МИНОБРНАУКИ РОССИИ

Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Российский государственный гуманитарный университет»
(ФГБОУ ВО «РГГУ»)

ИНСТИТУТ ИНФОРМАЦИОННЫХ НАУК И ТЕХНОЛОГИЙ БЕЗОПАСНОСТИ
ФАКУЛЬТЕТ ИНФОРМАЦИОННЫХ СИСТЕМ И БЕЗОПАСНОСТИ
Кафедра комплексной защиты информации

БИОМЕТРИЧЕСКИЕ СИСТЕМЫ АУТЕНТИФИКАЦИИ

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ
Направление подготовки 10.03.01 Информационная безопасность
Направленность (профиль) подготовки:
Безопасность автоматизированных систем
Уровень квалификации выпускника – бакалавр

Форма обучения очная

РПД адаптирована для лиц
с ограниченными возможностями
здоровья и инвалидов

Москва 2021

Биометрические системы аутентификации
Рабочая программа дисциплины
Составитель:
Кандидат технических наук, и.о. зав. кафедрой КЗИ Д.А. Митюшин

Ответственный редактор
Кандидат технических наук, и.о. зав. кафедрой КЗИ Д.А. Митюшин

УТВЕРЖДЕНО
Протокол заседания кафедры
комплексной защиты информации
№_10_ от__20.05.2021 г._____

ОГЛАВЛЕНИЕ

1. Пояснительная записка

1.1. Цель и задачи дисциплины:

Цель дисциплины – профессиональная подготовка студентов, необходимая для освоения методов и технологий, связанных с обеспечением безопасности автоматизированной системы от несанкционированного доступа.

Задачи дисциплины:
– получение систематизированных знаний о современных концепциях, методах и технологиях биометрии;
– формирование умений использовать современные достижения биометрии в области обеспечения безопасности автоматизированных систем от несанкционированного доступа посторонних лиц при реализации своей профессиональной деятельности;
– развитие аналитического мышления, умения строго излагать свои мысли, развитие способностей к обобщению и анализу информации, постановке целей и выбору путей ее достижения.

1.2. Перечень планируемых результатов обучения по дисциплине (модулю), соотнесённых с индикаторами достижения компетенций

Компетенция (код и наименование)	**Индикаторы компетенций** (код и наименование)	**Результаты обучения**
ОПК-4.1 Способен проводить организационные мероприятия по обеспечению безопасности информации в автоматизированных системах	*ОПК-4.1.1 Знает нормативные, руководящие и методические документы уполномоченных федеральных органов исполнительной власти по защите информации*	*Знать:* • *руководящие документы по защите информации с помощью биометрических систем.*
	ОПК-4.1.2 Умеет разрабатывать документы в области обеспечения безопасности информации в автоматизированной системе при ее эксплуатации (включая управление инцидентами информационной безопасности)	*Уметь:* • *разрабатывать документы в области обеспечения безопасности информации в АС при использовании биометрических технологий.*
	ОПК-4.1.3 Владеет навыками планирования мероприятий по обеспечению защиты информации и организацию работы персонала автоматизированной системы с учётом требований по защите информации	*Владеть:* • *практическими навыками по обеспечению защиты информации и организацию работы персонала АС при использовании биометрических технологий*
ПК-3 Способен управлять защитой информации в автоматизированных системах	*ПК-3.1 Знает основные методы управления защитой информации, информационные ресурсы автоматизированных систем, подлежащие защите;*	*Знать:* • *биометрические программно-аппаратные средства защиты информации автоматизированных*

	основные угрозы безопасности информации, модели нарушителя в автоматизированных системах	*систем.*
	ПК-3.2 *Умеет разрабатывать предложения по совершенствованию системы управления защиты информации автоматизированных систем; классифицировать и оценивать угрозы безопасности информации; оценивать информационные риски в автоматизированных системах*	*Уметь:* • *разрабатывать предложения по совершенствованию системы управления защиты информации автоматизированных систем*
	ПК-3.3 *Владеет навыками составления комплекса правил, процедур, практических приёмов, принципов и методов, средств обеспечения защиты информации в автоматизированной системе*	*Владеть:* • *навыками проектирования биометрических систем аутентификации в составе АС;* • *составления комплекса правил, процедур, практических приёмов, принципов и методов, средств обеспечения защиты информации в АС с использованием биометрических технологией.*
ПК-9 *Способен осуществлять подбор, изучение и обобщение научно-технической литературы, нормативных и методических материалов, составлять обзор по вопросам обеспечения информационной безопасности по профилю своей профессиональной деятельности*	*ПК-9.1* *Знает нормативные правовые акты в области защиты информации, национальные, межгосударственные и международные стандарты в области защиты информации, руководящие и методические документы уполномоченных федеральных органов исполнительной власти по защите информации*	*Знать:* • *требования нормативных и руководящих документов РФ по использованию биометрических технологий в защите информации АС*
	ПК-9.2 *Владеет организационными мерами по защите информации*	*Уметь:* • *разрабатывать нормативные документы по обеспечению безопасности АС с использованием биометрических технологий*
	ПК-9.3 *Умеет работать с*	*Владеть:* • *навыками работы с*

	программным обеспечением с соблюдением действующих требований по защите информации	*программным обеспечением биометрических систем аутентификации.*

1.3. Место дисциплины в структуре основной образовательной программы

Дисциплина «Биометрические системы аутентификации» относится к дисциплинам части, формируемой участниками образовательных отношений, блока дисциплин учебного плана.
Для освоения дисциплины необходимы знания, умения и владения, сформированные в ходе изучения следующих дисциплин и прохождения практик: «Математические основы защиты информации», «Интегрированные системы охраны», «Электроника и схемотехника».
В результате освоения дисциплины формируются знания, умения и владения, необходимые для изучения следующих дисциплин и прохождения практик: «Преддипломная практика».

2. Структура дисциплины

Структура дисциплины для очной формы обучения

Общая трудоёмкость дисциплины составляет _2_ з.е., _76__ ч., в том числе контактная работа обучающихся с преподавателем _40_ ч., промежуточная аттестация _-_ ч., самостоятельная работа обучающихся _36_ ч.

