МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное бюджетное образовательное учреждение высшего образования
«РОССИЙСКИЙ БИОТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ (РОСБИОТЕХ)»

РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ

Б1.О.28. Защита информации

(Адаптированная рабочая программа для лиц с ограниченными возможностями здоровья и инвалидов)

Направление подготовки:	09.03.01 Информатика и вычислительная техника
Программа бакалавриата:	Модели, методы и программное обеспечение анализа проектных решений
Уровень программы:	бакалавриат
Форма обучения:	очная

2024

1. ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОБУЧЕНИЯ ПО ДИСЦИПЛИНЕ И ЕЕ МЕСТО В СТРУКТУРЕ ОПОП

1. Общие положения

1.1. Цели и задачи дисциплины

Заложить терминологический фундамент, рассмотреть основные

общеметодологические принципы теории информационной безопасности; изучить методы и средства обеспечения ИБ, методы нарушения конфиденциальности, целостности и доступности информации и противодействия этим нарушениям.

Задачи освоения дисциплины являются:

- Формирование знаний у студентов о современном состоянии проблемы обеспечения информационной безопасности при использовании компьютерных технологий, существующих угрозах, видах обеспечения информационной безопасности, методах и средствах защиты информации и основах построения комплексных систем защиты - изучить среды трехмерной компьютерной графики как средства моделирования и анимации;

изучение физических основ инженерно-технической защиты информации; – изучение технических средств добывания и защиты информации;

– изучение организационных основ инженерно-технической защиты информации;

– изучение методического обеспечения инженерно-технической защиты информации.

1.2. Место дисциплины в структуре образовательной программы

Данная учебная дисциплина включена в базовую часть образовательной программы бакалавриата по направлению подготовки 09.03.01 «Информатика и вычислительная техника» Осваивается на 4 курсе, в 7 и 8 семестрах. Итоговая аттестация – зачет на 7 семестре; экзамен на 8 семестре.

Дисциплина «Информационная безопасность» относится к базовой части дисциплин образовательной программы. Данный курс базируется на знаниях, полученных в области информатики, операционных систем, сети и телекоммуникации. Знания, умения и навыки, полученные в процессе изучения данного курса, могут быть использованы студентами для подготовки выпускной квалификационной работы.

1.3. Перечень планируемых результатов обучения по дисциплине, соотнесенных с планируемыми результатами освоения образовательной программы:

Освоение дисциплины направлено на формирование следующих общекультурных и профессиональных компетенций бакалавра:

Дисциплина входит в состав части образовательной программы, формируемой участниками образовательных отношений.

Таблица 1.1 – Результаты обучения по дисциплине

Код, наименование индикатора	Результаты обучения по дисциплине
ОПК-3 Способен решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности **ОПК -8 Способен разрабатывать алгоритмы и программы, пригодные для практического применения**	
ИД-1 (ОПК-3) Знать:	принципы, методы и средства решения стандартных задач профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности
ИД-2 (ОПК-3, ОПК-8) Уметь	решать стандартные задачи профессиональной деятельности на основе информационной и библиографической ку льтуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности
ИД-3 (ОПК-3, ОПК-8) Владеть:	иметь навыки: подготовки обзоров, аннотаций, составления рефератов, научных докладов, публикаций и библиографии по научно-исследовательской работе с учетом требований информационной безопасности

Результаты обучения по дисциплине достигаются в рамках осуществления всех видов контактной и самостоятельной работы обучающихся в соответствии с утвержденным учебным планом.

Индикаторы достижения компетенций считаются сформированными при достижении соответствующих им результатов обучения.

2. ОБЪЁМ ДИСЦИПЛИНЫ

Объем дисциплины составляет 5 зачетных единиц.

Ниже приведено распределение общего объема дисциплины (в академических часах) в соответствии с утвержденным учебным планом.

Таблица 1. Виды работ

Виды работ	Форма обучения
	Очная
	7 семестр
занятия лекционного типа	16
практические занятия	16
Контроль (зачет)	4
Самостоятельная работа	36
	8 семестр
занятия лекционного типа	24
практические занятия	24
Контроль (экзамен)	36
Самостоятельная работа	**24**
Всего	**182**

3. Содержание дисциплины

3.1 Перечень разделов и (или) тем дисциплины и их дидактическое содержание

Таблица 2. Разделы и темы дисциплины

№ компетенции	№ п/п	Наименование раздела (темы) дисциплины	Содержание раздела (темы) в дидактических единицах
ОПК-3, ОПК-8	**1**	Тема 1. Основные понятия и определения в области информационной безопасности	Основные понятия и определения, относящиеся к ИБ. Необходимость защиты информации. Основные задачи обеспечения защиты информации. Объекты, цели и задачи защиты информации
	2	Тема 2. Угрозы информационной безопасности. Каналы утечки информации	Понятие угрозы. Классификация видов угроз ИБ по различным признакам. Технологические аспекты утечки безопасности. Угрозы доступности, целостности и конфиденциальности. Юридические аспекты информационной безопасности. Классификация атак. Сетевые атаки. Окно опасности. ПЗ Анализ способов нарушений информационной безопасности
	3	Тема 3. Вредоносное ПО. Компьютерные вирусы и средства защиты от них.	Понятие компьютерного вируса. Признаки появления вируса. Классификация вирусов. Вирусная сигнатура. Антивирусные программы. Программы «сторожа», ревизоры, доктора, детекторы, вакцины. Основные функции правовой базы. Законодательство РФ в области защиты информации. Владельцы защищаемой информации. Понятие государственная тайна, коммерческая тайна. Профессиональная тайна, служебная тайна. Криптографические методы информационной безопасности. ПЗ: Анализ способов нарушений информационной безопасности

