Приложение 4

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

федеральное государственное автономное
образовательное учреждение высшего образования
«Национальный исследовательский Нижегородский государственный университет
им. Н.И. Лобачевского»

Арзамасский филиал ННГУ - Факультет естественных и математических наук

УТВЕРЖДЕНО

решением президиума Ученого совета ННГУ

протокол № 1 от 16.01.2024 г.

Рабочая программа дисциплины

Информационная безопасность

Уровень высшего образования
Бакалавриат

Направление подготовки / специальность
09.03.03 - Прикладная информатика

Направленность образовательной программы
Системное и прикладное программирование

Форма обучения
очная, очно-заочная

г. Арзамас

2024 год начала подготовки

1. Место дисциплины в структуре ОПОП

Дисциплина Б1.О.22 Информационная безопасность относится к обязательной части образовательной программы.

2. Планируемые результаты обучения по дисциплине, соотнесенные с планируемыми результатами освоения образовательной программы (компетенциями и индикаторами достижения компетенций)

Формируемые компетенции (код, содержание компетенции)	**Планируемые результаты обучения по дисциплине (модулю), в соответствии с индикатором достижения компетенции**		**Наименование оценочного средства**	
	Индикатор достижения компетенции (код, содержание индикатора)	**Результаты обучения по дисциплине**	**Для текущего контроля успеваемости**	**Для промежуточной аттестации**
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-3.1: Демонстрирует знание принципов, методов и средств решения стандартных задач профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности.* *ОПК-3.2: Демонстрирует умение применять информационно-коммуникационные технологии решения стандартных задач профессиональной деятельности на основе информационной и библиографической культуры с учетом основных требований информационной безопасности.* *ОПК-3.3: Имеет практический опыт решения стандартных задач профессиональной деятельности с соблюдением требований информационной безопасности.*	*ОПК-3.1:* *Знать принципы, методы и средства решения стандартных задач профессиональной деятельности* *Уметь выбрать принципы, методы и средства решения стандартных задач профессиональной деятельности* *Владеть навыками применения методов и средств решения стандартных задач профессиональной деятельности* *ОПК-3.2:* *Знать принципы решения стандартных задач профессиональной деятельности* *Уметь выбрать способы решения задач профессиональной деятельности* *Владеть навыками выбора способа решения задач профессиональной деятельности* *ОПК-3.3:* *Знать особенности подготовки обзоров, аннотаций, составления*	*Задания* *Практическое задание* *Реферат* *Тест*	*Зачёт:* *Контрольные вопросы*

		рефератов, научных докладов, публикаций, и библиографии по научно-исследовательской работе с учетом требований информационной безопасности *Уметь подготовить обзоры, аннотации, рефераты, научные публикации, и библиографию по научно-исследовательской работе с учетом требований информационной безопасности* *Владеть навыками подготовки обзоров, аннотаций, составления рефератов, научных докладов, публикаций, и библиографии по научно-исследовательской работе с учетом требований информационной безопасности*		
ОПК-4: Способен участвовать в разработке стандартов, норм и правил, а также технической документации, связанной с профессиональной деятельностью;	*ОПК-4.1: Демонстрирует знание основных стандартов, норм и правил оформления технической документации на различных стадиях проектирования и поддержки жизненного цикла информационной системы.* *ОПК-4.2: Применяет стандарты, нормы и правила (в том числе установленные самостоятельно) при оформлении технической документации на различных стадиях проектирования и поддержки жизненного цикла информационной системы.* *ОПК-4.3: Имеет практический опыт разработки технической документации на различных этапах проектирования и поддержки жизненного цикла информационной системы.*	*ОПК-4.1:* *Знать принципы выбора основной нормативно-справочной документации при разработке ИС* *Уметь выбирать основные стандарты оформления технической документации на различных стадиях жизненного цикла информационной системы* *Владеть навыками применения нормативно-справочной документации при разработке ИС* *ОПК-4.2:* *Знать инструменты выбора стандартов оформления технической документации на различных стадиях жизненного цикла информационной системы* *Уметь выбирать стандарты оформления технической документации на различных стадиях жизненного цикла информационной системы* *Владеть навыками*	*Задания* *Практическое задание* *Реферат* *Тест*	*Зачёт:* *Контрольные вопросы*

		использования стандартов оформления технической документации на различных стадиях жизненного цикла информационной системы *ОПК-4.3:* *Знать принципы составления технической документации на различных этапах жизненного цикла информационной системы* *Уметь использовать ПО для составления технической документации на различных этапах жизненного цикла информационной системы* *Владеть навыками составления технической документации на различных этапах жизненного цикла информационной системы*		

3. Структура и содержание дисциплины

3.1 Трудоемкость дисциплины

	очная	**очно-заочная**
Общая трудоемкость, з.е.	**3**	**3**
Часов по учебному плану	**108**	**108**
в том числе		
аудиторные занятия (контактная работа):		
- занятия лекционного типа	**16**	**8**
- занятия семинарского типа (практические занятия / лабораторные работы)	**34**	**8**
- КСР	**1**	**1**
самостоятельная работа	**57**	**91**
Промежуточная аттестация	**0** **Зачёт**	**0** **Зачёт**

3.2. Содержание дисциплины

(структурированное по темам (разделам) с указанием отведенного на них количества академических часов и виды учебных занятий)

Наименование разделов и тем дисциплины	Всего (часы)	в том числе	
		Контактная работа (работа во взаимодействии с преподавателем), часы из них	Самостоятельная работа обучающегося,

			Занятия лекционного типа		Занятия семинарского типа (практические занятия/лабораторные работы), часы		Всего		часы	
	очно	очно-заочно	очно	очно-заочно	очно	очно-заочно	очно	очно-заочно	очно	очно-заочно
Тема 1. Понятие национальной безопасности, виды безопасности. Информационная безопасность РФ.	14	16	2	2	4	0	6	2	8	14
Тема 2. Терминологические основы информационной безопасности. Основные понятия и определения.	14	16	2	2	4	0	6	2	8	14
Тема 3. Общие методологические принципы теория информационной безопасности. Комплексность.	16	16	2	2	6	2	8	4	8	12
Тема 4. Угрозы. Классификация и анализ угроз информационной безопасности.	14	16	2	2	4	2	6	4	8	12
Тема 5. Методы нарушения конфиденциальности, целостности и доступности информации.	16	14	2	0	6	2	8	2	8	12
Тема 6. Причины, виды, каналы утечки и искажения информации.	15	15	2	0	4	2	6	2	9	13
Тема 7. Функции и задачи защиты информации. Проблемы региональной информационной безопасности.	18	14	4	0	6	0	10	0	8	14
Аттестация	0	0								
КСР	1	1					1	1		
Итого	108	108	16	8	34	8	51	17	57	91

