Минобрнауки России

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ

«ВОРОНЕЖСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»

(ФГБОУ ВО «ВГУ»)

УТВЕРЖДАЮ

Заведующий кафедрой

Сирота Александр Анатольевич

Кафедра технологий обработки и защиты информации

23.04.2024

РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ

Б1.В.ДВ.01.02 Защита информации

1. Код и наименование направления подготовки/специальности:

37.04.01 Психология

2. Профиль подготовки/специализация:

Информационно-психологические и гибридные войны

3. Квалификация (степень) выпускника:

Магистратура

4. Форма обучения:

Очная

5. Кафедра, отвечающая за реализацию дисциплины:

Кафедра технологий обработки и защиты информации

6. Составители программы:

Акимов Алексей Викторович, к.ф.-м.н., старший преподаватель

7. Рекомендована:

№5 от 05.03.2024

8. Учебный год:

2024-2025

9.Цели и задачи учебной дисциплины:

Изучение основ, методов и практик защиты информационных систем от атак злоумышленников.

Основные задачи дисциплины:

- знакомство студентов с основными принципами обеспечения информационной безопасности;

- знакомство студентов с устоявшейся терминологией, применяемой в области информационной безопасности;

- знакомство студентов с основными положениями российского и международного законодательства в области информационной безопасности;

- обучение студентов базовым методам и практикам обеспечения информационной безопасности;

- знакомство студентов с базовыми средствами обеспечения информационной безопасности и овладевание навыками работы с ними;

- изучение студентами особенностей организации деятельности по обеспечению информационной безопасности и поведения людей в условиях инцидентов информационной безопасности.

10. Место учебной дисциплины в структуре ООП:

Входит в блок дисциплин, формируемый участниками образовательных отношений Б1.В.

Для успешного освоения дисциплины необходимы входные знания в области информатики.

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

Код и название компетенции	Код и название индикатора компетенции	Знания, умения, навыки
ПК-2 Способен понимать принципы работы современных информационных технологий и программных средств, в том числе отечественного производства, и использовать их при решении прикладных задач профессиональной деятельности психолога	ПК-2.1 Осуществляет поиск, сбор, хранение, обработку, представление информации при решении прикладных задач профессиональной деятельности психолога в условиях информационно-психологических и гибридных войн	Знать: теоретические и технологические основы защиты информации, типовые методы сбора, анализа и обобщения разнородной информации для решения задач профессиональной деятельности психолога, связанных с предотвращением деструктивных воздействий цифровой и иных видов информации, в условиях информационно-психологических и гибридных войн. Уметь: использовать типовые методы сбора, анализа и обобщения разнородной информации для решения задач профессиональной деятельности психолога, связанных с обеспечением защиты информации и с предотвращением деструктивных воздействий цифровой и иных видов информации, в условиях информационно-психологических и гибридных войн. Владеть: навыками использования типовых методов сбора, анализа и обобщения разнородной информации для решения задач профессиональной деятельности психолога, связанных с обеспечением защиты информации и с предотвращением деструктивных воздействий цифровой и иных видов информации, в условиях информационно-психологических и гибридных войн.
	ПК-2.3 Подбирает и использует прикладные информационные технологии при решении задач профессиональной деятельности психолога в условиях информационно-психологических и гибридных войн	Знать: основные современные технологии и инструментальные средства, обеспечивающие защиту информации, необходимые для решения прикладных задач профессиональной деятельности психолога в условиях информационно-психологических и гибридных войн Уметь: отбирать и применять эффективные технологии и инструментальные средства защиты информации для решения задач профессиональной деятельности психолога, связанных с выявлением и предотвращением угроз информационной безопасности в условиях информационно-психологических и гибридных войн Владеть: навыками отбора и применения эффективных технологий и инструментальных средств защиты информации для решения задач профессиональной деятельности психолога, связанных с выявлением и предотвращением угроз информационной безопасности в условиях информационно-психологических и гибридных войн