	4	Тема 4. Стандарты информационной безопасности	Роль стандартов информационной безопасности. Методы и средства защиты информации. Критерии безопасности компьютерных систем министерства обороны США ("Оранжевая книга"). Классы защищенности компьютерных систем. Интерпретация и развитие Критериев безопасности. Руководящие документы ФСТЭК России. Рекомендации Х.800.
	5	Тема 5. Административный уровень информационной безопасности	Административный уровень информационной безопасности: основные понятия. Политика безопасности. Программа безопасности. Концепция информационной безопасности. . Программно-технический уровень безопасности.
	6	Тема 6. Процедурный уровень информационной безопасности .	Лицензирование и сертификация информационной безопасности. Организация внутриобъектового и пропускного режимов на предприятиях. Управление персоналом. Физическая защита. Поддержание работоспособности. Реагирование на нарушения режима безопасности. Планирование восстановительных работ. Организация подготовки и проведения заседаний по конфиденциальным вопросам. Защита информации при публикаторской деятельности, при рекламной деятельности. Защита информации при работе с посетителями. Организация работы с документами.
	7	Тема 7. Программно-технические методы защиты информационной безопасности	Критерий безопасности компьютерных сетей.. Основные понятия программно-технического уровня ИБ. Архитектурная безопасность. Парольная аутентификация. Одноразовые пароли. Идентификация/ аутентификация с помощью биометрических данных. Протоколирование. Активный аудит. Функциональные компоненты и архитектура. Криптография. Стеганография. Управление доступом. Понятие таксономии нарушения безопасности. Причины нарушения информационной безопасности. Аудит событий в рамках информационной системы. ПЗ: Основные технологии построения защищенных систем

3.2 Распределение учебного времени по семестру, разделам и (или) темам, видам учебных занятий, видам текущего контроля успеваемости очной формы обучения. *(*смотри условные обозначения)*

Таблица 3. Распределение текущего времени дисциплины

№ п/п	Вид занятия	Период обучения (семестр). Наименование раздела (темы) дисциплины. Тема учебного занятия	Количество часов	Формы текущего контроля успеваемости					
				РИ	Обс	Пр	Кп	КУ	РЗ
7 семестр									
	ЛЗ, ПЗ	Тема 1. Основные понятия и определения в области информационной безопасности	6/4	+		+		+	+
	ЛЗ, ПЗ	Тема 2. Угрозы информационной безопасности. Каналы утечки информации	4/6	+	+	+		+	+
	ЛЗ, ПЗ	Тема 3. Вредоносное ПО. Компьютерные вирусы и средства защиты от них.	6/6	+		+		+	+
		Зачет							
Всего за 7 семестр									
8 семестр									
	ЛЗ, ПЗ	Тема 4. Стандарты информационной безопасности	6/6	+	+	+	+	+	+
	ЛЗ, ПЗ	Тема 5. Административный уровень информационной безопасности	6/6	+		+		+	+
	ЛЗ, ПЗ	Тема 6. Процедурный уровень информационной безопасности .	6/6			+	+	+	+

	ЛЗ, ПЗ	Тема 7. Программно-технические методы защиты информационной безопасности	6/6		+	+			+
	Экзамен								
Всего за 8 семестр									
Всего по дисциплине									

***Формы контроля (условные обозначения)**

РИ	Контроль работы с информацией
Обс	Участие в обсуждении
Пр	Контроль результатов практикума
КТ	Контроль тестовый
Кп	Контроль письменный
КУ	Контроль устный
РЗ	Решение ситуационной задачи

3.3 Виды текущего контроля успеваемости

Текущий контроль	**ТК**
Рубежный контроль	**РК**

Текущий контроль проводится на семинарских занятиях путем устного и письменного опроса.

Рубежный контроль **-** проводится на контрольной работе или коллоквиуме и направлен на всестороннюю оценку закрепления студентами теоретических знаний и навыков по одному или нескольким разделам рабочей программы и включает 5-7 заданий (для письменной работы) или 2-3 теоретических вопроса (для коллоквиума) по разделам дисциплины, включенным в тему контрольной работы или коллоквиума.

3.4. Структура текущего контроля

Таблица 4. Структура текущего контроля

№ п/п	**№ семестра**	**Наименование раздела учебной дисциплины**	**Виды контроля и аттестации (ТК, РК)**	**Оценочные средства**		
				Форма	**Количество вопросов в задании**	**Количество независимых вариантов**

1	**3**	Тема 1. Основные понятия и определе-ния в области информационной безопасности	ТК	Обс, Пр, КУ, РЗ, КП	5	5
			РК	КУ, КП	5	5
2	**3**	Тема 2. Угрозы информационной безопасности. Кана-лы утечки информа-ции	ТК	Обс, Пр, КУ, РЗ, КП	5	5
			РК	КУ, КП	5	55
3	**3**	Тема 3. Вредоносное ПО. Компьютерные вирусы и средства защиты от них.	ТК	Обс, Пр, РЗ	5	5
			РК	КУ, КП	5	5
4	**4**	Тема 4. Стандарты информационной безопасности	ТК	Обс, Пр, РЗ	5	5
			РК	КУ, КП	5	5
5	**4**	Тема 5. Административный уровень информационной безопасности	ТК	Обс, Пр, РЗ	5	5
			РК	КУ, КП	5	5
6	**4**	Тема 6. Процедурный уровень информационной безопасности .	ТК	Обс, Пр, КУ, РЗ, КП	5	4
			РК	КУ, КП	5	5
	4	Тема 7. Программно-технические методы защиты информационной безопасности	ТК	Обс, Пр, КУ, РЗ, КП	5	5
			РК			

3.5. Методические указания для обучающихся по освоению дисциплины

Обучение складывается из аудиторных занятий, включающих лекционный курс и практические занятия, и самостоятельной работы. Основное учебное время уделяется изучению теоретической части предмета, а также изучению методов решения задач.