Содержание разделов и тем дисциплины

Тема 1. Понятие национальной безопасности, виды безопасности. Информационная безопасность РФ.
Важность информационной безопасности в современном мире и необходимость соблюдения международных стандартов. Понятие угрозы информационной безопасности и ее классификация. Основные виды угроз: вирусы, хакеры, кибератаки и т.д.
Роль международных стандартов в обеспечении информационной безопасности. Основные стандарты и рекомендаций: ISO/IEC 27001, GDPR, HIPAA и др.
Особенности информационной безопасности в России в условиях функционирования глобальных сетей. Анализ законодательной базы и мер по защите информации.
Практические рекомендации по обеспечению информационной безопасности в организации или личной жизни. Разработка стратегии защиты данных и регулярное обновление безопасности.
Тема 2. Терминологические основы информационной безопасности. Основные понятия и определения.
Терминология информационной безопасности: основные понятия и определения. Уровни информационной безопасности. Компоненты информационной безопасности. Классификация информации по степени конфиденциальности. Угрозы информационной безопасности.
Тема 3. Общие методологические принципы теория информационной безопасности. Комплексность.
Информационная безопасность как комплекс мер, направленных на защиту информации от различных угроз. Общие методологические принципы теории информационной безопасности. Принцип комплексности. Принцип системности.
Принцип непрерывности. Принцип адекватности. Правовые, организационные и технические аспекты защиты информации.
Тема 4. Угрозы. Классификация и анализ угроз информационной безопасности.
Угрозы информационной безопасности: определение и классификация. Анализ угроз информационной безопасности на примере конкретных организаций.

Способы предотвращения и минимизации угроз информационной безопасности.
Тема 5. Методы нарушения конфиденциальности, целостности и доступности информации.
Обзор основных видов нарушений информационной системы. Методы защиты от нарушений информационной системы. Работа с инструментами мониторинга безопасности (например, IDS/IPS). Обсуждение случаев реальных нарушений информационной системы и способов их предотвращения.
Тема 6. Причины, виды, каналы утечки и искажения информации.
Причины утечки и искажения информации:
Человеческий фактор. Технические проблемы.
Виды утечки и искажения информации:
Физическая утечка. Техническая утечка. Каналы утечки и искажения информации.
Тема 7. Функции и задачи защиты информации. Проблемы региональной информационной безопасности.
Конфиденциальность информации. Целостность информации. Доступность информации.
Аутентификация пользователей. Шифрование данных
Резервное копирование данных. Управление доступом пользователей к ресурсам системы.
Антивирусная защита. Обнаружение и предотвращение вторжений (IDS/IPS). Защита от утечек информации

4. Учебно-методическое обеспечение самостоятельной работы обучающихся

Самостоятельная работа обучающихся включает в себя подготовку к контрольным вопросам и заданиям для текущего контроля и промежуточной аттестации по итогам освоения дисциплины приведенным в п. 5.

Для обеспечения самостоятельной работы обучающихся используются:
- электронный курс "Информационная безопасность" (не нашел).
Иные учебно-методические материалы: Учебно-методические документы, регламентирующие самостоятельную работу
адреса доступа к документам:
https://arz.unn.ru/sveden/document/
https://arz.unn.ru/pdf/Metod_all_all.pdf

5. Фонд оценочных средств для текущего контроля успеваемости и промежуточной аттестации по дисциплине (модулю)

5.1 Типовые задания, необходимые для оценки результатов обучения при проведении текущего контроля успеваемости с указанием критериев их оценивания:

5.1.1 Типовые задания (оценочное средство - Задания) для оценки сформированности компетенции ОПК-3:

1. Теория защиты информации. Основные направления.
2. Обеспечение информационной безопасности и направления защиты.
3. Комплексность (целевая, инструментальная, структурная, функциональная, временная)
4. Требования к системе защиты информации.
5. Угрозы информации.
6. Виды угроз. Основные нарушения.
7. Характер происхождения угроз.
8. Источники угроз. Предпосылки появления у грог

9. Система защиты информации.
10. Классы каналов несанкционированного получения информации.
11. Причины нарушения целостности информации.
12. Методы и модели оценки уязвимости информации.
13. Общая модель воздействия на информацию.
14. Общая модель процесса нарушения физической целостности информации.
15. Структурированная схема потенциально возможных злоумышленных действий в автоматизированных системах обработки данных.
16. Методологические подходы к оценке уязвимости информации.
17. Модель защиты системы с полным перекрытием.
18. Рекомендации по использованию моделей оценки уязвимости информации.
19. Допущения в моделях оценки уязвимости информации.
20. Методы определения требований к защите информации.
21. Факторы, обусловливающие конкретные требования к защите, обусловленные спецификой автоматизированной обработки информации.
22. Классификация требований к средствам защиты информации.

5.1.2 Типовые задания (оценочное средство - Задания) для оценки сформированности компетенции ОПК-4:

1. Требования к защите, определяемые структурой автоматизированной системы обработки данных.
2. Требования к защите, обусловливаемые видом защищаемой информации.
3. Требования, обусловливаемые взаимодействием пользователя с комплексом средств автоматизации.
4. Анализ существующих методик определения требований к защите информации
5. Стандарт США «Критерии оценки гарантировано защищенных вычислительных систем в интересах Министерства обороны США». Основные положения.
6. О Руководящем документе Гостехкомиссни России «Классификация автоматизированных систем и требований по защите информации», выпущенном в 1992 г. Ч. I.
7. Классы защищенности средств вычислительной техники от несанкционированного доступа.
8. Факторы, влияющие на требуемый уровень защиты информации.
9. Функции и задачи защиты информации. Основные положения механизмов непосредственной зашиты и механизмы управления механизмами непосредственной защиты.
10. Методы формирования функций защиты.
11. События, возникающие при формировании функций защиты,
12. Классы задач функций защиты.
13. Класс задач функций защиты 1 - уменьшение степени распознавания объектов.
14. Класс задач функций защиты 2 - защита содержания обрабатываемой, хранимой и передаваемой информации.
15. Класс задач функций защиты 3 - защита информации от информационного воздействия
16. Функции защиты информации.
17. Стратегии защиты информации.