12. Объем дисциплины в зачетных единицах/час:

3/108

Форма промежуточной аттестации:

Экзамен

13. Трудоемкость по видам учебной работы

Вид учебной работы	Семестр 2	Всего
Аудиторные занятия	32	32
Лекционные занятия	16	16
Практические занятия		0
Лабораторные занятия	16	16
Самостоятельная работа	40	40
Курсовая работа		0
Промежуточная аттестация	36	36
Часы на контроль	36	36
Всего	108	108

13.1. Содержание дисциплины

п/п	Наименование раздела дисциплины	Содержание раздела дисциплины	Реализация раздела дисциплины с помощью онлайн-курса, ЭУМК
1. Лекции			
1.1	Общие принципы обеспечения безопасности	1. Информационная безопасность. Определение. Цели. Задачи. 2. Риски и угрозы. Управление рисками. Классификация рисков. 3. Облачные системы. Общее устройство и модели обслуживания. 4. Законодательство в области информационной безопасности. 5. Шифрование. Классификация методов шифрования.	

п/п	Наименование раздела дисциплины	Содержание раздела дисциплины	Реализация раздела дисциплины с помощью онлайн-курса, ЭУМК
1.2	Устройство архитектуры безопасности	1. Разграничение доступа. Группы и роли. 2. Аутентификация и авторизация. Порядок предоставления и проверки прав доступа. 3. Факторы и системы аутентификации. Технология единого входа. 4. Развертывание ПО. Хранение секретов в коде. 5. Пароли и ключи безопасности. Парольная политика. 6. Действия в условиях инцидента информационной безопасности.	
2. Практические занятия			
2.1	нет		
3. Лабораторные работы			
3.1	Общие принципы обеспечения безопасности	1. Информационная безопасность. Определение. Цели. Задачи. 2. Риски и угрозы. Управление рисками. Классификация рисков. 3. Облачные системы. Общее устройство и модели обслуживания.	

п/п	Наименование раздела дисциплины	Содержание раздела дисциплины	Реализация раздела дисциплины с помощью онлайн-курса, ЭУМК
3.2	Построение архитектуры безопасности	1. Разграничение доступа. Группы и роли. 2. Аутентификация и авторизация. Порядок предоставления и проверки прав доступа. 3. Факторы и системы аутентификации. Технология единого входа. 4. Развертывание ПО. Хранение секретов в коде. 5. Пароли и ключи безопасности. Парольная политика.	

13.2. Темы (разделы) дисциплины и виды занятий

№ п/п	Наименование темы (раздела)	Лекционные занятия	Практические занятия	Лабораторные занятия	Самостоятельная работа	Всего
1	Общие принципы обеспечения безопасности	7		6	20	33
2	Устройство архитектуры безопасности	9		10	20	39
		16	0	16	40	72

14. Методические указания для обучающихся по освоению дисциплины

1) При изучении дисциплины рекомендуется использовать следующие средства:

- рекомендуемую основную и дополнительную литературу;
- методические указания и пособия; контрольные задания для закрепления теоретического материала;
- электронные версии учебников и методических указаний для выполнения лабораторно - практических работ (при необходимости материалы рассылаются по электронной почте).

2) Для максимального усвоения дисциплины рекомендуется проведение письменного опроса (тестирование, решение задач) студентов по материалам лекций и практических работ. Подборка

вопросов для тестирования осуществляется на основе изученного теоретического материала. Такой подход позволяет повысить мотивацию студентов при конспектировании лекционного материала.

3) При проведении лабораторных занятий обеспечивается максимальная степень соответствия с материалом лекционных занятий и осуществляется экспериментальная проверка методов, алгоритмов и технологий обработки информации, излагаемых в рамках лекций.

4) При переходе на дистанционный режим обучения для создания электронных курсов, чтения лекций онлайн и проведения лабораторно- практических занятий используется информационные ресурсы Образовательного портала "Электронный университет ВГУ (https:\\edu.vsu.ru), базирующегося на системе дистанционного обучения Moodle, развернутой в университете.