При изучении учебной дисциплины необходимо использовать лекционный материал, основную учебную литературу.

В соответствии с требованиями ФГОС ВО в учебном процессе широко используются активные и интерактивные формы проведения занятий, включающие имитационные технологии (взаимоконтроль и взаимооценка знаний студентами, решение ситуационных задач) и неимитационные технологии (дискуссии). Удельный вес занятий, проводимых в интерактивных формах, составляет не менее 30% от аудиторных занятий.

Самостоятельная работа студентов подразумевает подготовку к занятиям, контрольным, зачетам и экзаменам, и включает в себя работу с учебной литературой, поиск научной информации. Работа с учебной литературой рассматривается как вид учебной работы по дисциплине и выполняется в пределах часов, отводимых на её изучение (в разделе СРС).

Каждый обучающийся обеспечен доступом к библиотечным фондам Института. По каждому разделу учебной дисциплины разработаны методические рекомендации для студентов и методические указания для преподавателей.

Текущий контроль усвоения предмета определяется собеседованием в ходе занятий, при решении типовых ситуационных задач.

Самостоятельная работа:

Внеаудиторная СРС по дисциплине «Защита информации» включает, в частности, следующие виды деятельности:

– проработку учебного материала (по конспектам, учебной и научной литературе);

– изучение тем теоретического курса, запланированных для самостоятельного освоения;

– подготовку к выполнению и сдаче лабораторных работ;

– подготовку к мероприятиям текущего контроля, зачетам и экзаменам;

– участие в выполнении коллективных проектов учебного назначения;

СР01. Подготовить к представлению доклад на заданную преподавателем тему, проиллюстрированный презентационным материалом для участия в лекции-конференции.

4. ПЕРЕЧЕНЬ УЧЕБНОЙ ЛИТЕРАТУРЫ, ИНФОРМАЦИОННЫХ РЕСУРСОВ И ТЕХНОЛОГИЙ

4.1.Перечень основной литературы

1. Булычёв, Г. Г. Программно-аппаратные средства защиты информации : учебно-методическое пособие / Г. Г. Булычёв. — Москва : РТУ МИРЭА, 2022 — Часть 1 — 2022. — 203 с. — ISBN 978-5-7339-1652-1. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/310781 (дата обращения: 20.10.2024). — Режим доступа: для авториз. пользователей.
2. Белов А. С. Модернизация системы информационной безопасности = Modernization of the Information Security System: The Approach to Determining the Frequency: подход к определению периодичности / А. С. Белов, М. М. Добрышин, Д. Е. Шугуров // Защита информации. Инсайд. - 2022. - № 4. - С. 76-
3. . Внуков, А. А. Защита информации : учебное пособие для вузов / А. А. Внуков. — 3-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2023. — 161 с. — (Высшее образование). — ISBN 978-5-534-07248-8. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https:// urait.ru/ bcode/512268 (дата обращения: 02.02.2023)
4. Бахаров, Л. Е. Информационная безопасность и защита информации : учебное пособие / Л. Е. Бахаров. — Москва : МИСИС, 2015. — 43 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/116711 (дата обращения: 20.10.2024). — Режим доступа: для авториз. пользователей.

Перечень дополнительной литературы

5. Алгоритм выявления угроз информационной безопасности в распределенных мультисервисных сетях органов государственного управления / А. Ю. Пучков, А. М. Соколов, С. С. Широков, Н. Н. Прокимнов // Прикладная информатика. - 2023. - Т. 18, № 2. - С. 85-102.
6. Васильев В. И. Оценка актуальных угроз безопасности информации с помощью технологии трансформеров / В. И. Васильев, А. М. Вульфин, Н. В. Кучкарова // Вопросы кибербезопасности. - 2022. - № 2. - С. 27-38.
7. Гладких А. В. Методы защиты от DDoS –атак в интеллектуальных сетях / А. В. Гладких // Цифровая трансформация общества и информационная безопасность : материалы Всеросс. науч.-практ. конф. (Екатеринбург, 18 мая 2022 г.) - Екатеринбург, 2022. - С. 3-5.
8. Голубев Г. Д. Обзор безопасности маломощных глобальных сетей: угрозы, проблемы и потенциальные решения / Г. Д. Голубев // Цифровая трансформация общества и информационная безопасность : материалы Всеросс. науч.-практ. конф. (Екатеринбург, 18 мая 2022 г.) - Екатеринбург, 2022. - С. 5-11.

9. Голубев Г. Д. Обзор безопасности маломощных глобальных сетей: угрозы, проблемы и потенциальные решения / Г. Д. Голубев // Цифровая трансформация общества и информационная безопасность : материалы Всеросс. науч.-практ. конф. (Екатеринбург, 18 мая 2022 г.) - Екатеринбург, 2022. - С. 5-11.