№ п/п	Темы дисциплины/	Семестр	Виды учебной работы (в часах)						Формы текущего контроля успеваемости, форма промежуточной аттестации *(по семестрам)*
			контактная					Самостоятельная работа	
			Лекции	Семинар	Практические занятия	Лабораторные занятия	Промежуточная аттестация		
1.	*Общие понятия о биометрии*	**7**	**2**	–	–	–	–	**2**	Устный опрос.
2.	*Правовые основы применения биометрических технологий в защите информации*	**7**	**2**	–	–	–	–	**2**	Устный опрос.
3.	*Структура и эффективность биометрических систем безопасности*	**7**	**2**	–	–	–	–	**2**	Устный опрос.
4.	*Технологии, основанные на анализе изображений пальцев рук*	**7**	**2**	–	–	–	–	**2**	Устный опрос.
5.	*Технологии, основанные на анализе изображения глаза*	**7**	**2**		–	–	–	**2**	Устный опрос.
6.	*Технологии, основанные на анализе изображения лица*	**7**	**2**					**2**	
7.	*Технологии, основанные на анализе геометрии контура кисти руки и рисунка вен*	**7**	**2**		–	–	–	**2**	Устный опрос.
8.	*Технологии, построенные на анализе голоса и динамических характеристик*	**7**	**2**		–	–	–	**2**	Устный опрос.
9.	*Практическая работа № 1. Освоение среды «Бионейроавтограф»*	**7**	–	–	**4**		–	**4**	Выполнение и защита практической работы.
10.	*Практическая работа № 2. Оценка вероятности ошибок второго рода*	**7**	–	–	**4**	–	–	**6**	Выполнение и защита практической работы.
11.	*Практическая работа № 3. Оценка вероятности ошибок первого рода*	**7**	–	–	**4**	–	–	**6**	Выполнение и защита практической работы.
12	*Практическая работа № 4. Коррекция ошибок выходных кодов нейронной сети за счёт*	**7**			**4**				Выполнение и защита практической

	введения в эти коды избыточности								работы.
13	*Практическая работа № 5. Работа с USB-сканером отпечатков пальцев*	**7**			**6**				Выполнение и защита практической работы.
.	*зачёт*	**7**	**–**	**–**	**2**	**–**	**–**	**4**	Зачёт по билетам
	Итого:		**16**		**24**			**36**	

3. Содержание дисциплины

№	Наименование раздела дисциплины	Содержание
1	***Тема 1. Общие понятия о биометрии***	Понятие о биометрии как научной дисциплине. Обзор технологий Основные термины. Классификация систем контролируемого обеспечения доступа. Виды биометрических параметров (физиологические, поведенческие). Краткий обзор существующих биометрических систем. Свойства биометрических параметров.
2	***Тема 2. Правовые основы применения биометрических технологий в защите информации***	Законодательные основы применения биометрических технологий в защите информации. Естественные ограничения, как причина сбоев биометрических систем. Атаки злоумышленников, как причина сбоев биометрических систем. Уязвимость биометрических систем. Требования к защищённости шаблонов, методы защиты. Морально-этические проблемы применения биометрии.
3	***Тема 3. Структура и эффективность биометрических систем безопасности***	Показатели эффективности биометрических методов и систем. Ошибки ложного отказа и ложного допуска, равный уровень ошибок. Области применения биометрических систем. Биометрическая система общего вида (описание и функции каждой подсистемы). Перспективы развития биометрических технологий. Показатели биометрических систем. Мультимодальные и многофакторные системы.
4	***Тема 4. Технологии, основанные на анализе изображений пальцев рук***	Описание папиллярных узоров. Виды сканеров (оптические, кремниевые, ультразвуковые, мультиспектральные). Методы распознавания изображений пальцев (корреляционное сравнение, сравнение по особым точкам, сравнение по узору).
5	***Тема 5. Технологии, основанные на анализе изображения глаза***	Строение глаза. Распознавание по радужной оболочке глаза. Общая схема. Проблемы анализа изображения радужной оболочки глаза. Использование изображения сетчатки глаза в качестве биометрической характеристики. Технология получения изображения. Преимущества и недостатки использования радужной оболочки и сетчатки при разграничении доступа.

6	***Тема 6. Технологии, основанные на анализе изображения лица***	Метод геометрических характеристик и его реализация. Гибкие контурные модели лица. Метод эластичных графов. Использование нейронных сетей. Распознавание человека по термограмме. Технологии, основанные на асимметрии тела (на примере асимметрии лица).
7	***Тема 7. Технологии, основанные на анализе геометрии контура кисти руки и рисунка вен***	Системы регистрации контура руки. Описание данных контура кисти руки с использованием 8-мисвязного цепного кода Фримена. Методы распознавания, основанные на геометрических характеристиках, на геометрических и образовых характеристиках, 3D-сканирование. Основные аспекты технологии идентификации по сосудистому руслу руки с использованием сети подкожных сосудов на тыльной стороне ладони.
8	***Тема 8. Технологии, построенные на анализе голоса и динамических характеристик***	Особенности биометрической идентификации личности по голосу. Основные этапы обработки речевого сигнала. Данные каналов динамики подписи. Построение кривых, отражающих динамику написания подписи. Наиболее часто извлекаемые характеристики динамики работы на клавиатуре. Биометрические технологии в будущем.

4. Образовательные технологии

№ п/п	Наименование раздела	Виды учебных занятий	Образовательные технологии
1	*Общие понятия о биометрии*	Лекция 1. Самостоятельная работа	Традиционная с использованием презентаций. Изучение материала по теме.
2	*Правовые основы применения биометрических технологий в защите информации*	Лекция 2. Самостоятельная работа	Традиционная с использованием презентаций. Изучение материала по теме.
3	*Структура и эффективность биометрических систем безопасности*	Лекция 3. Самостоятельная работа	Традиционная с использованием презентаций. Изучение материала по теме.
4	*Технологии, основанные на анализе изображений пальцев рук*	Лекция 4. Самостоятельная работа	Традиционная с использованием презентаций. Изучение материала по теме.
5	*Технологии, основанные на анализе изображения глаза*	Лекция 5. Самостоятельная работа	Традиционная с использованием презентаций. Изучение материала по теме.
6	*Технологии, основанные на анализе изображения лица*	Лекция 6. Самостоятельная работа	Традиционная с использованием презентаций. Изучение материала по теме.
7	*Технологии, основанные на анализе геометрии контура кисти руки и рисунка вен*	Лекция 7. Самостоятельная работа	Традиционная с использованием презентаций. Изучение материала по теме.
8	*Технологии, построенные на анализе голоса и динамических характеристик*	Лекция 8 Самостоятельная работа	Традиционная с использованием презентаций. Изучение материала по теме.
9	*Практическая работа № 1. Освоение среды «Бионейроавтограф»*	Практическая работа Самостоятельная работа	Выполнение и защита практической работы.
10	*Практическая работа № 2. Оценка вероятности ошибок второго рода*	Практическая работа Самостоятельная работа	Выполнение и защита практической работы.
11	*Практическая работа № 3. Оценка вероятности ошибок первого рода*	Практическая работа Самостоятельная работа	Выполнение и защита практической работы.
12	*Практическая работа № 4. Коррекция ошибок выходных кодов нейронной сети за счёт введения в эти коды избыточности*	Практическая работа Самостоятельная работа	Выполнение и защита практической работы.

13	*Практическая работа № 5. Работа с USB-сканером отпечатков пальцев*	Практическая работа Самостоятельная работа	Выполнение и защита практической работы.