5) При использовании дистанционных образовательных технологий и электронного обучения обучающиеся должны выполнять все указания преподавателей, вовремя подключаться к онлайн - занятиям, ответственно подходить к заданиям для самостоятельной работы.

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

№ п/п	Источник
1	Введение в информационную безопасность и защиту информации : учебное пособие / В. А. Трушин, Ю. А. Котов, Л. С. Левин, К. А. Донской. — Новосибирск : НГТУ, 2017. — 132 с. — ISBN 978-5-7782-3233-4. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/118219
2	Введение в информационную безопасность : учебное пособие / А. А. Малюк, В. С. Горбатов, В. И. Королев [и др.] ; под редакцией В. С. Горбатова. — Москва : Горячая линия-Телеком, 2018. — 288 с. — ISBN 978-5-9912-0160-5. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/111075
3	Бирюков, А. А. Информационная безопасность: защита и нападение / А. А. Бирюков. — 2-е изд. — Москва : ДМК Пресс, 2017. — 434 с. — ISBN 978-5-97060-435-9. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/93278

б) дополнительная литература:

№ п/п	Источник
1	Щербаков, Андрей Юрьевич. Современная компьютерная безопасность. Теоретические основы. Практические аспекты : учебное пособие для студ. вузов / А.Ю. Щербаков .— М. : Кн. мир, 2009 .— 351, [1] с. : ил., табл. — (Высшая школа) .— Библиогр.: с.350-351 .— ISBN 978-5-8041-0378-2.
2	Информатика: Введение в информационную безопасность : учебное пособие / М. А. Вус, В. С. Гусев, Д. В. Долгирев, А. А. Молдовян ; под общей редакцией М. А. Вуса. — Санкт-Петербург : Юридический центр, 2004. — 204 с. — ISBN 5-94201-399-3. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/146221

№ п/п	Источник
3	Основы управления информационной безопасностью: [учебное пособие для студентов вузов, обучающихся по направлениям подготовки (специальностям) укрупненной группы специальностей 090000 - "Информ. безопасность"] / А.П. Курило [и др.] .— 2-е изд., испр. — Москва : Горячая линия-Телеком, 2014 .— 243 с. : ил., табл. — (Вопросы управления информационной безопасностью ; Кн.1) .— Библиогр.: с.234-239 .— ISBN 978-5-9912-0361-6.
4	Краковский, Ю.М. Информационная безопасность и защита информации : учебное посо бие для студ. обуч. по специальности «Информационные системы и технологии» днев. и заоч. форм обучения / Ю.М. Краковский .— М. ; Ростов н/Д : МарТ, 2008 .— 287 с. : ил .— (Учебный курс) .— Библиогр.: с.221 .— ISBN 978-5-241-00925-8.
5	Таненбаум, Эндрю. Архитектура компьютера : пер. с англ. / Э.Таненбаум .— 4-е изд. — СПб. [и др.] : Питер, 2006 .— 698 с. : ил. табл. — (Классика Computer Science) .— Парал. тит. л. англ. — Библиогр. : с.654-664 .— Алф. указ. : с.685-698 .— ISBN 5-318-00298-6.
6	Левин М. Безопасность в сетях Internet и Intranet / М. Левин. – М.: Познават. кн. плюс, 2001. – 319 с.
7	Браун С. Виртуальные частные сети / С. Браун. – М.: Лори, 2001. – 508 с.
8	Теоретические основы компьютерной безопасности (учеб. пособие для ВУЗов) / П.Н. Девянин [и др.]. – М.: Радио и связь, 2000 – 192с.

