.Коваленко

Ф.И.О.)

Лист изменений и дополнений

Номер изменения, дата внесения изменения, номер страницы для внесения изменений	
ДО ВНЕСЕНИЯ ИЗМЕНЕНИЙ:	ПОСЛЕ ВНЕСЕНИЯ ИЗМЕНЕНИЙ:
Основание:	
Подпись лица, ответственного за внесение изменений	