5. Оценка планируемых результатов обучения

5.1. Система оценивания

Форма контроля	Макс. количество баллов	
	За одну работу	Всего
Текущий контроль:		
- опрос (темы 1-8) - практическое занятие (1-3)	3 12	24 36
Промежуточная аттестация зачёт		40 баллов
Итого за семестр зачёт		100 баллов

Перечень компетенций с указанием этапов их формирования в процессе освоения дисциплины представляется в виде таблицы:

№ п/п	***Контролируемые разделы (темы) дисциплины***	***Код контролируемой компетенции***	***Наименование оценочного средства***
1.	*Тема 1.*	ОПК-4.1.1, ОПК-4.1.2, ОПК-4.1.3, ПК-3.1, ПК-3.2, ПК-3.3, ПК-9.1, ПК-9.2, ПК-9.3	Опрос
2.	*Тема 2.*	ОПК-4.1.1, ОПК-4.1.2, ОПК-4.1.3, ПК-3.1, ПК-3.2, ПК-3.3, ПК-9.1, ПК-9.2, ПК-9.3	Опрос
3.	*Тема 3.*	ОПК-4.1.1, ОПК-4.1.2, ОПК-4.1.3, ПК-3.1, ПК-3.2, ПК-3.3, ПК-9.1, ПК-9.2, ПК-9.3	Опрос
4.	*Тема 4.*	ОПК-4.1.1, ОПК-4.1.2, ОПК-4.1.3, ПК-3.1, ПК-3.2, ПК-3.3, ПК-9.1, ПК-9.2, ПК-9.3	Опрос
5.	*Тема 5.*	ОПК-4.1.1, ОПК-4.1.2, ОПК-4.1.3, ПК-3.1, ПК-3.2, ПК-3.3, ПК-9.1, ПК-9.2, ПК-9.3	Опрос
6.	*Тема 6.*	ОПК-4.1.1, ОПК-4.1.2, ОПК-4.1.3, ПК-3.1, ПК-3.2, ПК-3.3, ПК-9.1, ПК-9.2, ПК-9.3	Опрос
7.	*Тема 7.*	ОПК-4.1.1, ОПК-4.1.2, ОПК-4.1.3, ПК-3.1, ПК-3.2, ПК-3.3, ПК-9.1, ПК-9.2, ПК-9.3	Опрос
8.	*Тема 8.*	ОПК-4.1.1, ОПК-4.1.2, ОПК-4.1.3, ПК-3.1, ПК-3.2, ПК-3.3, ПК-9.1, ПК-9.2, ПК-9.3	Опрос
10.	*Практическая работа № 1, 2, 3*	ОПК-4.1.1, ОПК-4.1.2, ОПК-4.1.3, ПК-3.1, ПК-3.2, ПК-3.3, ПК-9.1, ПК-9.2, ПК-9.3	План практического занятия

Полученный совокупный результат конвертируется в традиционную шкалу оценок и в шкалу оценок Европейской системы переноса и накопления кредитов (European Credit Transfer System; далее – ECTS) в соответствии с таблицей:

100-балльная шкала	Традиционная шкала		Шкала ECTS
95 – 100	отлично	зачтено	A
83 – 94			B
68 – 82	хорошо		C
56 – 67	удовлетворительно		D
50 – 55			E
20 – 49	неудовлетворительно	не зачтено	FX
0 – 19			F

5.2. Критерии выставления оценки по дисциплине

Баллы/ Шкала ECTS	Оценка по дисциплине	Критерии оценки результатов обучения по дисциплине
100-83/ A, B	«отлично»/ «зачтено (отлично)»/ «зачтено»	Выставляется обучающемуся, если он глубоко и прочно усвоил теоретический и практический материал, может продемонстрировать это на занятиях и в ходе промежуточной аттестации. Обучающийся исчерпывающе и логически стройно излагает учебный материал, умеет увязывать теорию с практикой, справляется с решением задач профессиональной направленности высокого уровня сложности, правильно обосновывает принятые решения. Свободно ориентируется в учебной и профессиональной литературе. Оценка по дисциплине выставляются обучающемуся с учётом результатов текущей и промежуточной аттестации. Компетенции, закреплённые за дисциплиной, сформированы на уровне – «высокий».
82-68/ C	«хорошо»/ «зачтено (хорошо)»/ «зачтено»	Выставляется обучающемуся, если он знает теоретический и практический материал, грамотно и по существу излагает его на занятиях и в ходе промежуточной аттестации, не допуская существенных неточностей. Обучающийся правильно применяет теоретические положения при решении практических задач профессиональной направленности разного уровня сложности, владеет необходимыми для этого навыками и приёмами. Достаточно хорошо ориентируется в учебной и профессиональной литературе. Оценка по дисциплине выставляются обучающемуся с учётом результатов текущей и промежуточной аттестации. Компетенции, закреплённые за дисциплиной, сформированы на уровне – «хороший».
67-50/ D, E	«удовлетворительно»/ «зачтено (удовлетворительно)»/ «зачтено»	Выставляется обучающемуся, если он знает на базовом уровне теоретический и практический материал, допускает отдельные ошибки при его изложении на занятиях и в ходе промежуточной аттестации. Обучающийся испытывает определённые затруднения в применении теоретических положений при решении

Баллы/ Шкала ECTS	Оценка по дисциплине	Критерии оценки результатов обучения по дисциплине
		практических задач профессиональной направленности стандартного уровня сложности, владеет необходимыми для этого базовыми навыками и приёмами. Демонстрирует достаточный уровень знания учебной литературы по дисциплине. Оценка по дисциплине выставляются обучающемуся с учётом результатов текущей и промежуточной аттестации. Компетенции, закреплённые за дисциплиной, сформированы на уровне – «достаточный».
49-0/ F,FX	«неудовлетворительно»/ не зачтено	Выставляется обучающемуся, если он не знает на базовом уровне теоретический и практический материал, допускает грубые ошибки при его изложении на занятиях и в ходе промежуточной аттестации. Обучающийся испытывает серьёзные затруднения в применении теоретических положений при решении практических задач профессиональной направленности стандартного уровня сложности, не владеет необходимыми для этого навыками и приёмами. Демонстрирует фрагментарные знания учебной литературы по дисциплине. Оценка по дисциплине выставляются обучающемуся с учётом результатов текущей и промежуточной аттестации. Компетенции на уровне «достаточный», закреплённые за дисциплиной, не сформированы.

5.3. Оценочные средства (материалы) для текущего контроля успеваемости, промежуточной аттестации обучающихся по дисциплине

Устный опрос

Устный опрос – это средство контроля, организованное как специальная беседа преподавателя с обучающимся на темы, связанные с изучаемой дисциплиной, и рассчитанное на выяснение объёма знаний обучающегося по определённому разделу, теме, проблеме и т.п.