18. Способы и средства защиты информации.
19. Способы «абсолютной системы защиты*'
20. Архитектура систем защиты информации. Требования.
21. Общеметодологические принципы архитектуры системы защиты информации.
22. Построение средств защиты информации
23. Ядро системы защиты информации
24. Семирубежная модель

Критерии оценивания (оценочное средство - Задания)

Оценка	Критерии оценивания
отлично	Ответ полный и правильный на основании изученной теории; материал изложен в необходимой логической последовательности, грамотный научный язык; ответ самостоятельный
хорошо	Ответ полный и правильный на основании изученной теории; материал изложен в необходимой логической последовательности при этом допущены две-три несущественные ошибки, исправленные по требованию преподавателя
удовлетворительно	Ответ полный, но при этом допущена существенная ошибка или неполный, несвязный ответ.
неудовлетворительно	Ответ обнаруживает непонимание студентом основного содержания учебного материала или допущены существенные ошибки, которые не могут быть исправлены при наводящих вопросах преподавателя

5.1.3 Типовые задания (оценочное средство - Практическое задание) для оценки сформированности компетенции ОПК-3:

Задание № 1. «Безопасность информационных систем»
Вопросы:

1. Что вы представляете под безопасностью информационный системы.
2. Что относиться к основным характеристикам защищаемой информации?
3. Что вы отнесете к информации ограниченного доступа?
4. По каким направлениям будет осуществляться дальнейшее развитие системы безопасности?

Задание:
Определите в каких формах представлена информация на вашей домашней ЭВМ. Опишите, как обеспечивается информационная безопасность вашей ПЭВМ и отвечает ли современным требованиям развития систем безопасности.
Задание № 2. «Информационные и иные угрозы»
Вопросы:

1. Что такое угроза безопасности информации.
2. Приведите примеры программно-математических угроз.

3. Какие организационные угрозы вы знаете. Приведите примеры.
4. Как по вашему мнению возможна утечка информации по физическому каналу в аудиториях информатики филиала?

Задание:

Определите и классифицируйте угрозы безопасности вашего домашнего ПЭВМ.

Задание №3. «Организация защиты информации»

Вопросы:

1. Какие модели защиты информации вы знаете и их основные достоинства и недостатки?
2. Приведите примеры организации защиты информации (см.Таблицу 1)?

Таблица 1. Виды информационного пространства для организации защиты информации по вариантам

№ варианта	Вид информационного пространства для защиты
1, 5, 9 ,13	Корпоративная сеть
2, 6, 10,14	Локальная сеть
3, 7, 11,15	Сеть Internet
4, 8, 12,16	Файловая система

Задание:

В приведенном вами примере организации защиты информации найдите недостатки системы, предложите пути их устранения.

Задание №4. «Удаленное администрирование в сети»

Вопросы:

1. Какие способы аутентификации пользователей могут применяться в компьютерных системах?
2. В чем заключаются недостатки парольной аутентификации и как она может быть усилена?
3. Какова недостатки межсетевых экранов вы можете привести?
4. В чем сущность удаленного администрирования?

Задание:

Предложите схему удаленного администрирования сети филиала. Выбор схемы и соответствующего ПО обоснуйте.

Задание №5. «Безопасность автоматизированной информационной системы»

Вопросы:

1. В чем состоит предмет и объекты защиты информации в АСОД?
2. Что такое надежность информации и ее уязвимость?
3. Перечислите каналы несанкционированного получения информации в АСОД?

4. Каковы методы подтверждения подлинности пользователей и разграничения их доступа к компьютерным ресурсам?
5. Перечислите методы идентификации и установления подлинности субъектов и различных объектов.
6. В чем состоят задачи информационной целостности?
7. Что значит разграничение и контроль доступа к информации?
8. Какие имеются методы и средства защиты информации от случайных воздействий?

Задание:
Опишите каким образом осуществлено разграничение доступа к информационным ресурсам на вашей ПЭВМ, в случае отсутствия его обоснуйте.

5.1.4 Типовые задания (оценочное средство - Практическое задание) для оценки сформированности компетенции ОПК-4:

Задание № 6. «Антивирусная безопасность»
Вопросы:

1. В чем состоит проблема вирусного заражения программ?
2. Приведите пример современного вируса, способы его обнаружения и наносимый ущерб?
3. Какие вредоносные программные закладки кроме вирусов вам известны?
4. Какие существуют методы борьбы с компьютерными вирусами?

Задание:
Раскройте сущность приведенного вируса.

№ варианта	Вид вируса
1, 5, 9 ,13	Стелс-вирус
2, 6, 10,14	Boot- вирус
3, 7, 11,15	Макровирус
4, 8, 12,16	Вирус-червь

Задание № 7. «Антивирусные программы»
Вопросы:

1. Какие основные антивирусные программы вы знаете, кратко охарактеризуйте их.
2. Каким образом происходит лечение зараженных дисков?
3. Что такое программа – полифаг?
4. Что такое программа - детектор?

Задание:

Опишите антивирусные программы, которые вы использовали и используете в данный момент. Ваш выбор обоснуйте.

Задание №8. «Обеспечение технической безопасности»

Вопросы:

1. В чем заключается проблема обеспечения технической безопасности?
2. Приведите примеры отказа аппаратного обеспечения, создающего угрозу информационной безопасности.
3. В чем заключается сущность резервного копирования информации?
4. Какое программное и техническое обеспечение применяется при дублировании информации?
5. Каковы основные аспекты восстановления удаленной информации?
6. Опишите основные программы для восстановления информации?
7. В чем заключается необходимость разбивки жесткого диска на логические и каким программным обеспеченьем можно это произвести?

Задание:

Приведите примеры, когда вам приходилось восстанавливать удаленную информацию. Опишите и обоснуйте логическую разбивку вашего жесткого диска.

Задание №9. «Организационное обеспечение информационной безопасности»

Вопросы:

1. Что входит в понятие организационного обеспечения?
2. Приведите примеры и укажите области применения.
3. Какие основные виды организационного обеспечения безопасности используются в работе филиала.

Задание:

Определите какие организационные меры вы используете в своем быту, приведите примеры использования в учебном процессе.