10. Щеглов, А. Ю. Защита информации: основы теории : учебник для вузов / А. Ю. Щеглов, К. А. Щеглов. — Москва : Издательство Юрайт, 2023. — 309 с. — (Высшее образование). — ISBN 978-5-534-04732-5. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https:// urait.ru/ bcode/511998 (дата обращения: 02.02.2023).

11. Казарин, О. В. Программно- аппаратные средства защиты информации. Защита программного обеспечения : учебник и практикум для вузов / О. В. Казарин, А. С. Забабурин. — Москва : Издательство Юрайт, 2023. — 312 с. — (Высшее образование). — ISBN 978-5-9916-9043-0. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/513300 (дата обращения: 02.02.2023).

12.Баринова А. Как HR-у самостоятельно провести обучение по информационной безопасности: готовый конспект лекций по главным угрозам / А. Баринова // Директор по персоналу. - 2022. - № 5. - С. 40-45.

13.Бахаров, Л. Е. Информационная безопасность и защита информации : учебное пособие / Л. Е. Бахаров. — Москва : МИСИС, 2015. — 43 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/116711 (дата обращения: 20.10.2024). — Режим доступа: для авториз. пользователей.

4.2. Интернет-ресурсы, в том числе современные профессиональные базы данных и информационные справочные системы:

1. Электронная информационно-образовательная среда АНО ВПО "СЗТУ"

(ЭИОС СЗТУ) [Электронный ресурс]. - Режим доступа: http://edu.nwotu.ru/

2. Электронная библиотека АНО ВПО "СЗТУ" [Электронный ресурс]. - Режим доступа: http://lib.nwotu.ru:8087/jirbis2/

3. Электронно-библиотечная система IPRbooks [Электронный ресурс]. - Режим доступа: http://www.iprbookshop.ru/

4. Информационная система "Единое окно доступа к образовательным ресурсам" [Электронный ресурс]. - Режим доступа: http://window.edu.ru/

5. Информационная системы доступа к электронным каталогам библиотек

сферы образования и науки (ИС ЭКБСОН) [Электронный ресурс]. – Режим доступа: http://www.vlibrary.ru/

Ресурсы электронной информационно-образовательной среды института представлены в локальном нормативном акте «Положение об электронной информационно-образовательной среде РОСБИОТЕХ

Электронные образовательные ресурсы, к которым обеспечен доступ обучающихся, в т.ч. приспособленные для использования инвалидами и лицами с ограниченными возможностями здоровья, приведены на официальном сайте института в разделе «Об институте» - «Сведения об образовательной организации» - «Материально-техническое обеспечение и оснащенность образовательного процесса».

5. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ

К современному специалисту общество предъявляет достаточно широкий перечень требований, среди которых немаловажное значение имеет наличие у выпускников определенных способностей и умений самостоятельно добывать знания из различных источников, систематизировать полученную информацию, давать оценку конкретной ситуации. Формирование такого умения происходит в течение всего периода Вашего обучения через участие в практических занятиях, выполнение контрольных заданий и тестов. При этом Ваша самостоятельная работа играет решающую роль в ходе всего учебного процесса.

Успешное освоение компетенций, формируемых данной учебной дисциплиной, предполагает оптимальное использование Вами времени самостоятельной работы. Целесообразно посвящать до 20 минут изучению конспекта лекции в тот же день после лекции и за день перед лекцией. Теоретический материал изучать в течение недели до 2 часов, а готовиться к практическому занятию по дисциплине до 1.5 часов.

На каждую лекцию, а также на каждое практическое занятие в рамках самостоятельной работы предусмотрена индивидуальная подготовка студентов, для закрепления лекционного материала, изучения некоторых вопросов, заданных лектором для самостоятельного изучения и решения задач для самостоятельного закрепления учебного материала.

Для самостоятельной работы используется учебно-методическое обеспечение в виде учебников, учебных и учебно-методических пособий из рекомендуемого списка, в том числе на электронных носителях и Интернет-ресурсы. Тематика самостоятельной работы соответствует содержанию разделов и тем дисциплины.

В индивидуальных случаях с целью углубленного изучения материала дисциплины тематика самостоятельной работы может несколько расширять рамки содержания тем дисциплины.

Виды самостоятельной работы обучаемых:

- проработка конспектов лекций;
- изучение дополнительных учебных вопросов по дополнительным источникам, в том числе Интернет-ресурсам;
- выполнение практических заданий (решение задач, выполнение упражнений) в рамках содержания разделов и тем дисциплины, в том числе с использованием ПЭВМ;
- выполнение творческих заданий (формулировка и формализация новых задач в различных областях применения методов теории информации и кодирования; подготовка и написание рефератов; разработка алгоритмов и программ, реализующих методы информационного анализа систем и теории кодирования) по отдельным вопросам для углубленного изучения дисциплины.

Формы контроля самостоятельной работы обучаемых: выборочный опрос или письменная контрольная работа на аудиторных занятиях по материалам самостоятельной работы обучаемых; проверка отчетов и рефератов; проверка заданий на компьютере.

На самостоятельных занятиях прививается умение организовывать свой труд, приобретать новые знания с использованием учебной литературы и современных информационных образовательных технологий.