Перечень устных вопросов для проверки знаний

№	Вопрос	Реализуемая компетенция
1.	Назовите классические способы аутентификации	ОПК-4.1.2, ОПК-4.1.3, ПК-3.1, ПК-3.2, ПК-3.3, ПК-9.1, ПК-9.2, ПК-9.3
2.	Назовите и поясните два аутентификационных метода биометрии	ОПК-4.1.3, ПК-3.1, ПК-3.2, ПК-3.3, ПК-9.1, ПК-9.2, ПК-9.3
3.	Назовите пять свойств биометрических параметров	ПК-3.1, ПК-3.2, ПК-3.3, ПК-9.1, ПК-9.2, ПК-9.3
4.	Назовите наиболее часто используемые биометрические параметры	ПК-3.1, ПК-3.2, ПК-3.3, ПК-9.1, ПК-9.2, ПК-9.3
5.	Что такое положительная и отрицательная идентификация?	ОПК-4.1.1, ОПК-4.1.2, ОПК-4.1.3, ПК-3.1, ПК-3.2, ПК-3.3, ПК-9.1, ПК-9.2, ПК-9.3

6.	Отличие биометрической верификации от биометрической идентификации	ПК-3.1, ПК-3.2, ПК-3.3, ПК-9.1, ПК-9.2, ПК-9.3
7.	Назовите два возможных вида базы данных биометрической идентификации	ПК-3.1, ПК-3.2, ПК-3.3, ПК-9.1, ПК-9.2
8.	В чём отличие положительной биометрической регистрации от отрицательной	ОПК-4.1.1, ОПК-4.1.2, ОПК-4.1.3, ПК-3.1, ПК-3.2, ПК-3.3
9.	Основные нормативные правовые акты регламентирующие использование биометрии при защите информации	ОПК-4.1.1, ОПК-4.1.2, ОПК-4.1.3, ПК-3.1, ПК-3.2, ПК-3.3, ПК-9.1, ПК-9.2, ПК-9.3
10.	Назовите причины сбоев биометрических систем	ПК-3.1, ПК-3.2, ПК-3.3, ПК-9.1, ПК-9.2, ПК-9.3
11.	Перечислите уязвимости биометрических систем	ПК-3.1, ПК-3.2, ПК-3.3, ПК-9.1, ПК-9.2, ПК-9.3
12.	Назовите основные паттерны папиллярных узоров	ОПК-4.1.1, ОПК-4.1.2, ОПК-4.1.3, ПК-3.1, ПК-3.2, ПК-3.3, ПК-9.1, ПК-9.2, ПК-9.3
13.	Назовите методы считывания информации о папиллярных узорах	ОПК-4.1.1, ОПК-4.1.2, ОПК-4.1.3, ПК-3.1, ПК-3.2, ПК-3.3, ПК-9.1, ПК-9.2, ПК-9.3
14.	Способы получения изображения при распознавании лица	ОПК-4.1.1, ОПК-4.1.2, ОПК-4.1.3, ПК-3.1, ПК-3.2, ПК-3.3, ПК-9.1, ПК-9.2, ПК-9.3
15.	Сложности при распознавании лиц	ОПК-4.1.1, ОПК-4.1.2, ОПК-4.1.3, ПК-3.1, ПК-3.2, ПК-3.3, ПК-9.1, ПК-9.2, ПК-9.3
16.	Охарактеризуйте ошибки ложного отказа и ложного допуска	ОПК-4.1.1, ОПК-4.1.2, ОПК-4.1.3, ПК-3.1, ПК-3.2, ПК-3.3, ПК-9.1, ПК-9.2, ПК-9.3
17.	Преимущества и недостатки использование радужной оболочки глаза в качестве биометрической характеристики	ОПК-4.1.1, ОПК-4.1.2, ОПК-4.1.3, ПК-3.1, ПК-3.2, ПК-3.3, ПК-9.1, ПК-9.2, ПК-9.3
18.	Преимущества и недостатки использование сетчатки в качестве биометрической характеристики	ОПК-4.1.1, ОПК-4.1.2, ОПК-4.1.3, ПК-3.1, ПК-3.2, ПК-3.3, ПК-9.1, ПК-9.2, ПК-9.3
19.	Особенности распознавания лица по термограмме	ОПК-4.1.1, ОПК-4.1.2, ОПК-4.1.3, ПК-3.1, ПК-3.2, ПК-3.3, ПК-9.1, ПК-9.2, ПК-9.3
20.	Назовите системы регистрации контура руки.	ОПК-4.1.1, ОПК-4.1.2, ОПК-4.1.3, ПК-3.1, ПК-3.2, ПК-3.3, ПК-9.1, ПК-9.2, ПК-9.3
21.	Особенности атак на верификацию голоса	ОПК-4.1.1, ОПК-4.1.2,

		ОПК-4.1.3, ПК-3.1, ПК-3.2, ПК-3.3, ПК-9.1, ПК-9.2, ПК-9.3
22.	Особенности верификации по клавиатурному почерку	ОПК-4.1.1, ОПК-4.1.2, ОПК-4.1.3, ПК-3.1, ПК-3.2, ПК-3.3, ПК-9.1, ПК-9.2, ПК-9.3

Промежуточная аттестация (зачёт) – проверка сформированности компетенций – ОПК-4.1, ПК-3, ПК-9

№	Вопрос	Реализуемая компетенция
1.	Классификация систем контролируемого обеспечения доступа. Краткий обзор существующих биометрических систем.	ОПК-4.1.1, ОПК-4.1.2, ОПК-4.1.3, ПК-3.1, ПК-3.2, ПК-3.3, ПК-9.1, ПК-9.2, ПК-9.3
2.	Виды биометрических параметров. Свойства биометрических параметров.	ОПК-4.1.2, ОПК-4.1.3, ПК-3.1, ПК-3.2, ПК-3.3, ПК-9.1, ПК-9.2, ПК-9.3
3.	Законодательные основы применения биометрических технологий в защите информации	ОПК-4.1.1, ОПК-4.1.2, ОПК-4.1.3, ПК-3.1, ПК-3.2, ПК-3.3,
4.	Уязвимость биометрических систем. Требования к защищённости шаблонов, методы защиты.	ОПК-4.1.1, ОПК-4.1.2, ОПК-4.1.3, ПК-3.1, ПК-3.2, ПК-3.3, ПК-9.1, ПК-9.2, ПК-9.3
5.	Морально-этические проблемы применения биометрии.	ОПК-4.1.1, ОПК-4.1.2, ОПК-4.1.3, ПК-3.1, ПК-3.2, ПК-3.3,
6.	Показатели эффективности биометрических методов и систем. Ошибки ложного отказа и ложного допуска, равный уровень ошибок.	ОПК-4.1.1, ОПК-4.1.2, ОПК-4.1.3, ПК-3.1, ПК-3.2, ПК-3.3, ПК-9.1, ПК-9.2, ПК-9.3
7.	Области применения биометрических систем. Биометрическая система общего вида (описание и функции каждой подсистемы).	ОПК-4.1.1, ОПК-4.1.2, ОПК-4.1.3, ПК-3.1, ПК-3.2, ПК-3.3, ПК-9.1, ПК-9.2, ПК-9.3
8.	Перспективы развития биометрических технологий. Показатели биометрических систем.	ОПК-4.1.1, ОПК-4.1.2, ОПК-4.1.3, ПК-3.1, ПК-3.2, ПК-3.3, ПК-9.1, ПК-9.2, ПК-9.3
9.	Мультимодальные и многофакторные биометрические системы.	ОПК-4.1.1, ОПК-4.1.2, ОПК-4.1.3, ПК-3.1, ПК-3.2, ПК-3.3, ПК-9.1, ПК-9.2, ПК-9.3
10.	Описание и классификация папиллярных узоров	ОПК-4.1.1, ОПК-4.1.2, ОПК-4.1.3, ПК-3.1, ПК-3.2, ПК-3.3, ПК-9.1, ПК-9.2, ПК-9.3
11.	Виды сканеров папиллярных узоров	ПК-3.1, ПК-3.2, ПК-3.3, ПК-9.1, ПК-9.2, ПК-9.3
12.	Методы распознавания изображений папиллярных узоров	ОПК-4.1.1, ОПК-4.1.2, ОПК-4.1.3, ПК-3.1, ПК-3.2,

