

Документ подписан простой электронной подписью

Информация о владельце:

ФИО: Юров Сергей Серафимович Автономная некоммерческая организация высшего образования

Должность: ректор

Дата подписания: 02.11.2022 17:33:17

Уникальный программный ключ:

3cba11a39f7f7fadc578ee5ed1f72a427b45709d10da52f2f114bf9bf44b8f14

“ИНСТИТУТ БИЗНЕСА И ДИЗАЙНА”

ФАКУЛЬТЕТ УПРАВЛЕНИЯ БИЗНЕСОМ



УТВЕРЖДАЮ

Ректор

С.С. Юров

«24» февраля 2022 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Б1.В.12 БИОМЕТРИЧЕСКИЕ СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ

Для направления подготовки:

09.03.02 Информационные системы и технологии
(уровень бакалавриата)

Типы задач профессиональной деятельности:

производственно-технологический; организационно-управленческий; проектный.

Направленность (профиль):

Информационные системы и технологии в бизнесе

Форма обучения:

очная, заочная

Москва – 2022

Разработчик: Мелехов Игорь Сергеевич, преподаватель кафедры гуманитарных и естественно-научных дисциплин
АНО ВО «Институт бизнеса и дизайна».

«15» января 2022 г



/И.С. Мелехов /

СОГЛАСОВАНО:

Декан факультета



(подпись)

/Н.Е. Козырева /

Заведующий кафедрой
разработчика РПД



(подпись)

/Е.С.Мальцева /

Протокол заседания кафедры № 6 от «27» января 2022 г.

1. ЦЕЛЬ И ЗАДАЧИ ДИСЦИПЛИНЫ

Цель:

Получить представление о работе, устройстве и проектировании биометрических систем защиты информации.

Задачи:

- приобретение знаний о различных видах биометрических систем защиты информации, принципах устройства биометрических систем защиты информации и противодействия ДВИ их функционирования;
- получение знаний о стандартах в области биометрических систем защиты информации и юридических особенностей по защите баз данных, содержащих биометрическую информацию;
- овладение практическими навыками по использованию методов и средств биометрических систем защиты информации, применяемых для обеспечения информационной безопасности

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОПОП

2.1. Место дисциплины в учебном плане:

Блок: Блок 1. Дисциплины (модули).

Часть: Часть, формируемая участниками образовательных отношений

Осваивается: 7 семестр очная форма обучения, 8 семестр заочная форма обучения.

3. КОМПЕТЕНЦИИ, ФОРМИРУЕМЫЕ В РЕЗУЛЬТАТЕ ОСВОЕНИЯ ДИСЦИПЛИНЫ

ПК-2 Способность выполнять работы по обеспечению функционирования баз данных и обеспечению их информационной безопасности

4. РЕЗУЛЬТАТЫ ОСВОЕНИЯ ДИСЦИПЛИНЫ ОБУЧАЮЩИМИСЯ

Код и наименование компетенции	Индикаторы достижения компетенции	Результаты обучения
ПК-2 Способность выполнять работы по обеспечению функционирования баз данных и обеспечению их информационной безопасности	ПК-2.1 Знать: методы и способы обеспечения функционирования баз данных и обеспечения их информационной безопасности ПК-2.2 Уметь: выполнять работы по обеспечению функционирования баз данных и обеспечению их информационной безопасности ПК-2.3 Владеть: методами и способами выполнять работы по обеспечению функционирования баз данных и обеспечению их информационной безопасности	Знает: основные законодательные акты и специальные стандарты в области БСЗИ; классификацию средств БСЗИ Умеет: подбирать компоненты БСЗИ исходя из требований к их функционированию в различных производственных условиях; производить настройку компонентов БСЗИ Владеет: навыками разработки проектной и технической документации, проектируемой системы защиты информации, включающей биометрические средства защиты информации. навыками пользования БСЗИ.

5. ОБЪЕМ ДИСЦИПЛИНЫ И РАСПРЕДЕЛЕНИЕ ВИДОВ УЧЕБНОЙ РАБОТЫ ПО СЕМЕСТРАМ

Общая трудоемкость дисциплины «Биометрические системы защиты информации» для студентов всех форм обучения, реализуемых в АНО ВО «Институт бизнеса и дизайна» по направлению подготовки 09.03.02 Информационные системы и технологии: 3 з.е. / 108 час.

Вид учебной работы	Всего число часов и (или) зачетных единиц (по формам обучения)	
	Очная	Заочная
Аудиторные занятия	36	14
<i>в том числе:</i>		
Лекции	18	6
Практические занятия	18	8
Лабораторные работы	-	
Самостоятельная работа	72	90
<i>в том числе:</i>		
часы на выполнение КР / КП	-	-
Промежуточная аттестация:		
Вид	Зачет	Зачет
Трудоемкость (час.)		4
Общая трудоемкость з.е. / часов	3 з.е. / 108 час.	3 з.е. / 108 час.

6. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

Темы дисциплины		Количество часов (по формам обучения)							
№	Наименование	Очная				Заочная			
		Лекции	Практические занятия	Лабораторные работы	Самост. работа (в т.ч. КР / КП)	Лекции	Практические занятия	Лабораторные работы	Самост. работа (в т.ч. КР / КП)
1	Тема 1. БСЗИ как часть информационной безопасности	1	1		7		1		9
2	Тема 2. Особенности биометрии в сфере защиты информации	1	1		7	1			9
3	Тема 3. Система стандартизации БСЗИ	2	2		7	1			9
4	Тема 4. Основные методы биометрической идентификации	2	2		7	1	1		9
5	Тема 5. Перспективные методы биометрической идентификации	2	2		7		1		9
6	Тема 6. Применение биометрии в системах защиты информации	2	2		7	1	1		9

Темы дисциплины		Количество часов (по формам обучения)								
№	Наименование	Очная				Заочная				
		Лекции	Практические занятия	Лабораторные работы	Самост. работа (в т.ч. КР / КП)	Лекции	Практические занятия	Лабораторные работы	Самост. работа (в т.ч. КР / КП)	
7	Тема 7. Особенности правовой защиты биометрических баз данных	2	2		7	1	1		9	
8	Тема 8. Организация защиты Био ИСПДН	2	2		7		1		9	
9	Тема 9. Обезличивание персональных данных	2	2		8	1	1		9	
10	Тема 10. Ответственность за несоблюдение законодательства в сфере сохранности биометрических БиоПД	2	2		8		1		9	
Итого (часов)		18	18		72	6	8		90	
Форма контроля:		зачет				зачет				4
Всего по дисциплине:		108 / 3 з.е.				108 / 3 з.е.				

СОДЕРЖАНИЕ ТЕМ ДИСЦИПЛИНЫ

Тема 1. БСЗИ как часть информационной безопасности

Информационная безопасность. Основные составляющие информационной безопасности. Особенность ИБ в БиоПД. Механизмы ИБ. Шифрование. Аудит. Механизм арбитража. Идентификация и аутентификация. Виды идентификации. Способы аутентификации. Идентификация/аутентификация с помощью биометрических данных.

Тема 2. Особенности биометрии в сфере защиты информации

Биометрические характеристики человека. Биометрическая система ЗИ. Основные компоненты биометрической системы. Алгоритм биометрической аутентификации. Методы биометрической идентификации. Статические. Динамические. Смешанные. Недостатки биометрических систем. Показатели биометрических систем.

Тема 3. Система стандартизации БСЗИ

Регуляторы в БСЗИ. Стандарты, определяющие прикладной программный интерфейс для разработки биометрических систем. Единый формат представления биометрических данных (СВЕФФ). Использование биометрии в сфере финансовых услуг. Специализированные биометрические стандарты. Стандарты РФ в области Биометрии.

Тема 4. Основные методы биометрической идентификации

Классификация методов БСЗИ. По отпечаткам пальцев (дактелоскопия). Средства БСЗИ. Характеристики метода. По характеристикам речи. Средства БСЗИ. Характеристики метода. По радужной оболочке глаза. Средства БСЗИ. Характеристики метода. По изображению лица. 2-d. 3-d. Средства БСЗИ. Характеристики метода. По изображению, получаемому с нескольких камер. Средства БСЗИ. Характеристики метода. Метод, реализующий накопления информации о лице. Средства БСЗИ. Характеристики метода. Метод проецирования шаблона. Средства БСЗИ. Характеристики метода. По

геометрии ладони руки. Средства БСЗИ. Характеристики метода. По сетчатке глаза. Средства БСЗИ. Характеристики метода. По венозному рисунку руки. Средства БСЗИ. Характеристики метода. По почерку. Средства БСЗИ. Характеристики метода.

Тема 5. Перспективные методы биометрической идентификации

На основе термограммы лица. Преимущества и недостатки. На анализе характеристик ДНК. Преимущества и недостатки. Анализ отпечатков ладоней. Преимущества и недостатки. Технология анализа формы ушной раковины. Преимущества и недостатки. Система «Электронный нос». Преимущества и недостатки. Перспективные биометрические системы. Преимущества и недостатки. Соотношение FAR и FRR для различных биометрических систем.

Тема 6. Применение биометрии в системах защиты информации

Генерирование ЭП с помощью БСЗИ. Схема работы. Мультибиометрическая система идентификации клиентов банка. Биокарты в госсекторе. Единый электронный документ и БСЗИ на примере ПАО «Сбербанка». БСЗИ в мониторинговых системах.

Тема 7. Особенности правовой защиты биометрических баз данных

Нормативная правовая база РФ в сфере БиоПД и Био ИСПДН Закон РФ N152-ФЗ «О персональных данных» Подзаконные акты ФЗ №152 в сфере БиоПД. Классификация информационных систем. Регулирование и контроль в сфере баз Биометрических данных. Классификация актуальных угроз в сфере баз Био ПД. Требования к защите персональных данных при их обработке в информационных системах персональных данных. Необходимые локальные правовые акты и документы.

Тема 8. Организация защиты Био ИСПДН

Основные правовые меры по организации ИБ при обработки персональных данных Основные организационные меры по организации ИБ при обработки персональных данных Основные технические меры по организации ИБ при обработки персональных данных Политика оператора в отношении обработки Био ПДн Выбор необходимых мер для обеспечения безопасности биометрических персональных данных.

Тема 9. Обезличивание персональных данных

Законодательство в сфере обезличивания ПД Статьи в законе о ПД Методические рекомендации по применению Приказа № 996 от 5 сентября 2013 года "Об утверждении требований и методов по обезличиванию персональных данных" Порядок проведения обезличивания ПД Свойства обезличенных данных. Полнота. Структурированность. Релевантность. Семантическая целостность. Применимость. Анонимность. Методы обезличивания персональных данных. Деобезличивание.

Тема 10. Ответственность за несоблюдение законодательства в сфере сохранности биометрических БиоПД

Виды юридической ответственности в сфере БиоПД. Административная КоАП статьи 5.39, ст. 13.11, 19.7. Уголовная УКРФ статьи 137, 140, 272, 273. Гражданско-правовая ГКРФ статьи 15, 151 Закон о ПД ст. 24. Дисциплинарная ТКРФ пп. "в" п. 6 ч.1 ст. 81, ст. 90, 192.