в) информационные электронно-образовательные ресурсы:

№ п/п	Источник
1	Электронный каталог Научной библиотеки Воронежского государственного университета. – (http // www.lib.vsu.ru/).
2	Образовательный портал «Электронный университет ВГУ».– (https://edu.vsu.ru/)
3	ЭБС Лань, Лицензионный договор №3010, (с 01/03/2024 по 28.02.2025) 06/02 24 от 13.02.2024 (с дополнительным соглашением №1 от 14.03.2024), ЭБС «Университетская библиотека online» (Контракт №3010 06/11 23 от 26.12.2023 (с 26.12.2023 по 25.12.2024), ЭБС «Консультант студента» – Лицензионный договор №980КС/12-2023 / 3010-06/01-24 от 24.01.2024 с 24.01.2024 по 11. 01.2025), Электронная библиотека ВГУ, Договор №ДС-208 от 01.02.2021 с ООО «ЦКБ «БИБКОМ» и ООО «Агентство «Книга-Сервис» о создании Электронной библиотеки ВГУ, (с 01.02.2021 по 31.01.2027), ЭБС BOOK.ru, Договор №3010 15/983 23 от 20.12.2023, (с 01.02.2024 по 31.01.2025).

16. Перечень учебно-методического обеспечения для самостоятельной работы

№ п/п	Источник
1	Введение в информационную безопасность : учебное пособие / А. А. Малюк, В. С. Горбатов, В. И. Королев [и др.] ; под редакцией В. С. Горбатова. — Москва : Горячая линия-Телеком, 2018. — 288 с. — ISBN 978-5-9912-0160-5. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/111075

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

При реализации дисциплины используются следующие образовательные технологии: логическое построение дисциплины, установление межпредметных связей, обозначение теоретического и практического компонентов в учебном материале, актуализация личного и учебно-профессионального опыта обучающихся. Применяются разные типы лекций (вводная, обзорная, информационная, проблемная), лабораторных занятий (проблемные, занятия-практикумы и др.). На занятиях используются следующие интерактивные формы: деловые игры, групповое обсуждение, метод case-stady (анализ и решение профессиональных ситуационных задач).

Применяются электронное обучение и дистанционные образовательные технологии в части освоения материала лекционных и практических занятий, самостоятельной работы по отдельным разделам дисциплины, прохождения текущей и промежуточной аттестации. Обучающиеся используют электронные ресурсы портала «Электронный университет ВГУ» – Moodle:URL:http://www.edu.vsu.ru/

Для реализации учебной дисциплины используются следующие информационные технологии, включая программное обеспечение и информационно-справочные системы:

Аппаратно-программный психодиагностический комплекс «Мультипсихометр». Контракт № 3010-07/44-20 от 29.06.2020 с ООО «РУССКИЙ ИНТЕГРАТОР» (Воронеж); бессрочный.

Программный комплекс «Psychometric Expert–9 Practic+ версии» (на 15 пользователей). Контракт № 3010-07/41-20 от 23.06.2020 с ООО «РУССКИЙ ИНТЕГРАТОР» (Воронеж), неисключительные (пользовательские) лицензионные права, бессрочная лицензия.

Прикладной пакет программ статистического анализа данных (начального уровня) Statistica Basic Academic 13.0 for Windows Ru (локальная версия на 15 пользователей). Контракт № 3010-07/41-20 от 23.06.2020 с ООО «РУССКИЙ ИНТЕГРАТОР» (Воронеж), бессрочная лицензия для локальной установки.

Прикладной пакет программ статистического анализа данных (углубленного уровня) Statistica Ultimate Academic 13.0 for Windows Ru (локальная версия на 11 пользователей). Контракт № 3010-07/41-20 от 23.06.2020 с ООО «РУССКИЙ ИНТЕГРАТОР» (Воронеж), бессрочная лицензия для локальной установки.

ПО Интерактивное учебное пособие «Наглядная математика». Контракт № 3010-07/22-16 от 23.03.2016 с ООО «Информационные технологии» (ООО «Интех», Воронеж); бессрочный.