		ПК-3.3, ПК-9.1, ПК-9.2, ПК-9.3
13.	Распознавание по радужной оболочке глаза. Общая схема. Проблемы анализа изображения радужной оболочки глаза.	ОПК-4.1.1, ОПК-4.1.2, ОПК-4.1.3, ПК-3.1, ПК-3.2, ПК-3.3, ПК-9.1, ПК-9.2, ПК-9.3
14.	Использование изображения сетчатки глаза в качестве биометрической характеристики. Технология получения изображения	ОПК-4.1.1, ОПК-4.1.2, ОПК-4.1.3, ПК-3.1, ПК-3.2, ПК-3.3, ПК-9.1, ПК-9.2, ПК-9.3
15.	Преимущества и недостатки использования радужной оболочки и сетчатки при разграничении доступа	ОПК-4.1.1, ОПК-4.1.2, ОПК-4.1.3, ПК-3.1, ПК-3.2, ПК-3.3, ПК-9.1, ПК-9.2, ПК-9.3
16.	Метод геометрических характеристик при анализе изображения лица и его реализация	ОПК-4.1.1, ОПК-4.1.2, ОПК-4.1.3, ПК-3.1, ПК-3.2, ПК-3.3, ПК-9.1, ПК-9.2, ПК-9.3
17.	Гибкие контурные модели лица.	ПК-3.1, ПК-3.2, ПК-3.3, ПК-9.1, ПК-9.2, ПК-9.3
18.	Метод эластичных графов при анализе изображения лица	ОПК-4.1.1, ОПК-4.1.2, ОПК-4.1.3, ПК-3.1, ПК-3.2, ПК-3.3, ПК-9.1, ПК-9.2, ПК-9.3
19.	Использование нейронных сетей при анализе изображения лица.	ПК-3.1, ПК-3.2, ПК-3.3, ПК-9.1, ПК-9.2, ПК-9.3
20.	Распознавание человека по термограмме.	ОПК-4.1.1, ОПК-4.1.2, ОПК-4.1.3, ПК-3.1, ПК-3.2, ПК-3.3, ПК-9.1, ПК-9.2, ПК-9.3
21.	Технологии, основанные на асимметрии тела (на примере асимметрии лица).	ОПК-4.1.1, ОПК-4.1.2, ОПК-4.1.3, ПК-3.1, ПК-3.2, ПК-3.3, ПК-9.1, ПК-9.2, ПК-9.3
22.	Системы регистрации контура руки.	ОПК-4.1.1, ОПК-4.1.2, ОПК-4.1.3, ПК-3.1, ПК-3.2, ПК-3.3, ПК-9.1, ПК-9.2, ПК-9.3
23.	Описание данных контура кисти руки с использованием 8-мисвязного цепного кода Фримена.	ОПК-4.1.1, ОПК-4.1.2, ОПК-4.1.3, ПК-3.1, ПК-3.2, ПК-3.3, ПК-9.1, ПК-9.2, ПК-9.3
24.	Методы распознавания, основанные на геометрических характеристиках, на геометрических и образовых характеристиках, 3D-сканирование.	ОПК-4.1.1, ОПК-4.1.2, ОПК-4.1.3, ПК-3.1, ПК-3.2, ПК-3.3, ПК-9.1, ПК-9.2, ПК-9.3
25.	Основные аспекты технологии идентификации по сосудистому руслу руки с использованием сети подкожных сосудов на тыльной стороне ладони.	ОПК-4.1.1, ОПК-4.1.2, ОПК-4.1.3, ПК-3.1, ПК-3.2, ПК-3.3, ПК-9.1, ПК-9.2, ПК-9.3
26.	Особенности биометрической идентификации личности по голосу. Основные этапы обработки	ОПК-4.1.1, ОПК-4.1.2, ОПК-4.1.3, ПК-3.1, ПК-3.2,

	речевого сигнала.	ПК-3.3, ПК-9.1, ПК-9.2, ПК-9.3
27.	Данные каналов динамики подписи. Построение кривых, отражающих динамику написания подписи.	ОПК-4.1.1, ОПК-4.1.2, ОПК-4.1.3, ПК-3.1, ПК-3.2, ПК-3.3, ПК-9.1, ПК-9.2, ПК-9.3
28.	Наиболее часто извлекаемые характеристики динамики работы на клавиатуре	ОПК-4.1.1, ОПК-4.1.2, ОПК-4.1.3, ПК-3.1, ПК-3.2, ПК-3.3, ПК-9.1, ПК-9.2, ПК-9.3

Примерные тестовые задания – проверка сформированности компетенций – ОПК-4.1, ПК-3, ПК-9

1. Выберите два аутентификационных метода в биометрии:
1) верификация;
2) авторизация;
3) идентификация.;
4) концентрация

6. Учебно-методическое и информационное обеспечение дисциплины

6.1. Список источников и литературы

Источники

Основные

1. Доктрина информационной безопасности РФ. Утверждена Президентом Российской Федерации от 05.12.2016г. №646. [Электронный ресурс]: Режим доступа: https://rg.ru/2016/12/06/doktrina-infobezobasnost-site-dok.html, свободный. - Загл. с экрана.
2. Федеральный закон РФ «Об информации, информационных технологиях и о защите информации» от 27 июля 2006 № 149-ФЗ. [Электронный ресурс]: Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_61798/, свободный. – Загл. с экрана.
3. Федеральный закон РФ «О персональных данных» от 27 июля 2006 № 152-ФЗ. [Электронный ресурс]: Режим доступа: http://www.consultant.ru/document/ cons_doc_LAW_61801/, свободный. – Загл. с экрана.
4. Приказ Министерства цифрового развития, связи и массовых коммуникаций Российской Федерации от 21.06.2018 № 307 «Об утверждении методик проверки соответствия предоставленных биометрических персональных данных физического лица его биометрическим персональным данным, содержащимся в единой информационной системе персональных данных, обеспечивающей обработку, включая сбор и хранение биометрических персональных данных, их проверку и передачу информации о степени их соответствия предоставленным биометрическим персональным данным гражданина Российской Федерации, а также об определении степени взаимного соответствия указанных биометрических персональных данных, достаточной для проведения идентификации, предусмотренной Федеральным законом от 27 июля 2006 года № 149-ФЗ «Об информации, информационных технологиях и о защите информации» [Электронный ресурс]: Режим доступа: http://publication.pravo.gov.ru/Document/View/ 0001201807060018
5. Приказ Министерства цифрового развития, связи и массовых коммуникаций РФ от 25 июня 2018 г. № 321 «Об утверждении порядка обработки, включая сбор и хранение, параметров биометрических персональных данных в целях идентификации, порядка размещения и обновления биометрических персональных данных в единой биометрической системе, а также требований к информационным технологиям и техническим средствам, предназначенным для обработки биометрических персональных данных в целях проведения идентификации” [Электронный ресурс]: Режим доступа: https://www.garant.ru/products/ipo/prime/doc/71885302/