Задание №10. «Правовое обеспечение информационной безопасности»

Вопросы:

1. Приведите основные законодательные и нормативные документы?
2. Каким образом можно их классифицировать?
3. Каковы перспективы дальнейшего развития в этой области вы видете?

Задание:

Определите какими нормативными документами ограничен круг задач, решаемых вами с использованием вашей домашней ПЭВМ.

Критерии оценивания (оценочное средство - Практическое задание)

Оценка	Критерии оценивания
зачтено	Ответ полный и правильный на основании изученной теории; теоретический материал и решение поставленных задач изложены в необходимой логической последовательности, грамотный научный язык; ответ самостоятельный. Могут быть допущены две-три несущественные ошибки, исправленные по требованию преподавателя

Оценка	Критерии оценивания
не зачтено	Ответ обнаруживает непонимание студентом основного содержания учебного материала или допущены существенные ошибки, которые не могут быть исправлены при наводящих вопросах преподавателя

5.1.5 Типовые задания (оценочное средство - Реферат) для оценки сформированности компетенции ОПК-3:

1. Проблемы информационной безопасности.
2. Основные критерии классификации угроз информационной безопасности..
3. Наиболее распространенные угрозы доступности.
4. Вредоносное программное обеспечение.
5. Основные угрозы целостности.
6. Основные угрозы конфиденциальности.
7. Основные угрозы доступности.
8. Стандарт ISO/IEC 15408 "Критерии оценки безопасности информационных технологий".
9. Административный уровень информационной безопасности.
10. Программа безопасности. Пример для предприятия.
11. Управление рисками.
12. Основные программно-технические меры.

5.1.6 Типовые задания (оценочное средство - Реферат) для оценки сформированности компетенции ОПК-4:

1. Идентификация и аутентификация.
2. Управление доступом.
3. Протоколирование и аудит.
4. Шифрование.
5. Алгоритмы шифрования.
6. Контроль целостности и Цифровые сертификаты.
7. Экранирование.
8. Классификация межсетевых экранов.
9. Туннелирование и управление доступом.
10. Информационная безопасность личности, общества, государства
11. Обеспечение информационной безопасности в сетях IP
12. Стандартизация в области информационной безопасности в сетях передачи данных
13. Стратегия обеспечения Информационной Безопасности предприятия

Критерии оценивания (оценочное средство - Реферат)

Оценка	Критерии оценивания
отлично	реферативная работа полностью раскрывает основные вопросы теоретического материала. Студент приводит информацию из первоисточников и изданий периодической печати, приводит практические примеры, в докладе отвечает на дополнительные вопросы преподавателя и

Оценка	Критерии оценивания
	студентов
хорошо	реферативная работа частично раскрывает основные вопросы теоретического материала. Студент приводит информацию из первоисточников, отвечает на дополнительные вопросы преподавателя и студентов (при докладе), но при этом дает не четкие ответы, без достаточно их аргументации
удовлетворительно	реферативная работа в общих чертах раскрывает основные вопросы теоретического материала. Студент приводит информацию только из учебников. При ответах на дополнительные вопросы в докладе путается в ответах, не может дать понятный и аргументированный ответ
неудовлетворительно	ставится за рефераты, в которых нет информации о проблематике работы и ее месте в контексте других работ по исследуемой теме.

5.1.7 Типовые задания (оценочное средство - Тест) для оценки сформированности компетенции ОПК-3:

Вопрос 1. Защита информации от утечки включает в себя следующие мероприятия:
а) защиту информации от разглашения;
б) защиту информации от несанкционированного воздействия;
в) защиту информации от непреднамеренного воздействия;
г) защиту информации от несанкционированного доступа.
Вопрос 2. Деятельность, направленная на предотвращение получения защищаемой информации заинтересованным субъектом с нарушением установленных правовыми документами или собственником, владельцем информации прав или правил доступа к защищаемой информации – это:
а) защита информации от несанкционированного воздействия;
б) защита информации от непреднамеренного воздействия;
в) защита информации от разглашения;
г) защита информации от несанкционированного доступа.
Вопрос 3. Дайте определение конфиденциальности информации.
а) гарантия доступа санкционированных пользователей к информации;
б) обеспечение надежной идентификации источника сообщения, а также гарантия того, что источник не является поддельным;
в) обеспечение неизменности информации при ее передаче;
г) обеспечение просмотра информации в приемлемом формате только для пользователей, имеющих право доступа к этой информации.
Вопрос 4. Модификация передаваемой информации со стороны третьего лица приводит к нарушению:
а) конфиденциальности передаваемой информации;
б) доступности информации;
в) аутентичности передаваемой информации;
г) конфиденциальности и целостности передаваемой информации.

Вопрос 5. К какому уровню модели взаимодействия открытых систем относится фильтрующий маршрутизатор?

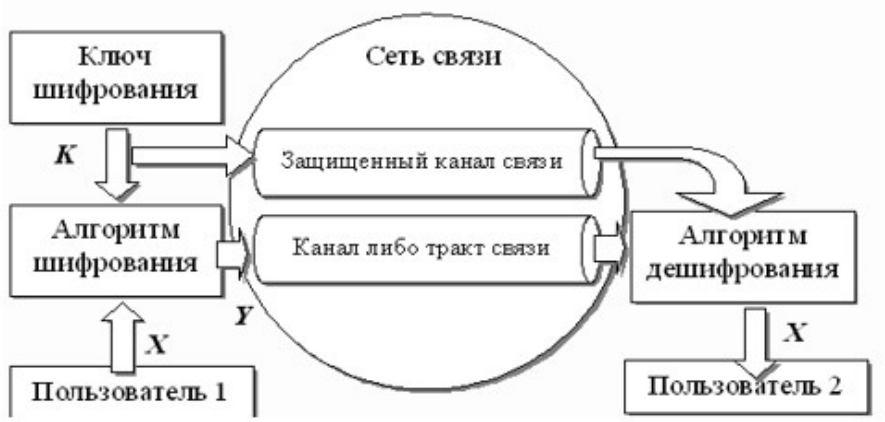
а) приложений;

б) транспортному;

в) сетевому;

г) сеансовому.

Вопрос 6. К какой криптосистеме относится приведенный рисунок?