7. ПРИМЕРНАЯ ТЕМАТИКА КУРСОВЫХ РАБОТ

Курсовая работа не предусмотрена

8. ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ПО ДИСЦИПЛИНЕ: Приложение 1.

9. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ:

9.1. Рекомендуемая литература:

1. Абденев, А. Современные системы управления информационной безопасностью: учебное пособие: [16+] / А. Абденев, Г. Дронова, В. Трушин; Новосибирский государственный технический университет. – Новосибирск: Новосибирский государственный технический университет, 2017. – 48с.

Режим доступа: по подписке. – URL: <https://biblioclub.ru/index.php?page=book&id=574594> .

2. Ищейнов, В. Я. Информационная безопасность и защита информации: теория и практика: учебное пособие: [16+] / В. Я. Ищейнов. – Москва; Берлин: Директ-Медиа, 2020. – 271 с

Режим доступа: по подписке. – URL: <https://biblioclub.ru/index.php?page=book&id=571485>

3. Минин, И. В. Защита конфиденциальной информации при электронном документообороте: учебное пособие: [16+] / И. В. Минин, О. В. Минин. – Новосибирск: Новосибирский государственный технический университет, 2011. – 20 с. –

Режим доступа: по подписке. – URL: <https://biblioclub.ru/index.php?page=book&id=228779>

4. Мицук, С. В. Защита и обработка конфиденциальных документов: виды тайн : учебное пособие : [16+] / С. В. Мицук ; Липецкий государственный педагогический университет им. П. П. Семенова-Тян-Шанского. – Липецк: Липецкий государственный педагогический университет имени П.П. Семенова-Тян-Шанского, 2017. – 62 с.

Режим доступа: по подписке. – URL: <https://biblioclub.ru/index.php?page=book&id=577437>

5. Основы информационной безопасности: учебник / В. Ю. Rogozin, И. Б. Галушкин, В. Новиков, С. Б. Вепрев; Академия Следственного комитета Российской Федерации. – Москва: Юнити-Дана: Закон и право, 2018. – 287 с.

Режим доступа: по подписке. – URL: <https://biblioclub.ru/index.php?page=book&id=562348>

9.2. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине (модулю), включая перечень лицензионного и свободно распространяемого программного обеспечения.

При осуществлении образовательного процесса по данной учебной дисциплине предполагается использование:

Лицензионное и свободно распространяемое программное обеспечение, в том числе отечественного производства:

1. Windows 10 Pro Professional (Договор: Tr000391618, срок действия с 20.02.2020 г. по 28.02.2023 г., Лицензия: V8732726);

2. Microsoft Office Professional Plus 2019 (Договор: Tr000391618, срок действия с 20.02.2020 г. по 28.02.2023 г., Лицензия: V8732726).

3. Браузер Google Chrome;

4. Браузер Yandex;

5. Adobe Reader - программа для просмотра, печати и комментирования документов в формате PDF

9.3. Перечень современных профессиональных баз данных, информационных справочных систем и ресурсов информационно-телекоммуникационной сети «Интернет»

1. <https://biblioclub.ru/> - университетская библиотечная система online Библиоклуб.ру

2. <http://window.edu.ru/> - единое окно доступа к образовательным ресурса

3. <https://uisrussia.msu.ru/> - база данных и аналитических публикаций университетской информационной системы Россия

4. <https://www.elibrary.ru/> - электронно-библиотечная система eLIBRARY.RU, крупнейшая в России электронная библиотека научных публикаций

5. <http://www.consultant.ru/> - справочная правовая система КонсультантПлюс

6. <https://gufo.me/> - справочная база энциклопедий и словарей

7. <https://slovaronline.com> - поисковая система по всем доступным словарям и энциклопедиям

8. <https://www.tandfonline.com/> - коллекция журналов Taylor&Francis Group включает в себя около двух тысяч журналов и более 4,5 млн. статей по различным областям знаний

9. <https://openedu.ru> - «Национальная платформа открытого образования» (ресурсы открытого доступа)

10. <https://www.rsl.ru> - Российская Государственная Библиотека (ресурсы открытого доступа)

11. <https://link.springer.com> - Международная реферативная база данных научных изданий Springerlink (ресурсы открытого доступа)

12. <https://zbmath.org> - Международная реферативная база данных научных изданий zbMATH (ресурсы открытого доступа)

10. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

1. Оборудованные учебные аудитории, в том числе с использованием видеопроектора и подключением к сети «Интернет» и доступом в электронную информационно-образовательную среду Института.

2. Аудитории для самостоятельной работы с подключением к сети «Интернет» и доступом в электронную информационно-образовательную среду Института.

3. Компьютерный класс с подключением к сети «Интернет» и доступом в электронную информационно-образовательную среду Института.

4. Аудио и видеоаппаратура.

№ 409

Учебная аудитория для проведения учебных занятий. Аудитория оснащена оборудованием и техническими средствами обучения:

а) учебной мебелью: столы, стулья, доска маркерная учебная

б) стационарный широкоформатный мультимедиа-проектор Epson EB-X41, экран, колонки.

в) 11 компьютеров, подключенных к сети

«Интернет», с обеспечением доступа в электронную информационно-образовательную среду АНО ВО «Институт бизнеса и дизайна»

№ 402

Помещение для самостоятельной работы. Аудитория оснащена оборудованием и техническими средствами обучения:

а) учебной мебелью: столы, стулья, доска маркерная учебная

б) стационарный широкоформатный мультимедиа-проектор Epson EB-X41, экран, колонки.

