МИНОБРНАУКИ РОССИИ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«ВОРОНЕЖСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»
(ФГБОУ ВО «ВГУ»)

УТВЕРЖДАЮ

Заведующий кафедрой
истории зарубежных стран и востоковедения
Мирошников А.В.

23.06.2022

РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ
Б1.О.12 Информационная безопасность и защита информации

1. Код и наименование направления подготовки: 58.03.01 Востоковедение и африканистика

2. Профиль подготовки: Востоковедные исследования

3. Квалификация выпускника: бакалавр

4. Форма обучения: очная

5. Кафедра, отвечающая за реализацию дисциплины: истории зарубежных стран и востоковедения

6. Составители программы: Золотарев Дмитрий Петрович, к.и.н., доцент кафедры истории зарубежных стран и востоковедения

7. Рекомендована: НМС исторического факультета, протокол № 6 от 23.06.2022.

8. Учебный год: 2023-2024 **Семестр(ы)/Триместр(ы):** 4

9. Цели и задачи учебной дисциплины

Целями освоения учебной дисциплины являются:

- формирование у студентов системы знаний в области информационной безопасности и применения на практике методов и средств защиты информации.

Задачи учебной дисциплины:

- овладение теоретическими, практическими и методическими вопросами обеспечения информационной безопасности и защиты информации;

- формирование практических навыков обеспечения защиты информации при использовании информационно-коммуникативных технологий.

10. Место учебной дисциплины в структуре ООП: Дисциплина относится к обязательной части блока Б1 учебного плана образовательной программы «Востоковедные исследования».

11. Планируемые результаты обучения по дисциплине/модулю (знания, умения, навыки), соотнесенные с планируемыми результатами освоения образовательной программы (компетенциями) и индикаторами их достижения:

Код	Название компетенции	Код(ы)	Индикатор(ы)	Планируемые результаты обучения
ОПК-3	Способен понимать принципы работы современных информационных технологий и использовать их для решения задач профессиональной деятельности	ОПК-3.1	Осуществляет поиск, сбор, хранение, обработку, представление информации при решении задач профессиональной деятельности	Знать: концепцию информационной безопасности, конституционные и законодательные основы ее реализации; основные тенденции и направления формирования и функционирования комплексной системы защиты информации в различных типах организационных структур; Уметь: работать с традиционными носителями информации; Владеть: навыками работы с программными средствами обеспечения информационной безопасности.
		ОПК-3.2	Подбирает и использует информационные технологии при решении задач профессиональной деятельности	Знать: информационно-коммуникационные технологии, применяемые для решения стандартных задач профессиональной деятельности; Уметь: работать с информацией в глобальных компьютерных сетях с учетом основных требований информационной безопасности при решении задач профессиональной деятельности. Владеть: навыками применения нормативных документов, разработанных ФСТЭК РФ и другими профильными ведомствами при решении задач профессиональной деятельности.

12. Объем дисциплины в зачетных единицах/час. — 2 ЗЕТ/ 72 часа.

Форма промежуточной аттестации зачет

13. Трудоемкость по видам учебной работы

Вид учебной работы		Трудоемкость			
		Всего	По семестрам		
			семестр № 4	№ семестра	…
Аудиторные занятия					
в том числе:	лекции	18	18		
	практические				
	лабораторные	18	18		
	групповые консультации				
Самостоятельная работа		36	36		
в том числе: курсовая работа (проект)					

Индивидуальные консультации				
Форма промежуточной аттестации *(экзамен – __час.)*	0	0		
Итого:	72	72		