а) с одним ключом;

б) с двумя ключами;

в) классическая криптосистема;

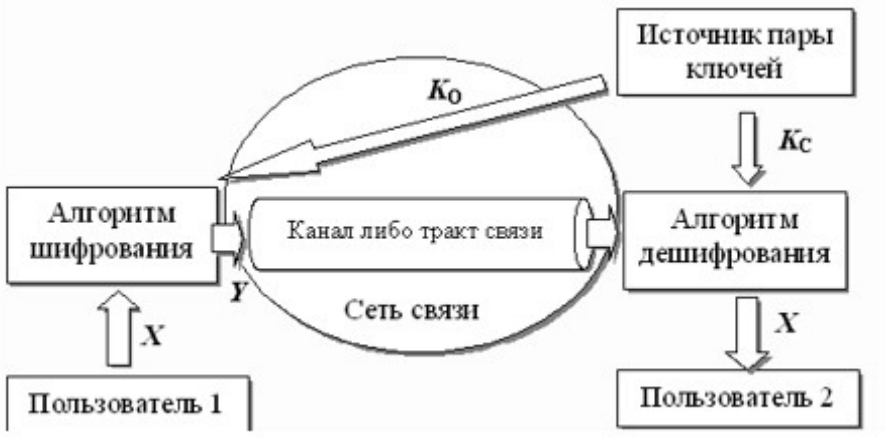
г) не относится к системе криптографии;

д) относится к симметричным криптосистемам;

е) относится к асимметричным криптосистемам.

1. верны варианты б, г, д;
2. верны варианты а, в, д;
3. верны варианты а, г, е;

Вопрос 7. К какой криптосистеме относится приведенный рисунок?



а) с одним ключом;

б) с двумя ключами;

в) классическая криптосистема;

г) не относится к системе криптографии;

д) относится к симметричным криптосистемам;

е) относится к асимметричным криптосистемам.

1. верны варианты б, г;
2. верны варианты а, в, г, д;
3. верны варианты а, в, г, е.

Вопрос 8. Известны следующие методы распределения открытых ключей:

1) индивидуальное публичное объявление открытых ключей пользователями;
2) использование публично доступного каталога открытых ключей;
3) участие авторитетного источника открытых ключей;
4) сертификаты открытых ключей.

Какой из методов не обеспечивает аутентификацию отправителя открытого ключа (КО)?

1. вариант 1;
2. вариант 2;
3. вариант 3;
4. вариант 4.

Вопрос 9. Совокупность требований безопасности и спецификаций, которая является основой для оценки конкретной системы информационной технологии – это:

а) задание по безопасности;
б) политика безопасности объекта оценки;
в) политика безопасности организации.

Вопрос 10. «Общие критерии оценки безопасности информационных технологий» ГОСТ Р ИСО/МЭК 15408 содержат:

а) критерии оценки безопасности, касающиеся административных мер безопасности, непосредственно не относящихся к мерам безопасности информационных технологий;
б) оценку специальных физических аспектов безопасности информационных технологий;
в) процедуры использования результатов оценки при аттестации продуктов и систем информационных технологий;
г) критерии для оценки специфических качеств криптографических алгоритмов;
д) механизмы для использования в качестве основы при оценке характеристик безопасности продуктов и систем информационных технологий.

5.1.8 Типовые задания (оценочное средство - Тест) для оценки сформированности компетенции ОПК-4:

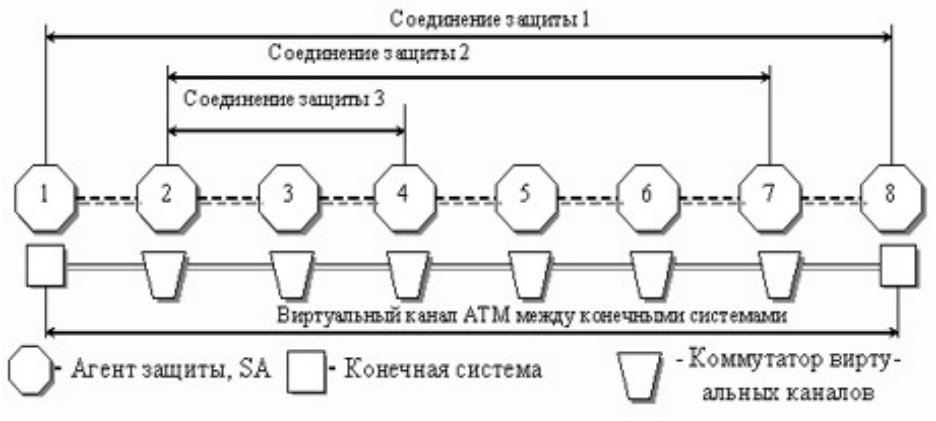
Вопрос 11. «Общие критерии оценки безопасности информационных технологий» ГОСТ Р ИСО/МЭК 15408 для пользователя дают возможность:

1) руководство и справочник при формулировании требований к функциям безопасности;
2) справочник по интерпретации функциональных требований и формулированию функциональных спецификаций для объектов оценки;
3) руководство по определению требуемого уровня доверия;
4) обязательное изложение критериев оценки, используемых при определении доверия к объектам оценки и оценки профилей защиты и заданий по безопасности.

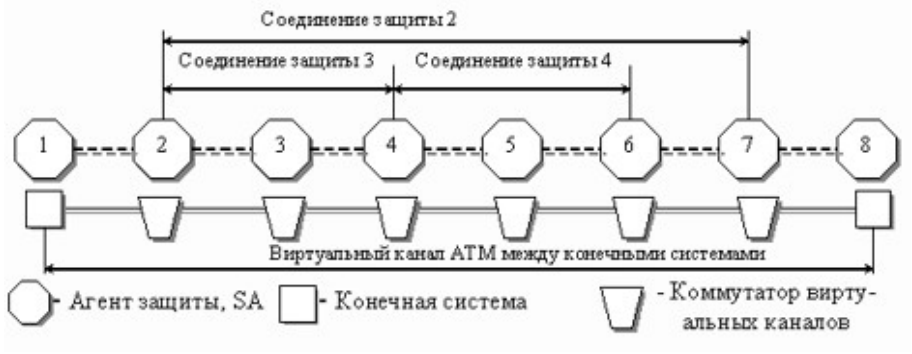
1. верны варианты 1, 3;
2. верны варианты 2, 4;
3. верны варианты 2, 3.

Вопрос 12. Определите правильный вариант организации соединений защиты информации.