в) 11 компьютеров, подключенных к сети «Интернет», с обеспечением доступа в электронную информационно-образовательную среду АНО ВО «Институт бизнеса и дизайна»

11. МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ ДЛЯ ОБУЧАЮЩИХСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ

В процессе освоения дисциплины студенту необходимо посетить все виды занятий, предусмотренные рабочей программой дисциплины и выполнить контрольные задания, предлагаемые преподавателем для успешного освоения дисциплины. Также следует изучить рабочую программу дисциплины, в которой определены цели и задачи дисциплины, компетенции обучающегося, формируемые в результате освоения дисциплины и планируемые результаты обучения. Рассмотреть содержание тем дисциплины; взаимосвязь тем лекций и практических занятий; бюджет времени по видам занятий; оценочные средства для текущей и промежуточной аттестации; критерии итоговой оценки результатов освоения дисциплины. Ознакомиться с методическими материалами, программно-информационным и материально-техническим обеспечением дисциплины.

Работа на лекции

Лекционные занятия включают изложение, обсуждение и разъяснение основных направлений и вопросов изучаемой дисциплины, знание которых необходимо в ходе реализации всех остальных видов занятий и в самостоятельной работе студентов. На лекциях студенты получают самые необходимые знания по изучаемой проблеме. Непременным условием для глубокого и прочного усвоения учебного материала является умение студентов сосредоточенно слушать лекции, активно, творчески воспринимать излагаемые сведения. Внимательное слушание лекций предполагает интенсивную умственную деятельность студента. Краткие записи лекций, конспектирование их помогает усвоить материал. Конспект является полезным тогда, когда записано самое существенное, основное. Запись лекций рекомендуется вести по возможности собственными формулировками.

Желательно запись осуществлять на одной странице, а следующую оставлять для проработки учебного материала самостоятельно в домашних условиях. Конспект лучше подразделять на пункты, параграфы, соблюдая красную строку. Принципиальные места, определения, формулы следует сопровождать замечаниями. Работая над конспектом лекций, всегда следует использовать не только основную литературу, но и ту литературу, которую дополнительно рекомендовал лектор.

Практические занятия

Подготовку к практическому занятию следует начинать с ознакомления с лекционным материалом, с изучения плана практических занятий. Определившись с проблемой, следует обратиться к рекомендуемой литературе. Владение понятийным аппаратом изучаемого курса является необходимым, поэтому готовясь к практическим занятиям, студенту следует активно пользоваться справочной литературой: энциклопедиями, словарями и др. В ходе проведения практических занятий, материал, излагаемый на лекциях, закрепляется, расширяется и дополняется при подготовке сообщений, рефератов, выполнении тестовых работ. Степень освоения каждой темы определяется преподавателем в ходе обсуждения ответов студентов.

Самостоятельная работа

Студент в процессе обучения должен не только освоить учебную программу, но и приобрести навыки самостоятельной работы. Самостоятельная работа студентов играет важную роль в воспитании сознательного отношения самих студентов к овладению теоретическими и практическими знаниями, привитии им привычки к направленному интеллектуальному труду. Самостоятельная работа проводится с целью углубления знаний по дисциплине. Материал, законспектированный на лекциях, необходимо регулярно дополнять сведениями из литературных источников, представленных в рабочей программе. Изучение литературы следует начинать с освоения соответствующих разделов дисциплины в учебниках, затем ознакомиться с монографиями или статьями по той тематике, которую изучает студент, и после этого – с брошюрами и статьями, содержащими материал, дающий углубленное представление о тех или иных аспектах рассматриваемой проблемы. Для расширения знаний по дисциплине студенту необходимо использовать Интернет-ресурсы и специализированные базы данных: проводить поиск в различных системах и использовать материалы сайтов, рекомендованных преподавателем на лекционных занятиях.

Подготовка к сессии

Основными ориентирами при подготовке к промежуточной аттестации по дисциплине являются конспект лекций и перечень рекомендуемой литературы. При подготовке к сессии студенту следует так организовать учебную работу, чтобы перед первым днем начала сессии были сданы и защищены все практические работы. Основное в подготовке к сессии – это повторение всего материала курса, по которому необходимо пройти аттестацию. При подготовке к сессии следует весь объем работы распределять равномерно по дням, отведенным для подготовки, контролировать каждый день выполнения работы.

Методические рекомендации для обучающихся с ОВЗ и инвалидов по освоению дисциплины

В АНО ВО «Институт бизнеса и дизайна» созданы специальные условия для получения высшего образования по образовательным программам обучающимися с ограниченными возможностями здоровья (ОВЗ).

Для перемещения инвалидов и лиц с ограниченными возможностями здоровья в АНО ВО «Институт бизнеса и дизайна» созданы специальные условия для беспрепятственного доступа в учебные помещения и другие помещения, а также их пребывания в указанных помещениях с учетом особенностей психофизического развития, индивидуальных возможностей и состояния здоровья таких обучающихся.

При получении образования обучающимся с ограниченными возможностями здоровья при необходимости предоставляются бесплатно специальные учебники и учебные пособия, иная учебная литература. Также имеется возможность предоставления услуг ассистента, оказывающего обучающимся с ограниченными возможностями здоровья необходимую техническую помощь, в том числе услуг сурдопереводчиков и тифлосурдопереводчиков.

Получение доступного и качественного высшего образования лицами с ограниченными возможностями здоровья обеспечено путем создания в институте комплекса необходимых условий обучения для данной категории обучающихся. Информация о специальных условиях, созданных для обучающихся с ограниченными возможностями здоровья, размещена на сайте института (<https://obe.ru/sveden/ovz/>).