13.1. Содержание дисциплины

№ п/п	Наименование раздела дисциплины	Содержание раздела дисциплины	Реализация раздела дисциплины с помощью онлайн-курса, ЭУМК*
1. Лекции			
1.1	Информационное общество и информационная безопасность: основные угрозы и способы их решения.	Информационное общество, его особенности. Информация и ее место в информационном обществе. Проблема защиты информации. Информационные войны и противостояния.	
1.2	Законодательство в области информационной безопасности	Международное право в сфере обеспечения информационной безопасности. Российское законодательство в данной сфере. Конституция Российской Федерации, Доктрина информационной безопасности Российской Федерации.	
1.3	Понятийный курса «информационная безопасность»	Основные понятия курса: Информационная опасность, информационная угроза, информационная безопасность, тайна, компьютерные системы управления, информационная война, вирус, тайна и ее виды, Информационный ресурс, информационная инфраструктура, угрозы информационной безопасности и др.	
1.4	Организационные основы защиты информации. Создание организационной подсистемы информационной безопасности предприятия	Разработка и ведение перечня сведений, составляющих предпринимательскую тайну. Состав сведений, которые не могут быть тайной. Назначение нормативно-методических материалов по регламентации системы защиты информации. Регламентация структуры и содержания комплексной системы защиты информации организации.	
1.5	Инженерно-техническая защита информации	Физические средства защиты. Угрозы безопасности собственности организации и персоналу. Виды охраняемых объектов, категории защищаемых помещений.	
1.6	Программные средства защиты информации в компьютерах, локальных сетях и средствах связи. Настройки безопасности ОС Windows 10.	Программно-технические методы обеспечения информационной безопасности. Парольная защита с помощью стандартных системных средств. Идентификация и аутентификация. Разграничение доступа. Протоколирование и аудит. Межсетевые экраны как средство защиты от несанкционированного доступа	
1.7	Программные средства защиты информации в компьютерах, локальных сетях и средствах связи. Настройки безопасности приложений Microsoft Office.	Характеристика пакета приложений Microsoft Office. Макросы и макровирусы. Цифровая подпись и цифровой сертификат для макроса. Возможности защиты информации в документах Microsoft Office.	
1.8	Программные средства защиты информации в компьютерах, локальных сетях и средствах связи. Антивирусные программы.	Основные виды компьютерных вирусов: загрузочные вирусы, вирусы в исполняемых компьютерных файлах, макровирусы, скрипт-вирусы, вирусы-мистификации. Профилактика вирусного заражения. Антивирусные программы. Методика применения антивирусных программ	
2. Лабораторные занятия			
2.1	Информационное общество и информационная безопасность: основные угрозы и способы их решения.	Информационная безопасность и способы ее обеспечения.	

2.2	Законодательство в области информационной безопасности	Федеральные законы в области информации и информационной безопасности. Указы президента РФ и постановления правительства РФ в области информации и информационной безопасности.	
2.3	Понятийный аппарат курса «информационная безопасность»	Основные понятия курса: Информационная опасность, информационная угроза, информационная безопасность, тайна, компьютерные системы управления, информационная война, вирус, тайна и ее виды, Информационный ресурс, информационная инфраструктура, угрозы информационной безопасности и др.	
2.4	Организационные основы защиты информации. Создание организационной подсистемы информационной безопасности предприятия	Разработка и ведение перечня сведений, составляющих предпринимательскую тайну. Состав сведений, которые не могут быть тайной. Назначение нормативно-методических материалов по регламентации системы защиты информации. Регламентация структуры и содержания комплексной системы защиты информации организации.	
2.5	Инженерно-техническая защита информации	Виды, назначение, задачи и организационные формы охраны объектов, функции персонала охраны Классификация экстремальных (чрезвычайных) ситуаций. Аппаратные средства защиты	
2.6	Программные средства защиты информации в компьютерах, локальных сетях и средствах связи. Настройки безопасности ОС Windows 10.	Программно-технические методы обеспечения информационной безопасности. Парольная защита с помощью стандартных системных средств. Идентификация и аутентификация. Разграничение доступа. Протоколирование и аудит. Межсетевые экраны как средство защиты от несанкционированного доступа	
2.7	Программные средства защиты информации в компьютерах, локальных сетях и средствах связи. Настройки безопасности приложений Microsoft Office.	Характеристика пакета приложений Microsoft Office. Макросы и макровирусы. Цифровая подпись и цифровой сертификат для макроса. Возможности защиты информации в документах Microsoft Office.	
2.8	Программные средства защиты информации в компьютерах, локальных сетях и средствах связи. Антивирусные программы.	Основные виды компьютерных вирусов: загрузочные вирусы, вирусы в исполняемых компьютерных файлах, макровирусы, скрипт-вирусы, вирусы-мистификации. Профилактика вирусного заражения. Антивирусные программы. Методика применения антивирусных программ	