Неисключительная лицензия на ПО Microsoft Office ProPlus 2019 RUS OLP NL Acdmc. Договор №3010-16/24-19 от 01.04.2019 с ООО «БалансСофт Проекты» (Ульяновск); бессрочный.

WinPro 8 RUS Upgrd OLP NL Acdm. Договор №3010-07/37-14 от 18.03.2014 с ООО «Перемена» (Воронеж); бессрочная лицензия.

Программы для ЭВМ МойОфис Частное Облако. Лицензия Корпоративная на пользователя для образовательных организаций. Договор №3010-15/972-18 от 08.11.2018 с АО «СофтЛайн Трейд»

(Москва); лицензия бессрочная.

Справочная правовая система «Консультант Плюс» для образования, версия сетевая. Договор о сотрудничестве №14-2000/RD от 10.04.2000 с АО ИК «Информсвязь-Черноземье» (Воронеж); бессрочный.

Справочная правовая система «Гарант – Образование», версия сетевая. Договор о сотрудничестве №4309/03/20 от 02.03.2020 с ООО «Гарант-Сервис» (Воронеж); бессрочный.

18. Материально-техническое обеспечение дисциплины:

Мультимедийная аудитория для проведения занятий лекционного и семинарского типов, текущего контроля и промежуточной аттестации, помещение для хранения и профилактического обслуживания учебного оборудования (г. Воронеж, проспект Революции, д. 24, ауд. 413): специализированная мебель, мультимедиапроектор NEC NP60, ноутбук Lenovo 640, экран для проектора.

Компьютерный класс (кабинет информационных технологий №2) для проведения занятий лекционного и семинарского типов, лабораторных занятий, индивидуальных и групповых консультаций, аудитория для самостоятельной работы, помещение для хранения и профилактического обслуживания учебного оборудования (г.Воронеж, проспект Революции, д.24, ауд. 303): специализированная мебель, 15 персональных компьютеров CORE I5-8400 / B365M PRO4 / DDR4 8GB / SSD 480GB / DVI/HDMI/VGA/450Вт / Win10pro / GW2480, интерактивная панель Lumien, 75", МФУ лазерное HP LaserJet Pro M28w(W2G55A).

19. Оценочные средства для проведения текущей и промежуточной аттестаций

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

№ п/п	Разделы дисциплины (модули)	Код компетенции	Код индикатора	Оценочные средства для текущей аттестации
1	Разделы 1-2 Общие принципы обеспечения безопасности Устройство архитектуры безопасности	ПК-2	ПК-2.1, ПК-2.3	Контрольная работа по соответствующим разделам. Лабораторные работы 1-5

Промежуточная аттестация

Форма контроля - Экзамен

Оценочные средства для промежуточной аттестации

Перечень вопросов, практическое задание

20 Типовые оценочные средства и методические материалы, определяющие процедуры оценивания

20.1 Текущий контроль успеваемости

Текущий контроль успеваемости по дисциплине осуществляется с помощью следующих оценочных средств:

- Устный опрос на практических занятиях
- Контрольная работа по теоретической части курса
- Лабораторные работы

20.1.1 Примерный перечень применяемых оценочных средств

№ п/п	Наименование оценочного средства	Представление оценочного средства в фонде	Критерии оценки
1	Устный опрос на практических занятиях	Вопросы по темам/разделам дисциплины	Правильный ответ – зачтено, неправильный или принципиально неточный ответ - не зачтено
2	Контрольная работа по разделам дисциплины	Теоретические вопросы по темам/разделам дисциплины	Шкала оценивания соответствует приведенной в разделе 20.2.3
3	Лабораторная работа	Содержит 5 лабораторных заданий.	При успешном выполнении работ в течение семестра фиксируется возможность оценивания только теоретической части дисциплины в ходе промежуточной аттестации (экзамена), в противном случае проверка задания по лабораторным работам выносится на экзамен.