Рекомендуется использовать методические указания и материалы по учебной дисциплине, текст лекций, а также электронные пособия, имеющиеся в системе VitaLMS.

Теоретический материал курса становится более понятным, когда дополнительно к прослушиванию лекций Вами изучаются и книги по данной учебной дисциплине. Полезно использовать несколько учебников, однако легче освоить курс, придерживаясь одного учебника и конспекта.

Рекомендуется, кроме «заучивания» материала, добиться понимания изучаемой темы дисциплины. С этой целью после прочтения очередной главы желательно выполнить несколько простых упражнений на соответствующую тему. Кроме того, очень полезно мысленно задать себе и попробовать ответить на следующие вопросы: о чем эта глава, какие новые понятия в ней введены, каков их смысл.

При подготовке к промежуточной аттестации необходимо освоить теоретические положения данной дисциплины, разобрать определения всех понятий и постановки моделей, описывающих процессы, рассмотреть примеры и самостоятельно решить несколько типовых задач из каждой темы. Дополнительно к изучению конспектов лекций необходимо пользоваться учебниками по учебной дисциплине.

6. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ

По всем видам учебной деятельности в рамках дисциплины используются аудитории, оснащенные необходимым специализированным оборудованием.

Таблица 5. Наименования помещения для проведения дисциплины

Наименование специальных помещений	Оснащенность специальных помещений	Перечень лицензионного программного обеспечения
учебная аудитория для проведения занятий семинарского типа, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации, – Компьютерный класс	Мебель: учебная мебель Комплект специализированной мебели: компьютерные столы Технические средства: компьютерная техника, коммуникационное оборудование, обеспечивающее доступ к сети Интернет (проводное соединение и беспроводное соединение по технологии Wi-Fi)	MS Office, Windows; 7-Zip сервисное без ограничений файловый архиватор Java SE (GNU GPL) средства разработки приложений на языке программирования Java Netbeans IDE GNU GPL среда разработки приложений на языке программирования Java Visual Prolog Personal Edition проприетарная (свободное для учебных заведений) среда разработки приложений на языке программирования Пролог StarUML (GNU GPL) средства разработки UML диаграмм DevC++ (GNU GPL) среда разработки приложений на языке программирования C/C++ XAMPP (GNUGPL) сборка веб-сервера (содержит Apache,MariaDB, PHP, Perl)
учебная аудитория для проведения занятий лекционного типов	Мебель: учебная мебель Технические средства: компьютер, принтер, мультимедиа-проектор, проекционный экран	

Для самостоятельной работы обучающихся предусмотрены помещения, укомплектованные специализированной мебелью, оснащенные компьютерной техникой с возможностью подключения к сети «Интернет» и обеспечением доступа в электронную информационно-образовательную среду института.

Таблица 6. Наименование помещений для самостоятельной работы обучающихся

Наименование помещений для самостоятельной работы обучающихся	Оснащенность помещений для самостоятельной работы обучающихся	Перечень лицензионного программного обеспечения
Помещение для самостоятельной работы обучающихся	Мебель: учебная мебель Комплект специализированной мебели: компьютерные столы Оборудование: компьютерная техника с подключением к информационно-коммуникационной сети «Интернет» и доступом в электронную информационно-образовательную среду образовательной организации, коммуникационное оборудование, обеспечивающее доступ к сети интернет (проводное соединение и беспроводное соединение по технологии Wi-Fi)	ОС Windows Pro 10, MS Office Home and Student, антивирус и свободным ПО - PostgreSQL, R, JuliaPro, PyMol, BioPython, SigmaPlot

7. ТЕКУЩИЙ КОНТРОЛЬ УСПЕВАЕМОСТИ И ПРОМЕЖУТОЧНАЯ АТТЕСТАЦИЯ

Проверка достижения результатов обучения по дисциплине осуществляется в рамках текущего контроля успеваемости и промежуточной аттестации.

7.1. Текущий контроль успеваемости

Текущий контроль успеваемости включает в себя мероприятия по оцениванию выполнения лабораторных работ, заданий для самостоятельной работы. Мероприятия текущего контроля успеваемости приведены в таблице 7.1.

7.2. Промежуточная аттестация

Формы промежуточной аттестации по дисциплине приведены в таблице 7.2.

Таблица 7. Формы промежуточной аттестации

Обозначение	Форма отчетности	Очная
Экз01	экзамен	7 семестр

8. ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

8.1. Оценочные средства

Оценочные средства соотнесены с результатами обучения по дисциплине и индикаторами достижения компетенций.

ОПК-3 Способен решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности

ОПК -8 Способен разрабатывать алгоритмы и программы, пригодные для практического применения

Вопросы к промежуточной аттестации по итогам освоения дисциплины:

1.Какие требования необходимо выполнять при экранировании помещений, предназначенных для размещения вычислительной техники?
2.Какой процесс называется аутентификацией пользователя?
3.Какие схемы аутентификации вы знаете?
4.Что такое смарт-карты?
5.Какие требования предъявляются к современным криптографическим системам защиты информации?
6.Что такое симметричная криптосистема?
7.Какие виды симметричных криптосистем существуют?
8.Что такое асимметричная криптосистема?
9.Что понимается под односторонней функцией?
10.Как классифицируются криптографические алгоритмы по стойкости?
11.В чем заключается анализ надежности криптосистем?
12.Что такое дифференциальный криптоанализ?
13.В чем сущность криптоанализа со связанными ключами?
14.В чем сущность линейного криптоанализа?
15.Какие атаки изнутри вы знаете?
16.Какая программа называется логической бомбой?
17.Какими способами можно проверить систему безопасности?
18.Что является основными характеристиками технических средств защиты информации?
19. Что такое информационная безопасность?
20. Какие предпосылки и цели обеспечения информационной безопасности?
21. В чем заключаются национальные интересы РФ в информационной сфере?
22. Что включает в себя информационная борьба?
23. Какие пути решения проблем информационной безопасности РФ существуют?
24. Каковы общие принципы обеспечения защиты информации?