13.2. Темы (разделы) дисциплины и виды занятий

№ п/п	Наименование темы (раздела) дисциплины	Виды занятий (количество часов)				
		Лекции	Практические	Лабораторные	Самостоятельная работа	Всего
1	Информационное общество и информационная безопасность: основные угрозы и способы их решения.	2	2		4	8
2	Законодательство в области информационной безопасности	3	3		6	12
3	Понятийный аппарат курса «информационная безопасность»	2	2		4	8
4	Организационные основы защиты информации. Создание организационной подсистемы информаци-	2	2		4	8

	онной безопасности предприятия					
5	Инженерно-техническая защита информации	2	2		4	8
6	Программные средства защиты информации в компьютерах, локальных сетях и средствах связи. Настройки безопасности ОС Windows 10.	2	2		4	8
7	Программные средства защиты информации в компьютерах, локальных сетях и средствах связи. Настройки безопасности приложений Microsoft Office.	2	2		4	8
8	Программные средства защиты информации в компьютерах, локальных сетях и средствах связи. Антивирусные программы.	3	3		6	12
	Итого:	18	18		36	72

14. Методические указания для обучающихся по освоению дисциплины: В процессе изучения дисциплины предусмотрена контактная (лекции и лабораторные занятия) и самостоятельная работа обучающихся.

На первой лекции студенты знакомятся с целями, задачами и предметом изучаемого курса. Далее целесообразно ознакомление с рабочей программой учебной дисциплины, размещенной в электронной образовательной среде ВГУ. Таким образом будет получено представление о содержании курса и сформируются целевые установки при его изучении. В дальнейшем, в ходе лекционных занятий целесообразно фиксировать основные тезисы и их аргументацию, задавать преподавателю уточняющие вопросы.

Для подготовки к лабораторной работе обучающийся должен заранее ознакомиться с заданием и теоретическим материалом, а также с техникой безопасности при работе в компьютерной аудитории, после выполнения работы оформить отчет о проделанной работе и подготовиться к ее защите. При подготовке лабораторным работам особое внимание следует уделять особенностям использования изучаемых программных продуктов и грамотному оформлению полученных результатов.

Самостоятельная работа обучающихся направлена на самостоятельное изучение отдельных тем и вопросов учебной дисциплины и является обязательной для каждого обучающегося, ее объем определяется учебным планом, обучающийся работает с рекомендованными материалами при минимальном участии преподавателя.

Самостоятельная работа с учебниками, учебными пособиями, научной, справочной литературой, материалами периодических изданий и ресурсами сети Internet, статистическими данными является наиболее эффективным методом получения знаний, позволяет значительно активизировать процесс овладения информацией, способствует более глубокому усвоению изучаемого материала, формирует у обучающихся свое отношение к конкретной проблеме.

Вопросы, которые вызывают у обучающихся затруднения при подготовке, должны быть заранее сформулированы и озвучены во время занятий в аудитории для дополнительного разъяснения преподавателем.

Виды самостоятельной работы: конспектирование учебной и научной литературы; проработка учебного материала; работа в электронной библиотечной системе; работа с информационными

справочными системами, выполнение домашних заданий; подготовка к лабораторным работам; работа с вопросами для самопроверки.

15. Перечень основной и дополнительной литературы, ресурсов интернет, необходимых для освоения дисциплины

а) основная литература:

№ п/п	Источник
1	ГОСТ Р ИСО/МЭК 27002-2012 Информационная технология. Методы и средства обеспечения безопасности. Свод норм и правил менеджмента информационной безопасности
2	Скрипник, Д. А. Обеспечение безопасности персональных данных: курс / Д. А. Скрипник ; Национальный Открытый Университет "ИНТУИТ". – Москва: Интернет-Университет Информационных Технологий (ИНТУИТ), 2011. – 109 с. ил., схем. – Режим доступа: – URL: https://biblioclub.ru/index.php?page=book&id=234794 (дата обращения 30.04.2021)
3	Царегородцев, А. В. Методы и средства защиты информации в государственном управлении: учебное пособие / А. В. Царегородцев, М. М. Тараскин. – Москва: Проспект, 2017. – 205 с.: табл. – Режим доступа: – URL: https://biblioclub.ru/index.php?page=book&id=468250 (дата обращения 30.04.2021)
4	Шаньгин, В. Ф. Информационная безопасность и защита информации: практическое пособие / В. Ф. Шаньгин. – Москва: ДМК Пресс, 2014. – 702 с.: ил., табл., схем. – Режим доступа: – URL: https://biblioclub.ru/index.php?page=book&id=260320 (дата обращения 30.04.2021)

б) дополнительная литература:

№ п/п	Источник
5	Бондаренко, И. С. Методы и средства защиты информации. Практикум: учебное пособие / И. С. Бондаренко, Ю. В. Демчишин. – Москва: МИСИС, 2018. – 32 с. – Текст: электронный // Лань: электронно-библиотечная система. – URL: https://e.lanbook.com/book/115269 (дата обращения: 09.02.2021). – Режим доступа: для авториз. пользователей.
6	Информационная безопасность и защита информации. Практикум: учебное пособие / А. С. Минзов, С. В. Бобылева, П. А. Осипов, А. А. Попов. – Дубна: Государственный университет «Дубна», 2020. – 85 с. – ISBN 978-5-89847-608-3. – Текст: электронный // Лань: электронно-библиотечная система. – URL: https://e.lanbook.com/book/154490 (дата обращения: 09.02.2021). – Режим доступа: для авториз. пользователей.
7	Информационная безопасность. Лабораторный практикум: учебное пособие. – Пермь: ПГГПУ, 2018. – 87 с. – ISBN 978-5-85219-007-9. – Текст: электронный // Лань: электронно-библиотечная система. – URL: https://e.lanbook.com/book/129509 (дата обращения: 09.02.2021). – Режим доступа: для авториз. пользователей.
8	Смирнов, В. И. Защита информации: лабораторный практикум: учебное пособие / В. И. Смирнов. – Йошкар-Ола: ПГТУ, 2017. – 68 с. – ISBN 978-5-8158-1866-8. – Текст: электронный // Лань: электронно-библиотечная система. – URL: https://e.lanbook.com/book/98193 (дата обращения: 09.02.2021). – Режим доступа: для авториз. пользователей.

в) информационные электронно-образовательные ресурсы (официальные ресурсы интернет)*:

№ п/п	Ресурс
1	Университетская библиотека ONLINE: электронно-библиотечная система. – URL: http://www.biblioclub.ru (дата обращения: 01.06.2021).
2	Электронно-библиотечная система "Лань". – URL: https://e.lanbook.com/ (дата обращения: 01.06.2021).
3	Электронный каталог Научной библиотеки ВГУ. – URL: http//www.lib.vsu.ru (дата обращения: 01.06.2021).
4	Золотарев Д.П. Информационная безопасность и защита информации: ЭУМК – URL: https://edu.vsu.ru/course/view.php?id=23203

16. Перечень учебно-методического обеспечения для самостоятельной работы

№ п/п	Источник
1	Золотарев Д.П. Информационная безопасность и защита информации: ЭУМК – URL: https://edu.vsu.ru/course/view.php?id=23203

17. Образовательные технологии, используемые при реализации учебной дисциплины, включая дистанционные образовательные технологии (ДОТ, электронное обучение (ЭО), смешанное обучение):

Основой использования образовательных технологий по дисциплине выступает системно-деятельностный подход, обеспечивающий наибольшую эффективность обучения и его практико-ориентированную составляющую. В организационном отношении образовательный процесс включает групповую и индивидуальную работу студентов. В рамках лекционных и практических занятий используются вербальные, наглядные, аудиовизуальные, компьютерные технологии, проблемное обучение.

Дисциплина реализуется с использованием дистанционных образовательных технологий. По дисциплине разработан ЭУМК Информационная безопасность и защита информации: ЭУМК – URL: https://edu.vsu.ru/course/view.php?id=23203 .