Дополнительные

6. Постановление Правительства Российской Федерации от 6 июля 2008 г. № 512 «Об утверждении требований к материальным носителям биометрических персональных данных и технологиям хранения таких данных вне информационных систем персональных данных». [Электронный ресурс]: Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_78154/
7. ГОСТ Р ИСО/МЭК 19795-1-2007 «Автоматическая идентификация. Идентификация биометрическая. Эксплуатационные испытания и протоколы испытаний в биометрии. Часть 1. Принципы и структура» [Электронный ресурс]: Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_260066/
8. ГОСТ Р ИСО/МЭК 19784-1-2007 «Автоматическая идентификация. Идентификация биометрическая. Биометрический программный интерфейс. Часть 1. Спецификация». [Электронный ресурс]: Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_260065/
9. ГОСТ Р ИСО/МЭК 19794, который определяет требования ко всем основным биометрическим параметрам и к их измерению. Части 1-14 [Электронный ресурс]: Режим доступа: http://www.consultant.ru/

Литература

Основная

1. *Брюхомицкий, Ю. А* Биометрические технологии идентификации личности : учебное пособие / Ю. А. Брюхомицкий ; Южный федеральный университет. – Ростов-на-Дону ; Таганрог : Издательство Южного федерального университета, 2017. – 263 с. – ISBN 978-5-9275-2454-9. – Текст : электронный. – URL: https://znanium.com/catalog/product/1021574 (дата обращения: 10.05.2021). – Режим доступа: по подписке.

Дополнительная

2. *Мытник, К. Я.* Смарт-карты и информационная безопасность / К. Я. Мытник, С. П. Панасенко ; под редакцией В. Ф. Шаньгина. – Москва : ДМК Пресс, 2018. – 516 с. – ISBN 978-5-97060-690-2. — Текст : электронный // Лань : электронно-библиотечная система. – URL: https://e.lanbook.com/book/116128 (дата обращения: 10.05.2021). -- Режим доступа: для авториз. пользователей..
3. *Ворона, В. А.* Системы контроля и управления доступом / В. А. Ворона, В. А. Тихонов. – Москва : Горячая линия-Телеком, 2018. – 272 с. – ISBN 978-5-9912-0059-2. – Текст : электронный // Лань : электронно-библиотечная система. – URL: https://e.lanbook.com/book/111037 (дата обращения: 10.05.2021). -- Режим доступа: для авториз. пользователей.

6.2. Перечень ресурсов информационно-телекоммуникационной сети «Интернет»

1. Среда моделирования «Бионейронавтограф» [Электронный ресурс]. – Режим доступа свобод.: http://пниэи.рф/activity/science/noc.htm
2. Информационный бюллетень Jet Info [Электронный ресурс]. – Электрон. дан. – [М., 2014]. – Режим доступа свобод.: http://www.jetinfo.ru/ .
3. Glossary Commander. Служба тематических толковых словарей [Электронный ресурс]. – Электрон. дан. - [М., 2008]. - Режим доступа свобод.: http://glossary.ru/ .
4. Сайт справочно-правовой системы по федеральному и региональным законодательствам России - Режим доступа свобод.: http://pravo.ru/
5. Информационный портал в области защиты информации Режим доступа свобод.: http://www.securitylab.ru
6. Портал ФСТЭК http://www.fstec.ru

7. Материально-техническое обеспечение дисциплины

Для материально-технического обеспечения дисциплины необходимо:
1) для лекционных занятий – лекционный класс с видеопроектором и компьютером, на котором должно быть установлено следующее ПО:

№п/п	Наименование ПО	Производитель	Способ распространения
1	Microsoft Office 2010	Microsoft	лицензионное
2	Windows 7 Pro	Microsoft	лицензионное
3	Kaspersky Endpoint Security	Kaspersky	лицензионное

2) для практических занятий – компьютерный класс, оборудованный современными персональными компьютерами для каждого студента. На компьютере должны быть установлено следующее ПО:

№п/п	Наименование ПО	Производитель	Способ распространения
1	Microsoft Office 2010	Microsoft	лицензионное
2	Windows 10 Pro	Microsoft	лицензионное
3	Kaspersky Endpoint Security	Kaspersky	лицензионное

Для проведения занятий лекционного типа предлагаются тематические иллюстрации в формате презентаций PowerPoint.

Перечень БД и ИСС

№п/п	Наименование
1	Международные реферативные наукометрические БД, доступные в рамках национальной подписки в 2020 г. Web of Science Scopus
2	Профессиональные полнотекстовые БД, доступные в рамках национальной подписки в 2020 г. Журналы Cambridge University Press ProQuest Dissertation & Theses Global SAGE Journals Журналы Taylor and Francis
3	Профессиональные полнотекстовые БД JSTOR Издания по общественным и гуманитарным наукам Электронная библиотека Grebennikon.ru
4	Компьютерные справочные правовые системы Консультант Плюс, Гарант

8. Обеспечение образовательного процесса для лиц с ограниченными возможностями здоровья и инвалидов

В ходе реализации дисциплины используются следующие дополнительные методы обучения, текущего контроля успеваемости и промежуточной аттестации обучающихся в зависимости от их индивидуальных особенностей:

- для слепых и слабовидящих:

– лекции оформляются в виде электронного документа, доступного с помощью компьютера со специализированным программным обеспечением;

– письменные задания выполняются на компьютере со специализированным программным обеспечением, или могут быть заменены устным ответом;

– обеспечивается индивидуальное равномерное освещение не менее 300 люкс;

– для выполнения задания при необходимости предоставляется увеличивающее устройство; возможно также использование собственных увеличивающих устройств;

– письменные задания оформляются увеличенным шрифтом;

– экзамен и зачёт проводятся в устной форме или выполняются в письменной форме на компьютере.

- для глухих и слабослышащих:

– лекции оформляются в виде электронного документа, либо предоставляется звукоусиливающая аппаратура индивидуального пользования;

– письменные задания выполняются на компьютере в письменной форме;

– экзамен и зачёт проводятся в письменной форме на компьютере; возможно проведение в форме тестирования.

- для лиц с нарушениями опорно-двигательного аппарата:

– лекции оформляются в виде электронного документа, доступного с помощью компьютера со специализированным программным обеспечением;

– письменные задания выполняются на компьютере со специализированным программным обеспечением;

– экзамен и зачёт проводятся в устной форме или выполняются в письменной форме на компьютере.

При необходимости предусматривается увеличение времени для подготовки ответа.

Процедура проведения промежуточной аттестации для обучающихся устанавливается с учётом их индивидуальных психофизических особенностей. Промежуточная аттестация может проводиться в несколько этапов.