а)

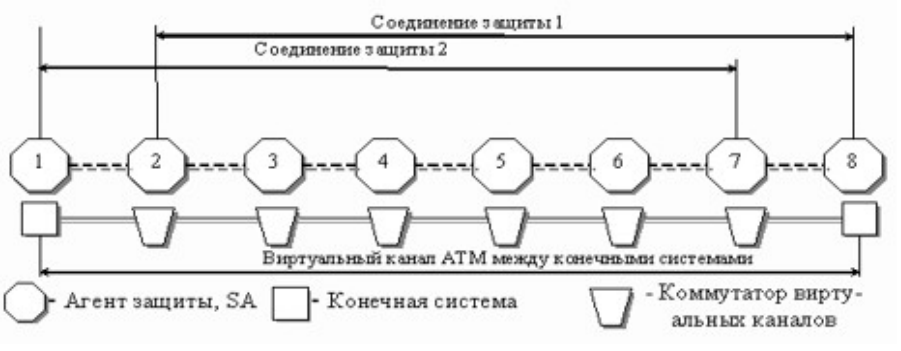


б)



в)

г)

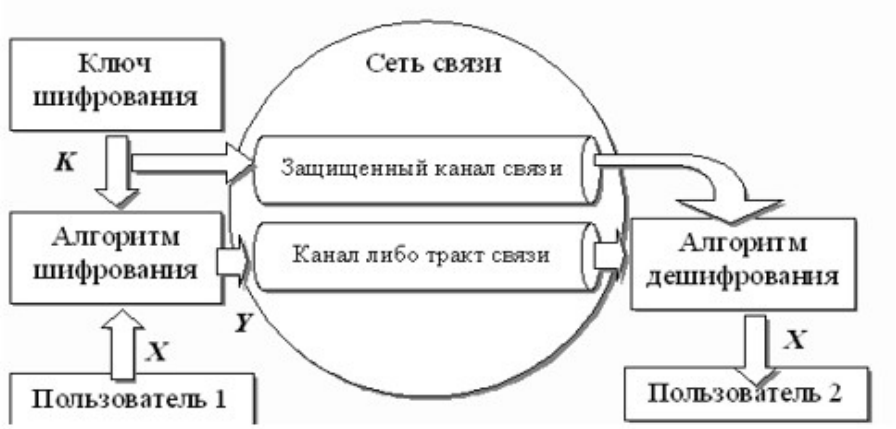


д) верны варианты а, б.

Вопрос 13. Какое предельное количество уровней вложения соединений защиты возможно для технологии ATM?

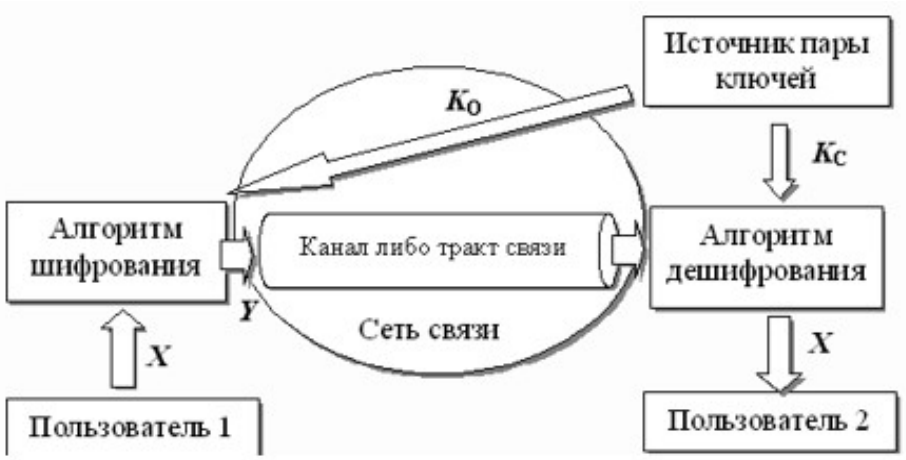
а) до 16 уровней;
б) до 32 уровней;
в) до 8 уровней;
г) до 8 уровней;

Вопрос 14. К какой криптосистеме относится приведенный рисунок?



а) с одним ключом;
б) с двумя ключами;
в) классическая криптосистема;
г) не относится к системе криптографии;
д) относится к симметричным криптосистемам;
е) относится к асимметричным криптосистемам.

Вопрос 15. К какой криптосистеме относится приведенный рисунок?



а) с одним ключом;
б) с двумя ключами;
в) классическая криптосистема;
г) не относится к системе криптографии;
д) относится к симметричным криптосистемам;
е) относится к асимметричным криптосистемам.

Вопрос 16. Какой оценочный уровень доверия позволяет разработчикам достичь высокого доверия путем применения специальных методов проектирования безопасности в строго контролируемой среде разработки с целью получения высококачественного объекта оценки для защиты высоко оцениваемых активов от значительных рисков?

а) 3;

б) 5;

в) 6;

г) 7;

д) 9.

Вопрос 17. Известны следующие методы распределения открытых ключей:

1) индивидуальное публичное объявление открытых ключей пользователями;

2) использование публично доступного каталога открытых ключей;

3) участие авторитетного источника открытых ключей;

4) сертификаты открытых ключей.

Какой из методов не обеспечивает аутентификацию отправителя открытого ключа (КО)?

1. вариант 1;
2. вариант 2;
3. вариант 3;
4. вариант 4.

Вопрос 18. Совокупность требований безопасности и спецификаций, которая является основой для оценки конкретной системы информационной технологии – это:

а) задание по безопасности;

б) политика безопасности объекта оценки;

в) политика безопасности организации.

Вопрос 19. «Общие критерии оценки безопасности информационных технологий» ГОСТ Р ИСО/МЭК 15408 содержат:

а) критерии оценки безопасности, касающиеся административных мер безопасности, непосредственно не относящихся к мерам безопасности информационных технологий;

б) оценку специальных физических аспектов безопасности информационных технологий;

в) процедуры использования результатов оценки при аттестации продуктов и систем информационных технологий;

г) критерии для оценки специфических качеств криптографических алгоритмов;

д) механизмы для использования в качестве основы при оценке характеристик безопасности продуктов и систем информационных технологий.