25. Какие имеются виды угроз информационной безопасности предприятия (организации)?
26. Какие источники наиболее распространенных угроз информационной безопасности существуют?
27. Какие виды сетевых атак имеются?
28.Какими способами снизить угрозу сниффинга пакетов?
29.Какие меры по устранению угрозы IP -спуфинга существуют?
30.Что включает борьба с атаками на уровне приложений?
31.Какие существуют проблемы обеспечения безопасности локальных вычислительных сетей?
32.В чем заключается распределенное хранение файлов?
33.Что включают в себя требования по обеспечению комплексной системы информационной безопасности?
34.Какие уровни информационной защиты существуют, их основные составляющие?
35.В чем заключаются задачи криптографии?
36.Зачем нужны ключи?
37.Какая схема шифрования называется многоалфавитной подстановкой?
38.Какие системы шифрования вы знаете?
39.Что включает в себя защита информации от несанкционированного доступа?
40.В чем заключаются достоинства и недостатки программно-аппаратных средств защиты информации?
41.Какие виды механизмов защиты могут быть реализованы для обеспечения идентификации и аутентификации пользователей?
42.Какие задачи выполняет подсистема управления доступом?
25.Какие требования предъявляются к подсистеме протоколирования аудита?
43.Какие виды механизмов защиты могут быть реализованы для обеспечения конфиденциальности данных и сообщений?
44.В чем заключается контроль участников взаимодействия?
45.Какие функции выполняет служба регистрации и наблюдения?
46.Что такое информационно-опасные сигналы, их основные параметры?
47.Какие требования предъявляются к автоматизированным системам защиты третьей группы?
48.Какие требования предъявляются к автоматизированным системам защиты второй группы?
50.Какие требования предъявляются к автоматизированным системам защиты первой группы?
51.Какие классы защиты информации от несанкционированного доступа для средств вычислительной техники имеются? От чего зависит выбор класса защищенности?
52.Какие требования предъявляются к межсетевым экранам?
53.Какие имеются показатели защищенности межсетевых экранов?
54.Какие атаки системы снаружи вы знаете?

55.Какая программа называется вирусом?
56.Какая атака называется атакой отказа в обслуживании?
57.Какие виды вирусов вы знаете?
58.Какие вирусы называются паразитическими?
59.Как распространяются вирусы?
60.Какие методы обнаружения вирусов вы знаете?
61.Какая программа называется монитором обращения?
62.Что представляет собой домен?
63.Как осуществляется защита при помощи ACL -списков?
64.Какой список называется перечнем возможностей?
65.Какие способы защиты перечней возможностей вы знаете?
66.Из чего состоит высоконадежная вычислительная база (TCB)?
67.Какие модели многоуровневой защиты вы знаете?
68.В чем заключается организация работ по защите от несанкционированного доступа интегрированной информационной системы управления предприятием?
69.Какие характеристики положены в основу системы классификации информационных систем управления предприятием?
70.Какие задачи решает система компьютерной безопасности?
71.Какие пути защиты информации в локальной сети существуют?
72.Какие задачи решают технические средства противодействия экономическому шпионажу?
73.Какой порядок организации системы видеонаблюдения?
74.Что включает в себя защита информационных систем с помощью планирования?
75.Какие условия работы оцениваются при планировании?
76.Из каких этапов состоят работы по обеспечению информационной безопасности предприятия?
77.Что такое мобильные программы?
78.Что такое концепция потоков?
79.Что представляет собой метод «песочниц»?
80.Что такое интерпретация?
81.Что такое программы с подписями?
82.Что представляет собой безопасность в системе Java ?
83.Назовите несколько примеров политик безопасности пакета JDK 1.2?
84.Какие международные документы регламентируют деятельность по обеспечению защиты информации?
85.Что понимают под политикой информационной безопасности?
86.Что включает в себя политика информационной безопасности РФ?
87.Какие нормативные документы РФ определяют концепцию защиты информации?

Приблизительные темы контрольных работ

1 Угрозы информационной безопасности предприятия (организации) и способы борьбы с ними
2 Современные средства защиты информации

3 Современные системы компьютерной безопасности
4 Современные средства противодействия экономическому шпионажу
5 Современные криптографические системы
6 Криптоанализ, современное состояние
7 Правовые основы защиты информации
8 Технические аспекты обеспечения защиты информации. Современное состояние
9 Атаки на систему безопасности и современные методы защиты
8
10 Современные пути решения проблемы информационной безопасности РФ

Приблизительные вопросы практического содержания

1. Угрозы информационной безопасности предприятия (организации) и способы борьбы с ними
2. Современные средства защиты информации
3. Современные системы компьютерной безопасности
4. Современные средства противодействия экономическому шпионажу 5. Современные криптографические системы

Приблизительные вопросы тестового содержания

1.1. Существенными признаками понятия «информационная безопасность» являются:

а) конфиденциальность;
б) секретность;
в) устойчивость к взлому;
г) целостность;
д) надежность;
е) доступность.