При проведении процедуры оценивания результатов обучения предусматривается использование технических средств, необходимых в связи с индивидуальными особенностями обучающихся. Эти средства могут быть предоставлены университетом, или могут использоваться собственные технические средства.

Проведение процедуры оценивания результатов обучения допускается с использованием дистанционных образовательных технологий.

Обеспечивается доступ к информационным и библиографическим ресурсам в сети Интернет для каждого обучающегося в формах, адаптированных к ограничениям их здоровья и восприятия информации:

- для слепых и слабовидящих:

– в печатной форме увеличенным шрифтом;

– в форме электронного документа;

– в форме аудиофайла.

- для глухих и слабослышащих:

– в печатной форме;

– в форме электронного документа.

- для обучающихся с нарушениями опорно-двигательного аппарата:

– в печатной форме;
– в форме электронного документа;
– в форме аудиофайла.

Учебные аудитории для всех видов контактной и самостоятельной работы, научная библиотека и иные помещения для обучения оснащены специальным оборудованием и учебными местами с техническими средствами обучения:

- для слепых и слабовидящих:
  – устройством для сканирования и чтения с камерой SARA CE;
  – дисплеем Брайля PAC Mate 20;
  – принтером Брайля EmBraille ViewPlus;
- для глухих и слабослышащих:
  – автоматизированным рабочим местом для людей с нарушением слуха и слабослышащих;
  – акустический усилитель и колонки;
- для обучающихся с нарушениями опорно-двигательного аппарата:
  – передвижными, регулируемыми эргономическими партами СИ-1;
  – компьютерной техникой со специальным программным обеспечением.

9. Методические материалы

9.1. Планы практических занятий – проверка сформированности компетенций – ОПК-4.1, ПК-3, ПК-9

Темы учебной дисциплины предусматривают проведение практических занятий, которые служат как целям текущего и промежуточного контроля за подготовкой студентов, так и целям получения практических навыков применения методов выработки решений, закрепления изученного материала, развития умений, приобретения опыта решения конкретных проблем, ведения дискуссий, аргументации и защиты выбранного решения. Помощь в этом оказывают задания для практических занятий, выдаваемые преподавателем на каждом занятии.
Целью практических занятий является закрепление теоретического материала и приобретение практических навыков работы с соответствующим оборудованием, программным обеспечением и нормативными правовыми документами.
Тематика практических занятий соответствует программе дисциплины.

Практическая работа № 1 (4 ч.). Освоение среды «Бионейроавтограф» – ОПК-4.1, ПК-3, ПК-9

Цели работы:
– ознакомление со средой моделирования «Бионейроавтограф»
Задания:
1. Запустить файл «бионейроавтограф.exe»:
2. Задать простой пароль и рукописный образ.
3. Обучить систему.
4. Изменить пароль на случайный 32-х символьный код. Для создания случайного пароля нажать клавишу «Автоматически сгенерировать новый пароль».
5. Переобучить систему на новом пароле.
6. В поле ввода введите любую другую букву и нажмите «Проверить». Если система обучена правильно, то появится сообщение о вводе неверного пароля и загорится красный сигнал светофора. Если введённый образ похож на обучающий, то может загореться жёлтый сигнал светофора. Нажать «ОК».
7. Ввести неверный символ. Посмотреть реакцию системы.

Указания по выполнению заданий:
1. На компьютере должна быть установлена программа «БиоНейроАвтограф».
2. Ответить на вопросы при защите работы

Материально-техническое обеспечение занятия:
1. Компьютеры по количеству обучающихся с развёрнутой ОС MS Windows, программным пакетом MS Office v.2010 и программой «БиоНейроАвтограф».

Список литературы:
1. *Брюхомицкий, Ю.А.* Биометрические технологии идентификации личности : учебное пособие / Ю. А. Брюхомицкий ; Южный федеральный университет. – Ростов-на-Дону ; Таганрог : Издательство Южного федерального университета, 2017. – 263 с. – ISBN 978-5-9275-2454-9. – Текст : электронный. – URL: https://znanium.com/catalog/product/1021574 (дата обращения: 10.05.2021). – Режим доступа: по подписке.
2. Среда моделирования «Бионейронавтограф» [Электронный ресурс]. – Режим доступа свобод.: http://пниэи.рф/activity/science/noc.htm.
3. Материалы лекций

Практическая работа № 2 (4 ч.). Оценка вероятности ошибок второго рода – проверка сформированности компетенций – ОПК-4.1, ПК-3, ПК-9

Цели работы:
– оценить вероятности ошибок второго рода (пропуск «Чужого») по ГОСТ Р 52633.3-2011

используя статистики расстояний Хэмминга.
– закрепление навыков работы с программой «БиоНейроАвтограф».

Задания:

1. Запустить файл «бионейроавтограф.exe».
2. Задать 32-х символьный простой пароль и рукописный образ.
3. Обучить систему.
4. Провести тестирование, введя другой рукописный символ.
5. Отображённое на экранной форме число несовпавших символов двоичного ключа (30) является расстоянием Хэмминга между кодом «Свой» рукописного образа «а» и кодом «Чужой» рукописного образа «к».
6. Собрать статистику, введя другие рукописные символы образов «Чужой» и заполнить таблицу 1 например:

Таблица №1.

Попытка / Образ	Расстояния Хэмминга до образа "*а*"									
	1	2	3	4	5	6	7	8	9	10
"*к*"	30	21	16	52	33	8	41	19	24	64
"*н*"	7	27	6	16	4	5	8	20	11	31
"*у*"	27	82	44	49	21	51	101	111	67	77
"*о*"	21	30	34	26	20	96	19	51	8	10
"*е*"	64	44	56	94	78	101	90	107	103	99

7. По каждой строке таблицы 1 вычислить математическое ожидание E(h) и стандартное отклонение σ(h) расстояний Хэмминга, данные сведите в таблицу 2, например:

Таблица № 2

Символ	E(h)	σ(h)	$P_{2,"."}$
"*к*"	30.8	16.37	0.037
"*н*"	13.5	9.13	0.085
"*у*"	63.1	28.4	0.054
"*о*"	31.5	24.48	0.106
"*е*"	85.6	23.78	0.0037

8. Располагая данными о математическом ожидании и стандартном отклонении рассчитайте вероятности ошибок второго рода для каждого из использованных рукописных образов « . », пользуясь гипотезой нормального закона распределения расстояний Хэмминга:

$$P_{2,"."} \approx \frac{1}{\sigma(h)\sqrt{2\pi}} \int_{-\infty}^{0} \exp\left\{\frac{-\left(E(h)-u\right)^2}{2\sigma^2(h)}\right\} du \qquad (1)$$

9. Вычислить для всех введённых биометрических образов усреднённую вероятность ошибки второго рода:

$$P_2 = \frac{0.037 + 0.085 + 0.054 + 0.106 + 0.0037}{5} = 0.057$$

10. Оценить стойкость к атакам подбора как обратную величину усреднённой вероятности ошибки второго рода:

$$(P_2)^{-1} \approx \frac{1}{0.057} = 17.5$$

11. Сделать вывод. Например, для рассматриваемого примера:

Рукописный биометрический образ «а», состоящий из одного символа, воспроизведённый манипулятором «мышь», является очень слабой защитой. Для её преодоления достаточно примерно 17 попыток атаки воспроизведения пароля, если злоумышленник знает, что пароль состоит из одного рукописного символа

12. Повторите численный эксперимент для ситуации, когда злоумышленник не знает длину рукописного пароля. Для этой цели введите пароль из одной рукописной буквы «п», затем пароль из двух рукописных букв «пг», затем пароль из трёх рукописных букв «пгу».