Вопрос 20. «Общие критерии оценки безопасности информационных технологий» ГОСТ Р ИСО/МЭК 15408 для пользователя дают возможность:

1) руководство и справочник при формулировании требований к функциям безопасности;

2) справочник по интерпретации функциональных требований и формулированию функциональных спецификаций для объектов оценки;

3) руководство по определению требуемого уровня доверия;

4) обязательное изложение критериев оценки, используемых при определении доверия к объектам оценки и оценки профилей защиты и заданий по безопасности.

1. верны варианты 1, 3;
2. верны варианты 2, 4;
3. верны варианты 2, 3.

Вопрос 21. Профиль защиты – это:

а) совокупность требований безопасности;

б) базовый набор требований доверия для оценки;

в) краткая спецификация объекта оценки совместно с требованиями и целями безопасности.

Вопрос 22. Какое количество оценочных уровней доверия предложено ГОСТ Р ИСО/МЭК 15048?

а) 3;

б) 5;

в) 7;

г) 9.

Критерии оценивания (оценочное средство - Тест)

Оценка	Критерии оценивания
отлично	85-100% правильных ответов
хорошо	66-84 % правильных ответов
удовлетворительно	50-65 % правильных ответов
неудовлетворительно	меньше 50 % правильных ответов

5.2. Описание шкал оценивания результатов обучения по дисциплине при промежуточной аттестации

Шкала оценивания сформированности компетенций

Уровень сформированности компетенций (индикатора достижения компетенций)	**неудовлетворительно**	**удовлетворительно**	**хорошо**	**отлично**
	не зачтено	**зачтено**		
Знания	Уровень знаний ниже минимальных требований. Имели место грубые ошибки	Минимально допустимый уровень знаний. Допущено много негрубых ошибок	Уровень знаний в объеме, соответствующем программе подготовки. Допущено несколько негрубых ошибок	Уровень знаний в объеме, соответствующем программе подготовки, без ошибок
Умения	При решении стандартных задач не продемонстрированы основные умения. Имели место грубые	Продемонстрированы основные умения. Решены типовые задачи с негрубыми ошибками.	Продемонстрированы все основные умения. Решены все основные задачи с негрубыми ошибками.	Продемонстрированы все основные умения. Решены все основные задачи с отдельными несущественными

	ошибки	Выполнены все задания, но не в полном объеме	Выполнены все задания в полном объеме, но некоторые с недочетами	недочетами, выполнены все задания в полном объеме
Навыки	При решении стандартных задач не продемонстрированы базовые навыки. Имели место грубые ошибки	Имеется минимальный набор навыков для решения стандартных задач с некоторыми недочетами	Продемонстрированы базовые навыки при решении стандартных задач с некоторыми недочетами	Продемонстрированы навыки при решении нестандартных задач без ошибок и недочетов

Шкала оценивания при промежуточной аттестации

Оценка		Уровень подготовки
зачтено	**отлично**	Все компетенции (части компетенций), на формирование которых направлена дисциплина, сформированы на уровне не ниже «отлично», при этом хотя бы одна компетенция сформирована на уровне «отлично»
	хорошо	Все компетенции (части компетенций), на формирование которых направлена дисциплина, сформированы на уровне не ниже «хорошо», при этом хотя бы одна компетенция сформирована на уровне «хорошо»
	удовлетворительно	Все компетенции (части компетенций), на формирование которых направлена дисциплина, сформированы на уровне не ниже «удовлетворительно», при этом хотя бы одна компетенция сформирована на уровне «удовлетворительно»
не зачтено	**неудовлетворительно**	Хотя бы одна компетенция сформирована на уровне «неудовлетворительно».

5.3 Типовые контрольные задания или иные материалы, необходимые для оценки результатов обучения на промежуточной аттестации с указанием критериев их оценивания:

5.3.1 Типовые задания (оценочное средство - Контрольные вопросы) для оценки сформированности компетенции ОПК-3

1. Общая характеристика компьютерных вирусов.
2. Принципы проявления вирусов.
3. Структура вируса.
4. Основные особенности наиболее распространенных вирусов.
5. Модели поведения вирусов и их деструктивные действия: файловые вирусы.
6. Модели поведения вирусов и их деструктивные действия: steals-вирусы.
7. Модели поведения вирусов и их деструктивные действия: полиморфные вирусы.
8. Модели поведения вирусов и их деструктивные действия: сетевые вирусы.
9. Модели поведения вирусов и их деструктивные действия: резидентные вирусы.
10. Взлом парольной защиты.
11. Защита от воздействия вирусов: архивирование, входной контроль.
12. Защита от воздействия вирусов: сегментация, фильтрация, вакцинация, автоконтроль целостности, терапия.
13. Состав программного комплекса защиты от компьютерных вирусов (перечислить и объяснить компоненты).
14. История становления российского законодательства в области информационных технологий.
15. Объяснить основные принципы главы 1 и 2 закона РФ «О правовой охране программ для ЭВМ и баз данных» -1.

16. Виды компьютерных правонарушений: несанкционированный доступ, встраивание в программное обеспечение «логических бомб», разработка и распространение компьютерных вирусов.
17. Виды компьютерных правонарушений: подделка компьютерной информации, хищение компьютерной информации, нарушение авторского права.

5.3.2 Типовые задания (оценочное средство - Контрольные вопросы) для оценки сформированности компетенции ОПК-4

1. Классификация компьютерных вирусов.
2. Пути распространения вирусов.
3. Модели поведения вирусов и их деструктивные действия: загрузочные вирусы.
4. Модели поведения вирусов и их деструктивные действия: макровирусы.
5. Программы-шпионы: понятие, назначение, виды и группы.
6. Защита от воздействия вирусов: профилактика, ревизия, карантин.
7. Перечислить и объяснить средства нейтрализации компьютерных вирусов.
8. Объяснить основные принципы главы 3 и 4 закона РФ «О правовой охране программ для ЭВМ и баз данных» -1.