Для обучения инвалидов и лиц с ОВЗ, имеющих нарушения опорно-двигательного аппарата обеспечиваются и совершенствуются материально-технические условия беспрепятственного доступа в учебные помещения, столовую, туалетные, другие помещения, условия их пребывания в указанных помещениях (наличие пандусов, поручней, расширенных дверных проемов и др.).

Для адаптации к восприятию обучающимися инвалидами и лицами с ОВЗ с нарушенным слухом справочного, учебного материала, предусмотренного образовательной программой по выбранным направлениям подготовки, обеспечиваются следующие условия:

для лучшей ориентации в аудитории, применяются сигналы, оповещающие о начале и конце занятия (слово «звонок» пишется на доске);

внимание слабослышащего обучающегося привлекается педагогом жестом (на плечо кладется рука, осуществляется нерезкое похлопывание);

разговаривая с обучающимся, педагог смотрит на него, говорит ясно, короткими предложениями, обеспечивая возможность чтения по губам.

Компенсация затруднений речевого и интеллектуального развития слабослышащих инвалидов и лиц с ОВЗ проводится за счет:

использования схем, диаграмм, рисунков, компьютерных презентаций с гиперссылками, комментирующими отдельные компоненты изображения;

регулярного применения упражнений на графическое выделение существенных признаков предметов и явлений;

обеспечения возможности для обучающегося получить адресную консультацию по электронной почте по мере необходимости.

Для адаптации к восприятию инвалидами и лицами с ОВЗ с нарушениями зрения справочного, учебного, просветительского материала, предусмотренного образовательной программой АНО ВО «Институт бизнеса и дизайна» по выбранной специальности, обеспечиваются следующие условия:

ведется адаптация официального сайта в сети Интернет с учетом особых потребностей инвалидов по зрению, обеспечивается наличие крупношрифтовой справочной информации о расписании учебных занятий;

в начале учебного года обучающиеся несколько раз проводятся по зданию АНО ВО «Институт бизнеса и дизайна» для запоминания месторасположения кабинетов, помещений, которыми они будут пользоваться;

педагог, его собеседники, присутствующие представляются обучающимся, каждый раз называется тот, к кому педагог обращается;

действия, жесты, перемещения педагога коротко и ясно комментируются;

печатная информация предоставляется крупным шрифтом (от 18 пунктов), тотально озвучивается; обеспечивается необходимый уровень освещенности помещений;

предоставляется возможность использовать компьютеры во время занятий и право записи объяснения на диктофон (по желанию обучающегося).

Форма проведения текущей и промежуточной аттестации для обучающихся с ОВЗ определяется преподавателем в соответствии с учебным планом. При необходимости обучающемуся с ОВЗ с учетом его индивидуальных психофизических особенностей дается возможность пройти промежуточную аттестацию устно, письменно на бумаге, письменно на компьютере, в форме тестирования и т.п., либо предоставляется дополнительное время для подготовки ответа.

Автономная некоммерческая организация высшего образования
«ИНСТИТУТ БИЗНЕСА И ДИЗАЙНА»

Факультет управления бизнесом

Фонд оценочных средств

Текущего контроля и промежуточной аттестации
по дисциплине (модулю)

Б1.В.12 БИОМЕТРИЧЕСКИЕ СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ

Для направления подготовки:

09.03.02 Информационные системы и технологии
(уровень бакалавриата)

Типы задач профессиональной деятельности:

производственно-технологический; организационно-управленческий; проектный.

Направленность (профиль):

Информационные системы и технологии в бизнесе

Форма обучения:

очная, заочная

Москва – 2022

РЕЗУЛЬТАТЫ ОСВОЕНИЯ ДИСЦИПЛИНЫ ОБУЧАЮЩИМСЯ

Код и наименование компетенции	Индикаторы достижения компетенции	Результаты обучения
ПК-2 Способность выполнять работы по обеспечению функционирования баз данных и обеспечению их информационной безопасности	ПК-2.1 Знать: методы и способы обеспечения функционирования баз данных и обеспечения их информационной безопасности ПК-2.2 Уметь: выполнять работы по обеспечению функционирования баз данных и обеспечению их информационной безопасности ПК-2.3 Владеть: методами и способами выполнять работы по обеспечению функционирования баз данных и обеспечению их информационной безопасности	Знает: основные законодательные акты и специальные стандарты в области БСЗИ; классификацию средств БСЗИ Умеет: подбирать компоненты БСЗИ исходя из требований к их функционированию в различных производственных условиях; производить настройку компонентов БСЗИ Владеет: навыками разработки проектной и технической документации, проектируемой системы защиты информации, включающей биометрические средства защиты информации. навыками пользования БСЗИ.

ТИПОВЫЕ ОЦЕНОЧНЫЕ СРЕДСТВА, НЕОБХОДИМЫЕ ДЛЯ ОЦЕНКИ ПЛАНИРУЕМЫХ РЕЗУЛЬТАТОВ ОБУЧЕНИЯ ПО ДИСЦИПЛИНЕ (МОДУЛЮ):

ТЕКУЩИЙ КОНТРОЛЬ ПО УЧЕБНОЙ ДИСЦИПЛИНЕ (МОДУЛЮ)

Тест для формирования «ПК-2.1»

Вопрос №1 .

Информация это:

Варианты ответов:

1. сведения (сообщения, данные) независимо от формы представления
2. сведения о лицах, предметах, процессах, явлениях не зависимо от формы представления
3. сведения о носителях информации не зависимо от формы представления
4. сведения об информационном объекте не зависимо от формы представления

Вопрос №2 . Средство защиты информации это:

Варианты ответов:

1. техническое, программное средство, программно-техническое средство, вещество и/или материал, предназначенные или используемые для защиты информации.
2. средство, вещество и/или материал, предназначенные или используемые для защиты информации;
3. программное средство, и/или материал, предназначенные или используемые для защиты информации;
4. техническое, средство, и/или материал, предназначенные или используемые для защиты информации;

Вопрос №3 .