18. Материально-техническое обеспечение дисциплины:

специализированная мебель с компьютерной техникой (компьютеры) с возможностью подключения к сети «Интернет», мультимедиа-проектор Epson EB-X12, интерактивная доска Smart Board X885 87”, Office Home and Student 2019 All Lng PKL Onln CEE Only DwnLd C2R NR, WIN HOME 10 32-bit/64-bit All Lng PK Lic Online DwnLd NR, Kaspersky Endpoint Security для бизнеса - Универсальный Russian Edition

19. Оценочные средства для проведения текущей и промежуточной аттестаций и контроля

Порядок оценки освоения обучающимися учебного материала определяется содержанием следующих разделов дисциплины:

№ п/п	Наименование раздела дисциплины (модуля)	Компетенция(и)	Индикатор(ы) достижения компетенции	Оценочные средства
1.	Разделы 1-8	ОПК-3	ОПК-3.1	Практическое задание
2.	Разделы 2-8		ОПК-3.2	Лабораторная работа, дискуссия
Промежуточная аттестация форма контроля – зачет_____				Перечень вопросов практическое задание

20. Типовые оценочные средства и методические материалы, определяющие процедуры оценивания

20.1. Текущий контроль успеваемости

Контроль успеваемости по дисциплине осуществляется с помощью следующих оценочных средств: практическое задание, лабораторная работа, дискуссия.

Перечень практических заданий

1. Составьте документ «Политика безопасности предприятия».
2. Составьте документ «Распределение ответственности за обеспечение безопасности».
3. Составьте документ «Процесс внедрения новой информационной системы»
4. Составьте инструкцию по инвентаризации ресурсов.
5. Составьте соглашение о соблюдении режима информационной безопасности с сотрудниками (на примере одного сотрудника)
6. Составьте инструкцию о порядке реагирования на инциденты в области информационной безопасности, а также на сбои и неисправности.
7. Составьте инструкцию по защите от вредоносного ПО (вирусов, троянских коней).
8. Составьте инструкцию о безопасности носителей данных.

Описание технологии проведения

Практические задания выполняются на лабораторных занятиях в компьютерном классе и проверяются преподавателем.

Требования к выполнению заданий, шкалы и критерии оценивания

Практические задания оцениваются по шкале «зачтено – не зачтено». При выполнении практических заданий учитывается следующие показатели:

1) логичность структуры документа;

2) соответствие документа ГОСТ Р ИСО/МЭК 27002-2012 Информационная технология. Методы и средства обеспечения безопасности. Свод норм и правил менеджмента информационной безопасности;

3) корректность использования терминологического аппарата дисциплины;

4) грамотность оформления.

Оценка «зачтено» выставляется при соответствии задания всем четырем критериям. В случае несоответствия одному и более показателям задание возвращается на доработку обучающемуся.

При оценивании выполнения лабораторных работ оценивается техническая правильность выполнения. Оценка «зачтено» выставляется при полностью верном (правильном) техническом выполнении задания.

Перечень заданий для лабораторных работ

1. Настройте параметры локальной политики безопасности операционной системы Windows.
2. Создайте учетную запись пользователя с правами администратора. Установите пароль, соответствующий правилам безопасности.
3. Создайте учетную запись обычного пользователя. Установите имя пользователя «User1» и пароль «Istfak2022». Измените пароль на пароль соответствующий правилам безопасности.
4. Создайте учетную запись при помощи средства «Учетные записи пользователей» (диалоговое окно Выполнить). Отнесите ее к группе «Опытные пользователи».
5. Проведите шифрование документа и задание пароля для его открытия в MS Word.
6. Задайте пароль для изменения документа в MS Word.
7. Установите пароль в документе MS Excel. Измените его. Пароль должен отвечать требованиям надежности.
8. Установите пароль в документе MS PowerPoint. Пароль должен отвечать требованиям надежности. Измените его.
9. Создайте сертификат с автоподписью в Microsoft Office.
10. Подпишите макрос в документе в Microsoft Office.
11. Проведите настройку и обновление баз текущего антивируса.
12. Укажите параметры проверки и запустите проверку жесткого диска ПК антивирусом.