1.2. Сведения о лицах, предметах, фактах, событиях, явлениях и процессах независимо от формы их представления – это:

а) документированная информация;
б) информация;
в) конфиденциальная информация;
г) документ.

1.3. К информационным процессам относятся:

а) создание информации;

б) защита информации;

в) сбор информации;

г) обработка информации;

д) накопление информации;

е) поиск информации.

1.4. Свойство информации, значение которого устанавливается владельцем информации и отражает ограничение доступа к ней, – это:

а) конфиденциальность;

б) целостность;

в) доступность;

г) достоверность.

1.5. По конечному проявлению различают следующие угрозы информации (выберите несколько ответов):

а) блокирование;

б) ознакомление;

в) структурирование;

г) взлом;

д) модификация;

е) уничтожение.

Таблица 8.1 – Критерии оценивания мероприятий текущего контроля успеваемости

Наименование, обозначение	Показатель
Доклад	тема доклада раскрыта, сформулированы выводы; соблюдены требования к объему и оформлению доклада (презентации к докладу);
Отчет	тема раскрыта; использованы рекомендуемые источники; соблюдены требования к объему и оформлению отчета

При оценивании результатов обучения по дисциплине в ходе промежуточной аттестации используются следующие критерии и шкалы.

Зачет

Критерии оценивания зачёта:

Оценка «зачтено» выставляется, если студент твёрдо знает материал, грамотно и по существу излагает его, не допуская существенных неточностей в ответе на вопрос, правильно применяет теоретические положения при решении практических вопросов и задач, владеет необходимыми знаниями, умениями и навыками. 1

Оценка «не зачтено» выставляется, если студент не знает значительной части программного материала, допускает существенные ошибки, неуверенно, с большими затруднениями выполняет практические работы. 1

Также оценка «зачтено» может выставляться на основе успешных ответов на практических занятиях, выполненных домашних заданий и контрольных работ, отсутствия у обучающегося пропущенных или неотработанных занятий до проведения зачёта. 1

Экзамен (Экз01).

Задание состоит из 2 теоретических вопросов и 1 практического задания.

Время на подготовку: 60 минут.

Оценка «отлично» выставляется обучающемуся, если он глубоко и прочно усвоил программный материал, исчерпывающе, последовательно, четко и логически стройно его излагает, умеет тесно увязывать теорию с практикой, свободно справляется с задачами, вопросами и другими видами применения знаний, не затрудняется с ответом при видоизменении заданий, использует в ответе материал рекомендуемой литературы, правильно обосновывает принятое решение, владеет разносторонними навыками и приемами выполнения практических заданий.

Оценка «хорошо» выставляется обучающемуся, если он твердо знает программный материал, грамотно и по существу излагает его, не допуская существенных неточностей в ответах на вопросы, правильно применяет теоретические положения при решении практических заданий, владеет необходимыми навыками и приемами их выполнения.

Оценка «удовлетворительно» выставляется обучающемуся, если он имеет знания только основного материала, но не усвоил его деталей, допускает неточности, недостаточно правильные формулировки, нарушения логической последовательности в изложении программного материала, испытывает затруднения при выполнении практических работ.

Оценка «неудовлетворительно» выставляется обучающемуся, который не знает значительной части программного материала, допускает существенные ошибки в ответах на вопросы, неуверенно, с большими затруднениями выполняет практические задания.

Результат обучения по дисциплине считается достигнутым при получении обучающимся оценки «зачтено», «удовлетворительно», «хорошо», «отлично» по каждому из контрольных мероприятий, относящихся к данному результату обучения.

Особенности организации обучения лиц с ОВЗ и инвалидов

Для инвалидов и лиц с ОВЗ может изменяться объём дисциплины (модуля) в часах, выделенных на контактную работу обучающегося с преподавателем (по видам учебных занятий) и на самостоятельную работу обучающегося (при этом не увеличивается количество зачётных единиц, выделенных на освоение дисциплины).

Фонды оценочных средств адаптируются к ограничениям здоровья и восприятия информации обучающимися. Основные формы представления оценочных средств – в печатной форме или в форме электронного документа.

Формы контроля и оценки результатов обучения инвалидов и лиц с ОВЗ

Категории студентов с ОВЗ и инвалидностью	
С нарушением зрения	- устная проверка: дискуссии, тренинги, круглые столы, собеседования, устные коллоквиумы и др.; - с использованием компьютера и специального ПО: работа с электронными образовательными ресурсами, тестирование, рефераты, курсовые проекты, дистанционные формы, если позволяет острота зрения - графические работы и др.; - при возможности письменная проверка с использованием рельефно- точечной системы Брайля, увеличенного шрифта, использование специальных технических средств (тифлотехнических средств): контрольные, графические работы, тестирование, домашние задания, эссе, отчеты и др.
С нарушением слуха	– письменная проверка: контрольные, графические работы, тестирование, домашние задания, эссе, письменные коллоквиумы, отчеты и др.; – с использованием компьютера: работа с электронными образовательными ресурсами, тестирование, рефераты, курсовые проекты, графические работы, дистанционные формы и др.; - при возможности устная проверка с использованием специальных технических средств (аудиосредств, средств коммуникации, звукоусиливающей аппаратуры и др.): дискуссии, тренинги, круглые столы, собеседования, устные коллоквиумы и др
С нарушением опорно- двигательного аппарата	– письменная проверка с использованием специальных технических средств (альтернативных средств ввода, управления компьютером и др.): контрольные, графические работы, тестирование, домашние задания, эссе, письменные коллоквиумы, отчеты и др.; – устная проверка, с использованием специальных технических средств (средств коммуникаций): дискуссии, тренинги, круглые столы, собеседования, устные коллоквиумы и др.; – с использованием компьютера и специального ПО (альтернативных средств ввода и управления компьютером и др.): работа с электронными образовательными ресурсами, тестирование, рефераты, курсовые проекты, графические работы, дистанционные формы предпочтительнее обучающимся, ограниченным в передвижении и др.