Угроза безопасности информации это:

Варианты ответов:

1. совокупность условий и факторов, создающих потенциальную или реально существующую опасность нарушения безопасности информации.
2. субъект (физическое лицо или физическое явление), являющийся непосредственной причиной

- возникновения угрозы безопасности информации;
- 3. субъект (физическое лицо или физическое явление), являющийся непосредственной причиной возникновения и реализации угрозы безопасности информации;
- 4. совокупность причин и условий, создающих потенциальную опасность нарушения безопасности информации;

Вопрос №4 . Защищаемая информация это:

Варианты ответов:

- 1. информация, являющаяся предметом собственности и подлежащая защите в соответствии с требованиями правовых документов или требованиями, устанавливаемыми собственником информации;
- 2. информация, подлежащая защите в соответствии с требованиями правовых документов или требований, устанавливаемыми собственником информации;
- 3. информация, являющаяся предметом собственности и подлежащая защите в соответствии с требованиями устанавливаемыми собственником информации;
- 4. деятельность, направленная на предотвращение несанкционированных и непреднамеренных воздействий на защищаемую информацию.

Вопрос №5 .

Источник угрозы безопасности информации это:

Варианты ответов:

- 1. субъект (физическое лицо или физическое явление), являющийся непосредственной причиной возникновения угрозы безопасности информации.
- 2. совокупность условий и факторов, создающих потенциальную или реально существующую опасность нарушения безопасности информации;
- 3. совокупность условий и факторов, создающих реальную опасность нарушения безопасности информации;
- 4. совокупность условий и факторов, создающих потенциальную опасность нарушения безопасности информации;

Критерии оценки выполнения задания

Оценка	Критерии оценивания
Неудовлетворительно	от 0% до 30% правильных ответов из общего числа тестовых заданий
Удовлетворительно	от 31% до 50% правильных ответов из общего числа тестовых заданий
Хорошо	от 51% до 80% правильных ответов из общего числа тестовых заданий
Отлично	от 81% до 100% правильных ответов из общего числа тестовых заданий

Практическое задание для формирования «ПК-2.2»

По выбранной теме представить теоретический материал, с приведением конкретных примеров:

- 1. Общая характеристика ИБ: определение понятий «Информационная безопасность», «Безопасность информации», «Защита информации».
- 2. Характеристика свойств безопасности информации: доступности, целостности, конфиденциальности.
- 3. «Концепция национальной безопасности Российской Федерации» роли и значении информационной безопасности в общей системе национальной безопасности РФ.
- 4. Назначение, дата принятия, общая структура «Доктрины информационной безопасности Российской Федерации» (ДИБ РФ).
- 5. ДИБ РФ: определение понятия «информационная безопасность Российской Федерации» (ИБ РФ).
- 6. ДИБ РФ: информационные интересы личности, общества и государства в информационной сфере.
- 7. ДИБ РФ: обобщённые группы информационных интересов РФ.
- 8. ДИБ РФ: источники и виды угроз информационной безопасности РФ.
- 9. ДИБ РФ: общее содержание угроз информационной безопасности.
- 10. ДИБ РФ: основные методы обеспечения ИБ РФ и их краткая характеристика.

11. Особенности методов обеспечения ИБ РФ в сфере экономики.
12. ДИБ РФ: структура и задачи государственной системы обеспечения ИБ РФ.
13. Сущность и содержание правового обеспечения ИБ (ОИБ).
14. Вертикальная структура правового ОИБ: назначение НПА каждого уровня.
15. Горизонтальная структура правового ОИБ: существо и примеры нормативно-правовых актов, содержащих отдельные информационно-правовые нормы в сфере ИБ.
16. Назначение (цели) и общая структура закона РФ «Об информации, информационных технологиях и о защите информации».
17. Назначение (цели) и общая структура закона РФ «О государственной тайне».
18. Назначение (цели) и общая структура закона РФ «О персональных данных».
19. Назначение (цели) и общая структура закона РФ «О коммерческой тайне».
20. Назначение (цели) и общая структура закона РФ «Об электронной цифровой подписи»
 1. Краткая характеристика компьютерных систем (КС) как объектов защиты информации (ЗИ).
 2. Общая структура, виды КС, особенности каждого вида КС с точки зрения ЗИ.
 3. Угрозы безопасности информации (БИ) в КС, основные признаки классификации угроз.
 4. Виды и существо случайных (непреднамеренных) угроз БИ в КС.
 5. Виды и существо преднамеренных угроз БИ в КС.
 6. Общие методы противодействия случайным (непреднамеренным) угрозам БИ в КС.
 7. Общие методы противодействия преднамеренным угрозам БИ в КС.
 8. Методы дублирования информации как мера защиты от случайных угроз.
 9. Повышение надёжности как способ противодействия случайным угрозам БИ в КС.
 10. Обеспечение отказоустойчивости как способ противодействия случайным угрозам БИ в КС.

Критерии оценки выполнения задания

Оценка	Критерии оценивания
Неудовлетворительно	Работа выполнена не полностью и объем выполненной части работы не позволяет сделать правильных выводов
Удовлетворительно	Работа выполнена не полностью, но не менее 50% объема, что позволяет получить правильные результаты и выводы; в ходе проведения работы были допущены ошибки
Хорошо	Работа выполнена в полном объеме с соблюдением необходимой последовательности действий, но допущена одна ошибка или не более двух недочетов и обучающийся может их исправить самостоятельно или с небольшой помощью преподавателя
Отлично	Работа выполнена в полном объеме без ошибок с соблюдением необходимой последовательности действий

Практическое задание для формирования «ПК-2.2»

Задача 1. Решение вспомогательных задач для усвоения теоретических основ ИБ. Диагностика и настройка персонального компьютера

Задания:

1. Настройка средств ввода-вывода операционной системы Windows.
2. Настройка элементов управления Windows.
3. Резервное копирование данных.
4. Проверка жесткого диска.