Описание технологии проведения

Лабораторные работы выполняются на лабораторных занятиях в компьютерном классе.

Требования к выполнению заданий, шкалы и критерии оценивания

При оценивании выполнения лабораторных работ оценивается техническая правильность выполнения, соответствия работы всем техническим параметром задания. Оценка «зачтено» выставляется при полностью верном (правильном) техническом выполнении задания. Оценка «не зачтено» выставляется при не соответствии работы одному или более техническим параметрам задания.

Перечень тем и вопросов для дискуссий:

Информационное общество и информационная безопасность: основные угрозы и способы их решения.

1. Особенности информационного общества
2. Место информации в информационном обществе.
3. Безопасность информации и информационная безопасность: есть ли различия?
4. Современные угрозы информационной безопасности.

Законодательство в области информационной безопасности.

1. Международное право в области защиты информации.
2. Виды тайн и способы их охраны в отечественном законодательстве.
3. Доктрина информационной безопасности Российской федерации: изменения и тенденции.

Организационные основы защиты информации. Создание организационной подсистемы информационной безопасности предприятия

1. Основные принципы и условия организационной защиты информации
2. Основные подходы и требования к организации системы защиты информации
3. Основные силы и средства, используемые для организации защиты информации

Инженерно-техническая защита информации

1. Понятие инженерно-технической защиты информации.
2. Основные виды инженерно-технической защиты информации
3. Физические средства защиты информации
4. Аппаратные средства защиты информации
5. Программные средства защиты информации.
6. Криптографические и стеганографические средства защиты информации.
7. Комбинированные средства защиты информации.

Настройки безопасности ОС Windows 10.

1. Настройка параметров аутентификации в ОС Windows.
2. Группы политик, отвечающих за безопасность.
3. Реестр Windows и редактор реестра.
4. Учетные записи в ОС Windows.
5. Методы создания учетных записей.

Настройки безопасности приложений Microsoft Office.

1. Средства защиты MS Office.
2. Основные правила создания паролей.
3. Цифровая подпись документа и способы ее установки.
4. Шифрование документа и установка пароля в MS Word.
5. Макросы и их особенности. Макровирусы и защита от них.

Мероприятия по защите информации от вредоносных программ.

1. Понятие вирус и классификация вирусов.
2. Антивирусные программы и их предназначение.
3. Классификация антивирусных программ.
4. Брандмауэр Windows и его функции.
5. Типы хакерских атак и методы защиты от них.

Описание технологии проведения

Дискуссия проводится на лабораторном занятии. Обучающиеся участвуют в обсуждении, формулируя свою точку зрения и аргументируя её. Выступление в дискуссии может представлять собой развернутое монологическое высказывание в течение не более, чем 10 минут, а также отдельные реплики, ответы на уточняющие вопросы.

Требования к выполнению заданий, шкалы и критерии оценивания

При оценивании участия обучающегося в дискуссии оценивается соответствие его выступления следующим показателям:

1) четкость формулируемых тезисов;

2)аргументированность ответа;

3) владение понятийным аппаратом дисциплины;

4) способность иллюстрировать ответ примерами практического использования теоретического материала;

5) ориентация в функциональных возможностях изучаемых программных продуктах;

6) способность быстро ориентироваться в материале, отвечая на дополнительные вопросы в рамках изучаемого объема;

7) грамотность и связность речи.

Оценка «зачтено» выставляется при соответствии ответа обучающегося не менее, чем пяти показателям. При несоответствии ответа обучающегося более, чем двум из перечисленных показателей выставляется оценка «не зачтено».

20.2. Промежуточная аттестация

Промежуточная аттестация по дисциплине осуществляется с помощью следующих оценочных средств: перечень вопросов, практическое задание.

По решению кафедры обучающийся может быть аттестован по итогам работы в семестре. При несогласии обучающегося с оценкой он имеет право на прохождение промежуточной аттестации на общих основаниях.