В ходе проведения промежуточной аттестации предусмотрено:

– предъявление обучающимся печатных и (или) электронных материалов в формах, адаптированных к ограничениям их здоровья;

– возможность пользоваться индивидуальными устройствами и средствами, позволяющими адаптировать материалы, осуществлять приём и передачу информации с учетом их индивидуальных особенностей;

– увеличение продолжительности проведения аттестации;

– возможность присутствия ассистента и оказания им необходимой помощи (занять рабочее место, передвигаться, прочитать и оформить задание, общаться с преподавателем).

Адаптация условий обучения, учебных материалов и особенности их использования.

Варианты адаптации задания могут быть разными и касаться разных его аспектов: формы задания, инструкции к заданию, его объема, уровня сложности, содержания.

При нарушениях слуха:

1. При организации образовательного процесса необходима особая фиксация на артикуляции выступающего, следует говорить громче и четче, подбирая подходящий уровень;

2. Процесс обучения требует использования дополнительных приемов для повышения эффективности запоминания материала;

3. Некоторые основные понятия изучаемого материала студентам с нарушенным слухом необходимо объяснять дополнительно. На занятиях требуется уделять повышенное внимание специальным профессиональным терминам, а также использованию профессиональной лексики. Для лучшего усвоения слабослышащими специальной терминологии необходимо каждый раз писать на доске используемые термины и контролировать их усвоение;

4. В процессе обучения рекомендуется использовать разнообразный наглядный материал. Сложные для понимания темы должны быть снабжены как можно большим количеством наглядного материала.;

5. Создание текстовых средств учебного назначения для студентов с нарушенным слухом требует участия сурдопереводчика;

6. Применение поэтапной системы контроля, текущего и промежуточного, способствует непрерывной аттестации студентов;

7. Сочетание всех видов речевой деятельности (говорения, слушания, чтения, письма, дактилирования, зрительного восприятия с лица и с руки говорящего);

8. Соблюдение слухоречевого режима на каждом занятии;

9. Использование информационных технологий, в том числе учебно-методических презентаций, контролирующих и контрольно-обучающих программ, которые проектируются по общей технологической схеме;

10. Сокращения объема записей за счет использования опорных конспектов, различных схем, придающих упрощенный схематический вид изучаемым понятиям.

При нарушении зрения:

1. Наличие альтернативной версии официального сайта организации в информационно-телекоммуникационной сети "Интернет" для слабовидящих;

2. Размещение в доступных для обучающихся, являющихся слепыми или слабовидящими, местах и в адаптированной форме (с учетом их особых потребностей) справочной информации о расписании учебных занятий (информация должна быть выполнена крупным рельефно-контрастным шрифтом (на белом или желтом фоне) и продублирована шрифтом Брайля);

3. Использование чёткого и увеличенного по размеру шрифта и графических объектов в мультимедийных презентациях;

4. Озвучивание визуальной информации, представленной обучающимся в ходе занятий

5. Обеспечение особого речевого режима преподавания: лекции читаются громко, разборчиво, отчётливо, с паузами между смысловыми блоками информации, обеспечивается интонирование, повторение, акцентирование, профилактика рассеивания внимания;

6. Присутствие ассистента, оказывающего обучающемуся необходимую помощь;

7. Обеспечение выпуска альтернативных форматов печатных материалов (крупный шрифт или аудиофайлы);

8. Обеспечение доступа обучающегося, являющегося слепым и использующего собаку-проводника, к зданию организации.

При нарушении опорно-двигательного аппарата:

1. Материально-технические условия обеспечивают возможность беспрепятственного доступа обучающихся в учебные помещения, столовые, туалетные и другие помещения организации, а также пребывания в указанных помещениях (наличие пандусов, поручней, расширенных дверных проемов, лифтов, локальное понижение стоек-барьеров, наличие специальных кресел и других приспособлений);

2. При работе со студентами с нарушением опорно-двигательного аппарата используются методы, активизирующие познавательную деятельность обучающихся, развивающие устную и письменную речь и формирующие необходимые учебные навыки;

3. Габариты рабочего стола соответствуют эргономическим требованиям работы инвалида на коляске и функциональным требованиям выполнения рабочих операций в пределах зоны досягаемости;

4. Применение дополнительных средств активизации процессов запоминания и повторения;

5. Наличие чёткой системы и алгоритма организации самостоятельных работ и проверки заданий с обязательной корректировкой и комментариями;

6. Увеличение доли методов социальной стимуляции (обращение внимания, апелляция к ограничениям по времени, контактные виды работ, групповые задания др.

7. Наличие возможности использовать индивидуальные устройства и средства, позволяющие обеспечить реализацию эргономических принципов и комфортное пребывание на месте в течение всего периода учёбы (подставки, специальные подушки и др.).