Задача 2. Формирование требований к системам защиты информации в виде профилей защиты в

рамках идеологии «Общих критериев».

Задания

1. Сформулируйте интересы государства, общества и личности в информационной сфере
2. Чем определяется ценность информации для владельца?
3. В чем заключается комплексное обеспечение ИБ РФ?
4. Каковы основные методы и средства защиты процессов переработки информации в защищенных КС?
5. Назовите основные принципы процессов переработки информации. 6. Назовите основные виды угроз.

Задача 3. Ознакомление со штатными средствами ОС по обеспечению информационной безопасности на примере WINDOWS .

Задания:

1. Создание и установка прав доступа пользователей.
2. Установка прав доступа к объектам

Задача 4. Защита документа в Microsoft Word. Восстановление текста, поврежденного документа. Изучить возможности ограничения изменений в документе:

Задания:

1. Установить в документе пароль для открытия документа, руководствуясь правилами, описанными в работе.
2. Установить в документе пароль разрешения записи.
3. Установить режим: Рекомендовать доступ только для чтения.
4. Проверить не содержит ли документ скрытых данных.
5. Изменить интервал времени автоматического сохранения документов.
6. Установить режим сохранения резервной копии документа.

Задача 5. Защита документа в MicrosoftExcel. Изучить возможности ограничения просмотра и изменения пользователями данных в электронных таблицах.

Задания:

1. Установить пароль для открытия книги.
2. Установить пароль для разрешения записи.
3. Установить защиту ячеек.

Критерии оценки выполнения задания

Оценка	Критерии оценивания
Неудовлетворительно	Работа выполнена не полностью и объем выполненной части работы не позволяет сделать правильных выводов
Удовлетворительно	Работа выполнена не полностью, но не менее 50% объема, что позволяет получить правильные результаты и выводы; в ходе проведения работы были допущены ошибки

Хорошо	Работа выполнена в полном объеме с соблюдением необходимой последовательности действий, но допущена одна ошибка или не более двух недочетов и обучающийся может их исправить самостоятельно или с небольшой помощью преподавателя
Отлично	Работа выполнена в полном объеме без ошибок с соблюдением необходимой последовательности действий

Практическое задание для формирования «ПК-2.3»

1. Опишите используемые при реализации политики ИБ стандарты, процессы и правила безопасности и отобразите схематически их взаимосвязь.
2. Перечислите государственные, ведомственные и организационные нормативные акты, регламентирующие защиту информации в издательской деятельности.
3. Перечислите возможные пути и методы несанкционированного доступа к источникам защищаемой информации.
4. Разработайте перечень организационно-правовых методов для построения вербального объекта защиты информации.
5. Отобразите схему разработки политики информационной безопасности для вербального предприятия.

Критерии оценки выполнения задания

Оценка	Критерии оценивания
Неудовлетворительно	Работа выполнена не полностью и объем выполненной части работы не позволяет сделать правильных выводов
Удовлетворительно	Работа выполнена не полностью, но не менее 50% объема, что позволяет получить правильные результаты и выводы; в ходе проведения работы были допущены ошибки
Хорошо	Работа выполнена в полном объеме с соблюдением необходимой последовательности действий, но допущена одна ошибка или не более двух недочетов и обучающийся может их исправить самостоятельно или с небольшой помощью преподавателя
Отлично	Работа выполнена в полном объеме без ошибок с соблюдением необходимой последовательности действий

Практическое задание для формирования «ПК-2.3»

1. Перечислите правовые нормы охраны интеллектуальной собственности на произведение паркового искусства.
2. Составьте перечень исключительных прав на литературное произведение.
3. Опишите имущественные и неимущественные права обладателя литературного произведения.
4. Составьте лицензионный договор на передачу прав пользования программным обеспечением.
5. Составьте сублицензионный договор на передачу прав художественного фильма.

Критерии оценки выполнения задания

Оценка	Критерии оценивания
Неудовлетворительно	Работа выполнена не полностью и объем выполненной части работы не позволяет сделать правильных выводов
Удовлетворительно	Работа выполнена не полностью, но не менее 50% объема, что позволяет получить правильные результаты и выводы; в ходе проведения работы были допущены ошибки

Хорошо	Работа выполнена в полном объеме с соблюдением необходимой последовательности действий, но допущена одна ошибка или не более двух недочетов и обучающийся может их исправить самостоятельно или с небольшой помощью преподавателя
Отлично	Работа выполнена в полном объеме без ошибок с соблюдением необходимой последовательности действий

Вопросы для проведения промежуточной аттестации по итогам освоения дисциплины

Тема 1. БСЗИ как часть информационной безопасности

1. Информационная безопасность.
2. Защита информации.
3. Составляющие информационной безопасности.
4. Целостность.
5. Доступность.
6. Конфиденциальность.
7. Взаимосвязь ИБ и ЗИ.
8. Механизмы обеспечения ИБ.
9. Идентификация и Аутентификация.
10. Виды идентификации.
11. Способы аутентификации.

Тема 2. Особенности биометрии в сфере защиты информации

12. Основные компоненты биометрических систем ЗИ.
13. Биометрические шаблоны, формирование Биометрических шаблонов.
14. Классификация методов аутентификации и идентификации в биометрических системах.
Примеры.
15. Характеристики в БСЗИ.
16. Преимущества и недостатки БСЗИ, как подсистемы идентификации и аутентификации.
17. Far и FRR.