Критерии оценивания (оценочное средство - Контрольные вопросы)

Оценка	Критерии оценивания
зачтено	ответ полный и правильный на основании изученной теории; теоретический материал и решение поставленных задач изложены в необходимой логической последовательности, грамотный научный язык; ответ самостоятельный. Могут быть допущены две–три несущественные ошибки, исправленные по требованию преподавателя
не зачтено	ответ обнаруживает непонимание студентом основного содержания учебного материала или допущены существенные ошибки, которые не могут быть исправлены при наводящих вопросах преподавателя

6. Учебно-методическое и информационное обеспечение дисциплины (модуля)

Основная литература:

1. Васильев В.И. Интеллектуальные системы защиты информации : учебное пособие / Васильев В.И. - Москва : Машиностроение, 2021. - 172 с. - ISBN 978-5-907104-99-0., https://e-lib.unn.ru/MegaPro/UserEntry?Action=FindDocs&ids=808491&idb=0.
2. Внуков А. А. Защита информации в банковских системах : учебное пособие / А. А. Внуков. - 2-е изд. ; испр. и доп. - Москва : Юрайт, 2022. - 246 с. - (Высшее образование). - URL: https://urait.ru/bcode/490278 (дата обращения: 14.08.2022). - ISBN 978-5-534-01679-6 : 819.00. - Текст : электронный // ЭБС "Юрайт"., https://e-lib.unn.ru/MegaPro/UserEntry?Action=FindDocs&ids=820178&idb=0.
3. Щеглов А. Ю. Защита информации: основы теории / Щеглов А. Ю., Щеглов К. А. - Москва : Юрайт, 2022. - 309 с. - (Высшее образование). - URL: https://urait.ru/bcode/490019 (дата обращения: 05.01.2022). - ISBN 978-5-534-04732-5 : 969.00. - Текст : электронный // ЭБС "Юрайт"., https://e-

lib.unn.ru/MegaPro/UserEntry?Action=FindDocs&ids=787163&idb=0.
4. Гришина Наталия Васильевна. Информационная безопасность предприятия : Учебное пособие / Российский государственный гуманитарный университет. - 2-е изд. - Москва : Издательство "ФОРУМ", 2017. - 239 с. - ВО - Бакалавриат. - ISBN 978-5-00091-007-8. - ISBN 978-5-16-105165-8. - ISBN 978-5-16-010494-2., https://e-lib.unn.ru/MegaPro/UserEntry?Action=FindDocs&ids=611221&idb=0.

Дополнительная литература:

1. Башлы П.Н. Информационная безопасность и защита информации : Учебник. - Москва : Издательский Центр РИОР, 2013. - 222 с. - ВО - Бакалавриат., https://e-lib.unn.ru/MegaPro/UserEntry?Action=FindDocs&ids=613461&idb=0.
2. Ковалев Дмитрий Викторович. Информационная безопасность : Учебное пособие / Южный федеральный университет. - Ростов-на-Дону : Издательство Южного федерального университета (ЮФУ), 2016. - 74 с. - ВО - Магистратура. - ISBN 978-5-9275-2364-1., https://e-lib.unn.ru/MegaPro/UserEntry?Action=FindDocs&ids=624148&idb=0.
3. Внуков А. А. Защита информации в банковских системах : учебное пособие / А. А. Внуков. - 2-е изд. ; испр. и доп. - Москва : Юрайт, 2022. - 246 с. - (Высшее образование). - URL: https://urait.ru/bcode/490278 (дата обращения: 14.08.2022). - ISBN 978-5-534-01679-6 : 819.00. - Текст : электронный // ЭБС "Юрайт"., https://e-lib.unn.ru/MegaPro/UserEntry?Action=FindDocs&ids=820178&idb=0.

Программное обеспечение и Интернет-ресурсы (в соответствии с содержанием дисциплины):

Лицензионное программное обеспечение: Операционная система Windows.
Лицензионное программное обеспечение: Microsoft Office.

Профессиональные базы данных и информационные справочные системы

Российский индекс научного цитирования (РИНЦ), платформа Elibrary: национальная информационно-аналитическая система. Адрес доступа: http://elibrary.ru/project_risc.asp

ГАРАНТ. Информационно-правовой портал [Электронный ресурс].– Адрес доступа: http://www.garant.ru

Свободно распространяемое программное обеспечение:

программное обеспечение LibreOffice;
программное обеспечение Yandex Browser;
программное обеспечение Paint.NET;

программное обеспечение 1С:
* "Бухгалтерия предприятия", редакция 3.0, см. http://v8.1c.ru/buhv8/ ,
* "Управление торговлей", редакция 11.1, см. http://v8.1c.ru/trade/ ,
* "Зарплата и управление персоналом", редакция 3.0, см. http://v8.1c.ru/hrm/ ,
* "Управление небольшой фирмой", редакция 1.5, см. http://v8.1c.ru/small.biz/ ,

* "ERP Управление предприятием 2.0", см. http://v8.1c.ru/erp/ .
* "Бухгалтерия государственного учреждения", редакция 1.0, см. http://v8.1c.ru/stateacc/ ,
* "Зарплата и кадры государственного учреждения", редакция 1.0, http://v8.1c.ru/statehrm/ .
программное обеспечение PascalABC.NET
Электронные библиотечные системы и библиотеки:
Электронная библиотечная система "Лань" https://e.lanbook.com/
Электронная библиотечная система "Консультант студента" http://www.studentlibrary.ru/
Электронная библиотечная система "Юрайт"http://www.urait.ru/ebs
Электронная библиотечная система "Znanium" http://znanium.com/
Электронно-библиотечная система Университетская библиотека ONLINE http://biblioclub.ru/
Фундаментальная библиотека ННГУ www.lib.unn.ru/
Сайт библиотеки Арзамасского филиала ННГУ. – Адрес доступа: lib.arz.unn.ru
Ресурс «Массовые открытые онлайн-курсы Нижегородского университета им. Н.И. Лобачевского» https://mooc.unn.ru/
Портал «Современная цифровая образовательная среда Российской Федерации» https://online.edu.ru/public/promo

7. Материально-техническое обеспечение дисциплины (модуля)

Учебные аудитории для проведения учебных занятий, предусмотренных образовательной программой, оснащены мультимедийным оборудованием (проектор, экран), техническими средствами обучения, компьютерами.

Помещения для самостоятельной работы обучающихся оснащены компьютерной техникой с возможностью подключения к сети "Интернет" и обеспечены доступом в электронную информационно-образовательную среду.

Программа составлена в соответствии с требованиями ОС ННГУ по направлению подготовки/специальности 09.03.03 - Прикладная информатика.

Автор(ы): Сазанов Александр Анатольевич.

Рецензент(ы): Фокеев Максим Игоревич, кандидат педагогических наук.

Заведующий кафедрой: Нестерова Лариса Юрьевна, кандидат педагогических наук.

Программа одобрена на заседании методической комиссии от 10.01.2024 г., протокол № 1.