Перечень вопросов к зачету:

1. Информация и ее безопасность в информационном обществе.
2. Основные понятия курса (информационная безопасность, информационное противоборство, информационная война, информационная угроза и т.д.).
3. Правовое обеспечение информационной безопасности в РФ: общий обзор.
4. Доктрина информационной безопасности РФ. Национальные интересы России в информационной сфере
5. Система защиты информации и ее структуры.
6. Экономическая информация как товар и объект безопасности.
7. Профессиональные тайны, их виды. Объекты коммерческой тайны на предприятии.
8. Персональные данные и их защита.
9. Информационные угрозы, их виды и причины возникновения.
10. Информационные угрозы для государства.
11. Информационные угрозы для компании.
12. Информационные угрозы для личности (физического лица).
13. Способы воздействия информационных угроз на объекты.
14. Внешние и внутренние субъекты информационных угроз.
15. Компьютерные преступления и их классификация.
16. Вредоносные программы, их виды.
17. Политика безопасности и ее принципы.
18. Фрагментарный и системный подход к защите информации.
19. Методы и средства защиты информации.
20. Организационное обеспечение ИБ (информационной безопасности).
21. Организация конфиденциального делопроизводства.
22. Организационно-экономическое обеспечение ИБ.
23. Инженерно-техническое обеспечение компьютерной безопасности.
24. Организационно-правовой статус службы безопасности.
25. Стандарты в области ИБ и защиты информации.
26. Криптографические методы защиты информации.

Описание технологии проведения

Обучающийся получает контрольно-измерительный материал, в котором представлены два теоретических вопроса (из перечня вопросов к зачету) и одно практическое задание (из перечня практических заданий и заданий для лабораторных работ). Обучающемуся дается 45 минут для подготовки к устному ответу (при заполнении листа устного ответа) и выполнения практического задания. Обучающийся отвечает по вопросам КИМ, при необходимости преподаватель задает дополнительные вопросы, которые фиксируются в листе устного ответа. Далее преподаватель проверяет правильность выполнения практического задания.

Пример контрольно-измерительного материала:

УТВЕРЖДАЮ
Зав. кафедрой истории
зарубежных стран и востоковедения
_____ Мирошников А.В.
«29» июня 2022 г.

Направление 58.03.01 Востоковедение и африканистика
Дисциплина Информационная безопасность и защита информации
Курс 2
Форма обучения: очная
Вид аттестации: промежуточная
Вид контроля: зачет

Контрольно-измерительный материал № 11

1. Правовое обеспечение информационной безопасности в РФ: общий обзор.
2. Криптографические методы защиты информации.
3. Практическое задание: подпишите макрос в документе в Microsoft Office.

Преподаватель: Д.П. Золотарев

Требования к выполнению заданий, шкалы и критерии оценивания

Для оценивания результатов обучения на зачете учитываются следующие показатели:

− владение понятийным аппаратом и теоретическими основами дисциплины,

− способность иллюстрировать ответ примерами практического использования теоретического материала,

− способность связать вопросы теории с практическими заданиями,

− применять теоретические знания для решения практических задач,

− ориентация в функциональных возможностях изучаемых программных продуктах,

− грамотная, уверенная, связанная речь при устном ответе,

− способность быстро ориентироваться в материале, отвечая на дополнительные вопросы в рамках изучаемого объема.

Результат обучения оценивается: «зачтено», «не зачтено».

Соотношение показателей, критериев и шкалы оценивания результатов обучения

Критерии оценивания результатов обучения	Шкала оценок
Продемонстрировано знание базовых требований информационной безопасности; нормативных правовых актов в области защиты информации; основных методов, способов и мероприятий по обеспечению информационной безопасности в профессиональной деятельности; умение использовать программное обеспечение для решения задач, владение понятийным аппаратом дисциплины, правильно выполняет практическое задание.	зачтено
Ответ на контрольно-измерительный материал не соответствует более, чем двум из перечисленных показателей. Обучающийся демонстрирует отрывочные, фрагментарные знания, допускает грубые ошибки в ответе на вопрос КИМ, затрудняется ответить на дополнительные вопросы, правильно выполняет практическое задание.	не зачтено