Тема 3. Система стандартизации БСЗИ

18. Особенность выстраивания иерархии в Биометрических стандартов.
19. Международные и отечественные регуляторы в сфере биометрии и БСЗИ.
20. BioAri и Vari.
21. CBEFF.
22. X9.84.
23. Специализированные стандарты в БСЗИ.
24. Отечественные стандарты в Биометрии.

Тема 4. Основные методы биометрической идентификации

25. Основные методы биометрической идентификации.
26. Классификация биометрических средств ЗИ.
27. Классификация биометрических методов ИБ.
28. Системы по отпечаткам пальцев. На основании каких физических характеристик пальца можно составить биометрический шаблон?
29. Преимущества и недостатки метода отпечатка пальцев.
30. Системы по голосу. Какие физические характеристики входят в основу шаблона? Преимущества и недостатки.
31. Системы по радужной оболочке глаза. Преимущества и недостатки.
32. Основные подсистемы системы идентификации по радужной оболочке глаза. Статистические характеристики метода.
33. Системы идентификации и аутентификации по изображению лица. Классификация методов.
34. Системы идентификации и аутентификации по 2-d изображению лица. Преимущества и недостатки.
35. Особенности систем по 3-d распознаванию лица. Классификация систем и особенности.

Тема 5. Перспективные методы биометрической идентификации

36. Система распознавания по форме ушной раковины.
37. Перспективные методы БСЗИ.
38. Системы идентификации по геометрии руки. Виды систем. Преимущества и недостатки метода.
39. Метод распознавания по сетчатки глаза. Статистические показатели. Преимущества и недостатки.
40. Метод аутентификации и идентификации по венозному рисунку руки. Статистические показатели.
41. Классификация методов распознавания по почерку. Преимущества и недостатки.
42. Система электронного носа.

Тема 6. Применение биометрии в системах защиты информации

43. Применение биометрии в подсистемах безопасности и ИБ.
44. Механизм генерации ЭП с помощью биометрии.
45. Система BioLink Cl.
46. Применение технологий БСЗИ в картах Государственных систем социального обеспечения. Преимущества и недостатки
47. Возможности видеоаналитики в мониторинговых системах. Сферы и области применения.

Тема 7. Особенности правовой защиты биометрических баз данных

48. Основные положения ФЗ 152. В сфере защиты баз, содержащих биометрические ПД.
49. Основные положения ФЗ 152. Определение биометрические персональные данные.
50. Положение правительства №211 от 21.03.2012
51. Положение правительства №940 от 18.09.2009
52. Нормативные документы в сфере защиты биометрических систем ЗИ от Роскомнадзора.
53. Нормативные документы в сфере защиты биометрических систем ЗИ от ФСТЭК.
54. Нормативные документы в сфере защиты биометрических систем ЗИ от ФСБ.

Тема 8. Организация защиты Био ИСПДН

55. Политика оператора в отношении обработки ИСПДН.
56. Внутренние документы оператора ИСПДН в отношении системы обработки ПД.
57. Алгоритм действий для организации системы защиты ПД в нормативном правовом поле. Режимные мероприятия.
58. Организационные мероприятия, проводимые в отношении персонала, работающего с ПД оператором ИСПДН.
59. Классификация защищённости ИСПДН.
60. Распределение ответственности между исполнителями на стороне оператора за нарушения в сфере ИБ Биометрических персональных данных.
61. Перечень необходимых документов, связанных с функционированием ИСПДН, содержащим биометрические данные.

Тема 9. Обезличивание персональных данных

62. Свойства обезличенных данных
63. Полнота
64. Структурированность
65. Релевантность
66. Семантическая целостность
67. Применимость
68. Анонимность
69. Метод введения идентификаторов
70. Метод изменения состава или семантики
71. Метод декомпозиции
72. Метод перемешивания
73. Деобезличивание

Тема 10. Ответственность за несоблюдение законодательства в сфере сохранности биометрических БиоПД

74. Ответственность за неисполнение ФЗ 152.
 75. Виды ответственностей за нарушение в сфере БиоПД.
 76. Назовите виды правонарушений по Административной ответственности.
 77. Назовите виды правонарушений по Уголовной ответственности.
 78. Назовите виды правонарушений по Гражданско-правовой ответственности.
 79. Назовите виды правонарушений по Дисциплинарной ответственности.
 80. Назовите самое мелкое правонарушение с точки зрения законов РФ.
 81. Назовите самое крупное правонарушение с точки зрения законов РФ.

Уровни и критерии итоговой оценки результатов освоения дисциплины

	Критерии оценивания	Итоговая оценка
Уровень 1. Недостаточный	Незнание значительной части программного материала, неумение даже с помощью преподавателя сформулировать правильные ответы на задаваемые вопросы, невыполнение практических заданий	Неудовлетворительно/ Незачтено
Уровень 2. Базовый	Знание только основного материала, допустимы неточности в ответе на вопросы, нарушение логической последовательности в изложении программного материала, затруднения при решении практических задач	Удовлетворительно/ зачтено
Уровень 3. Повышенный	Твердые знания программного материала, допустимые несущественные неточности при ответе на вопросы, нарушение логической последовательности в изложении программного материала, затруднения при решении практических задач	Хорошо/ зачтено
Уровень 4. Продвинутый	Глубокое освоение программного материала, логически стройное его изложение, умение связать теорию с возможностью ее применения на практике, свободное решение задач и обоснование принятого решения	Отлично/ зачтено