20.1.2. Пример задания для выполнения лабораторной работы

Лабораторная работа № 1

Схема защищаемой информационной системы, зоны доверия, источники угроз

Цель работы

Представить и описать схему защищаемой информационной системы на своем примере. Перечислись и описать возможные источники угроз. Ознакомиться с базовыми принципами организации защиты информационных систем.

Форма контроля

Письменный отчёт (допускается преставление в электронном виде). Опрос в устной форме в соответствии с перечнем контрольных вопросов.

Количество отведённых аудиторных часов

2

Содержание работы

1. Разработать, представить и описать схему защищаемой информационной системы (ИС) на своем собственном примере на основе схемы на рисунке 1.

Рисунок 1 Схема защищаемой информационной системы из [1]

В качестве примера использовать ИС бизнеса или организации, достаточно сложную, чтобы включать в себя хотя бы двухуровневую клиент-серверную архитектуру и минимум два типа пользователей, выполняющих слабо пересекающиеся задачи в рамках одной инфраструктуры, не считая ее администраторов. Например, клиенты и персонал, если взять ИС магазина, или разные подразделения: отдел кадров и преподаватели, если взять ИС вуза.

На первом этапе определиться со списком типов пользователей вашей ИС. На втором добавить инфраструктуру. На третьем – нарисовать и зоны доверия.

Стрелки использовать однонаправленные, по направлению от запрашивающего информацию элемента схемы как на рисунке. Надписать протоколы взаимодействия.

Каждый элемент схемы описать текстом (включая стрелки и используемые протоколы) и обосновать его наличие, зачем он нужен и что делает, какие данные обрабатывает и/или передает/хранит. Также описать зоны доверия, что у каждой внутри и почему, с чем или кем она взаимодействует снаружи, каким образом защищена от внешнего мира и других зон доверия.

2. Перечислись и описать возможные источники угроз вашей ИС на основе четырех категорий:

- хактивисты,

- организованная преступность или преступники-одиночки,

- инсайдеры,

- государственные службы.

Разобрать, что и почему их может заинтересовать в вашей ИС и какими возможностями они обладают, какой вред могут нанести какой части вашей ИС.

Контрольные вопросы:

Какие части представленной инфраструктуры могли бы быть размещены в облаке? Какие части представленной инфраструктуры не следует размещать в облаке? Почему?

Какие части вашей ИС являются виртуализованными, какие реализованы физически? Почему?

Литература

1. Dotson, Chris. Practical Cloud Security / Chris Dotson. O’Reilly. 2019.180 p.

20.1.3 Методические материалы, определяющие процедуры оценивания знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций

Текущая аттестация проводится в соответствии с Положением о текущей аттестации обучающихся по программам высшего образования Воронежского государственного университета. Текущая аттестация проводится в формах устного опроса (индивидуальный опрос, фронтальная беседа) и письменных работ (контрольные, лабораторные работы). При оценивании могут использоваться количественные или качественные шкалы оценок.

20.1.4 ФОСы для проверки остаточных знаний

Приведённые ниже задания рекомендуется использовать при проведении диагностических работ

для оценки остаточных знаний по дисциплине

Компетенция ПК-2

Задания закрытого типа

1. Что не является моделью предоставления облачных услуг:
- Платформа как услуга
- Инфраструктура как услуга
- Программное обеспечение как услуга
- Ни одна из перечисленных
- Все являются

Правильный ответ: Все являются

2. Какой вариант обработки риска означает отказ от деятельности или условия, вызывающего этот риск:

- Снижение риска
- Избежание риска
- Перенос (делегирование) риска
- Сохранение (принятие) риска

Правильный ответ: Избежание риска

3. К какому уровню ценности информации относится дистрибутив WinRAR, без ключей и прочей информации о лицензии:

- Низкий
- Средний
- Высокий
- Может относится к нескольким

Правильный ответ: Низкий

4. Какой из указанных поставщиков облачных услуг не позволят помечать используемые вами ресурсы текстовыми метками или тегами:

- Все позволяют
- Amazon
- Microsoft
- Google
- IBM
- Kubernetes

Правильный ответ: Все позволяют

5. Алгоритмом шифрования не является:

- RSA
- Все являются
- Код Цезаря
- AES

Правильный ответ: Все являются

6. Базовым принципом информационной безопасности не является:

- Двухфакторная аутентификация

- Все являются
- Минимальные привилегии (права доступа)
- Эшелонированная защита (оборона)

Правильный ответ: Демилитаризованная зона

Задания открытого типа

1. Какова энтропия источника сообщений с алфавитом всего из двух символов и при этом вероятность их появления одинакова.

Ответ округлить с точностью до третьего знака после запятой, и разделитель -- запятая.

Использовать логарифм по основанию 2.

Правильный ответ: 1

2. Сколько вариантов ключей возможно для зашифрованного сообщения из трех символов при использовании ключа той же длины? Известно, что в нем могут быть только латинские символы нижнего регистра.

Правильный ответ: 17576

Задания с развёрнутым ответом

1. Опишите три категории облачных систем и их особенности с точки зрения обеспечения безопасности: общие и отличия друг от друга.

Критерии оценивания	**Шкала оценок**
Обучающийся приводит полное и безошибочное описание трех категорий облачных систем: представлены и детализовано описаны все их элементы и особенности обеспечения информационной безопасности для каждой из категорий.	3 балла
Обучающийся приводит достаточно полное описание трех категорий облачных систем: представлены и перечислены все их основные элементы и особенности обеспечения информационной безопасности для каждой из категорий. Допускаются незначительные неточности, нет должной детализации описания.	2 балла

Приведено не содержащее грубых ошибок описание трех категорий облачных систем, правильно отражающее их основные особенности с точки зрения обеспечения информационной безопасности.	1 балл
Представлено частичное описание особенностей трех категорий облачных систем, содержащее грубые ошибки или неточности.	0 баллов

2. Опишите основные принципы обеспечения информационной безопасности.

Критерии оценивания	**Шкала оценок**
Обучающийся приводит полное и детализованное описание не менее четырех основных принципов обеспечения информационной безопасности.	3 балла
Обучающийся приводит достаточно полное описание не менее трех основных принципов обеспечения информационной безопасности. Допускаются незначительные неточности, нет должной детализации описания.	2 балла
Приведено не содержащее грубых ошибок описание не менее трех основных принципов обеспечения информационной безопасности, правильно отражающее их основные особенности.	1 балл
Представлено менее трех принципов обеспечения информационной безопасности. Приведенное описание является частичным, содержит грубые ошибки или неточности.	0 баллов

20.2 Промежуточная аттестация

Промежуточная аттестация может включать в себя проверку теоретических вопросов, а также, при необходимости (в случае невыполнения в течение семестра), проверку выполнения установленного перечня лабораторных заданий, позволяющих оценить уровень полученных знаний и/или практическое (ие) задание(я), позволяющее (ие) оценить степень сформированности умений и навыков.

Для оценки теоретических знаний используется перечень контрольно-измерительных материалов. Каждый контрольно-измерительный материал для проведения промежуточной аттестации включает два задания - вопросов для контроля знаний, умений и владений в рамках оценки уровня сформированности компетенции. При оценивании используется количественная шкала. Критерии оценивания приведены ниже в таблице раздела 20.2.3.

20.2.1. Примерный перечень вопросов к экзамену

1. Информационная безопасность. Определение. Цели. Задачи.
2. Риски и угрозы.
3. Управление рисками. Классификация рисков.
3. Облачные системы. Общее устройство.
4. Модели обслуживания облачных систем.
5. Законодательство в области информационной безопасности.
6. Разграничение доступа. Группы и роли.
7. Аутентификация и авторизация.
8. Порядок предоставления и проверки прав доступа.
9. Факторы и системы аутентификации.
10. Технология единого входа.
11. Развертывание ПО.
12. Хранение секретов в коде.
13. Пароли и ключи безопасности. Парольная политика.
14. Действия в условиях инцидента информационной безопасности.
15. Шифрование. Классификация методов шифрования.

20.2.2. Пример контрольно-измерительного материала

УТВЕРЖДАЮ

Заведующий кафедрой технологий обработки и защиты информации

_____ А.А. Сирота

__.__.2024

Направление подготовки / специальность 37.04.01 Психология

Дисциплина Б1.В.ДВ.01.02 Защита информации

Форма обучения Очное

Вид контроля Экзамен

Вид аттестации Промежуточная

Контрольно-измерительный материал № 1

1. Информационная безопасность. Определение. Цели. Задачи.

2. Пароли и ключи безопасности. Парольная политика.

Преподаватель _____ А.В. Акимов

20.2.3 Описание критериев и шкалы оценивания компетенций (результатов обучения) при промежуточной аттестации

Для оценивания результатов обучения на экзамене используются следующие содержательные показатели (формулируется с учетом конкретных требований дисциплины):

1. знание теоретических основ учебного материала, основных определений, понятий и используемой терминологии;
2. умение связывать теорию с практикой, умение выявлять и анализировать основные закономерности, полученные, в том числе, в ходе выполнения практических заданий;
3. умение обосновывать свои суждения и профессиональную позицию по излагаемому вопросу;
4. владение навыками программирования в рамках выполняемых практических заданий;
5. владение навыками проведения компьютерного эксперимента, тестирования алгоритмов обработки информации.

Различные комбинации перечисленных показателей определяют критерии оценивания результатов обучения (сформированности компетенций) на государственном экзамене:

- высокий (углубленный) уровень сформированности компетенций;
- повышенный (продвинутый) уровень сформированности компетенций;
- пороговый (базовый) уровень сформированности компетенций.

Для оценивания результатов обучения на государственном экзамене используется 4-балльная шкала: «отлично», «хорошо», «удовлетворительно», «неудовлетворительно». Для оценивания результатов обучения на зачете используется – зачтено, не зачтено по результатам тестирования.

Соотношение показателей, критериев и шкалы оценивания результатов обучения на государственном экзамене представлено в следующей таблице.

Критерии оценивания компетенций и шкала оценок

Критерии оценивания компетенций	Уровень сформированности компетенций	Шкала оценок
Обучающийся демонстрирует полное соответствие знаний, умений, навыков по приведенным критериям свободно оперирует понятийным аппаратом и приобретенными знаниями, умениями, применяет их при решении практических задач. Успешно выполнены лабораторные работы в соответствии с установленным перечнем.	Повышенный уровень	Отлично
Ответ на контрольно-измерительный материал не полностью соответствует одному из перечисленных выше показателей, но обучающийся дает правильные ответы на дополнительные вопросы. При этом обучающийся демонстрирует соответствие знаний, умений, навыков приведенным в таблицах показателям, но допускает незначительные ошибки, неточности, испытывает затруднения при решении практических задач. Успешно выполнены лабораторные работы в соответствии с установленным перечнем.	Базовый уровень	Хорошо
Обучающийся демонстрирует неполное соответствие знаний, умений, навыков приведенным в таблицах показателям, допускает значительные ошибки при решении практических задач. При этом ответ на контрольно-измерительный материал не соответствует любым двум из перечисленных показателей, обучающийся дает неполные ответы на дополнительные вопросы. Успешно выполнены лабораторные работы в соответствии с установленным перечнем.	Пороговый уровень	Удовлетворительно

Ответ на контрольно-измерительный материал не соответствует любым трем из перечисленных показателей. Обучающийся демонстрирует отрывочные, фрагментарные знания, допускает грубые ошибки. Не выполнены лабораторные работы в соответствии с установленным перечнем.	–	Неудовлетворительно