13. Полученные данные сведите в таблицу 3, например:

Таблица 3.

Попытка / Образ	Расстояния Хэмминга до образа "*а*"									
	1	2	3	4	5	6	7	8	9	10
"*п*"	103	31	33	65	133	148	47	111	53	114
"*пг*"	163	135	163	167	141	148	162	152	149	123
"*пгу*"	156	82	71	109	93	91	106	101	108	98

14. Вычислить для данных таблицы 3 математическое ожидание E(h) = 112 и стандартное отклонение σ(h) = 39.4. Вычислите вероятность появления нулевых расстояний Хэмминга по формуле (1):

$$P_{2,"."} \approx \frac{1}{\sigma(h)\sqrt{2\pi}} \int_{-\infty}^{0} \exp\left\{\frac{-(112-u)^2}{2\cdot(39.4)^2}\right\} du = 0.0023$$

15. Вычислить стойкость к атакам подбора:

$$(P_2)^{-1} \approx \frac{1}{0.0023} = 435 \quad попыток$$

ВЫВОД: Если злоумышленник не знает длину рукописного пароля, то для успешной атаки подбора простейшего рукописного пароля из одной буквы ему потребуется осуществить порядка 435 попыток. Время на одну попытку ввода рукописных биометрических данных составляет примерно 10 секунд. Стойкость защиты составляет 4350 секунд или 72 минуты.

Указания по выполнению заданий:

1. На компьютере должна быть установлена программа «БиоНейроАвтограф».
2. Ответить на вопросы при защите работы

Материально-техническое обеспечение занятия:

1. Компьютеры по количеству обучающихся с развёрнутой ОС MS Windows, программным пакетом MS Office v.2010 и программой «БиоНейроАвтограф».

Список литературы:

1. *Брюхомицкий, Ю.А.* Биометрические технологии идентификации личности : учебное пособие / Ю. А. Брюхомицкий ; Южный федеральный университет. – Ростов-на-Дону ; Таганрог : Издательство Южного федерального университета, 2017. – 263 с. – ISBN 978-5-9275-2454-9. – Текст : электронный. – URL: https://znanium.com/catalog/product/1021574 (дата обращения: 10.05.2021). – Режим доступа: по подписке.
2. Среда моделирования «Бионейронавтограф» [Электронный ресурс]. – Режим доступа свобод.: http://пниэи.рф/activity/science/noc.htm.
3. Материалы лекций

Практическая работа № 3 (4 ч.). Оценка вероятности ошибок первого рода – проверка сформированности компетенций – ОПК-4.1, ПК-3, ПК-9

Цели работы:

– оценить вероятности ошибок второго рода (пропуск «Чужого») по ГОСТ Р 52633.3-2011 используя статистики расстояний Хэмминга.

– закрепление навыков работы с программой «БиоНейроАвтограф».

Задания:

1. Запустить файл «бионейроавтограф.exe».
2. Задать 32-х символьный простой пароль и рукописный образ.
3. Обучить систему.
4. Для проверки качества обучения ввести контрольный рукописный образ и нажать кнопку «Проверить». Далее ввести рукописный символ. Если средство аутентификации Вас узнает, то появится сообщение «Введён верный пароль!».
5. Провести тестирование способности узнавать "Своего", введя тот же самый рукописный символ 50 раз. При этом в большинстве случаев должен получаться верный код, а в редких случаях получается неверный выходной код доступа. Ввести данные в табл. 1, например:

Таблица №1

Попытка / Образ	Расстояния Хэмминга до образа "*a*"									
	1	2	3	4	5	6	7	8	9	10
"*a*"	0	0	0	0	0	0	0	0	0	0
"*a*"	0	0	0	0	0	0	0	0	**1**	0
"*a*"	0	0	0	**3**	0	0	0	0	0	0
"*a*"	0	0	0	0	0	0	0	0	0	0
"*a*"	0	0	0	0	0	0	0	0	0	0

6. Вычислить вероятность ошибок первого рода по обычной формуле для 10, 20, 30, 40 и 50 опытов:

$$P1 = \frac{0}{10} = 0;\ P1 = \frac{1}{20} = 0.05;\ P1 = \frac{2}{30} = 0.067;\ P1 = \frac{2}{40} = 0.05;\ P1 = \frac{2}{50} = 0.04.$$

7. Вычислить математическое ожидание расстояний Хэмминга для 10, 20, 30, 40 и 50 опытов E(h)=0.0; E(h)=0.05; E(h)=0.134; E(h)=0.1; E(h)=0.08.

Далее вычислить определённый интеграл распределения хи-квадрат расстояний Хэмминга с числом степеней свободы m= E(h)=0.0; 0.05; 0.134; 0.1; 0.08 в интервале от 1 до ∞ :

$$P_1 = \int_1^{\infty} p\left(\chi^2(h, m = 0.08)\right)dh = 0.023$$

для данных, приведённых выше получим:

P1=0.026; P1=0.014; P1=0.038; P1=0.029; P1=0.023.

8. Убедиться, что вычисления вероятности по обычной формуле (п.6) даёт более нестабильные результаты (большой разброс результатов) в сравнении более стабильным результатом оценок ошибок первого рода с учётом выявленных значений расстояний Хэмминга (меньший разброс результатов).
9. Проверить, какая из оценок точнее. Для этой цели продолжить испытания, повторив ещё 50 раз написание выбранного символа. Данные свести в таблицу 2, например:

Таблица № 2

Попытка / Образ	Расстояния Хэмминга до образа "*a*"									
	1	2	3	4	5	6	7	8	9	10
"*a*"	0	0	0	0	0	0	0	0	0	0
"*a*"	0	0	0	0	0	0	0	0	0	0
"*a*"	0	0	0	0	0	0	0	0	0	0
"*a*"	0	0	0	0	0	0	0	0	0	0
"*a*"	**2**	0	0	0	0	0	0	0	0	0

10. Вычислить вероятность ошибок для всех 100 опытов (учитываются результаты таблицы 1 и таблицы 2), например:

P1 = 3/100 = 0,03

11. Сравнить полученное значение вероятности ошибок первого рода с данными, вычисленными ранее на малом числе примеров. Принять решение, какой метод вычисления ошибок вероятностей первого рода точнее на малых тестовых выборках.
12. Переобучите средство аутентификации на двух, вводимых подряд, рукописных символах, например "aa". Вводить данные следует не менее 8 раз.
13. Проверить, как Вас узнает средство аутентификации, введя 20 раз рукописный образ из двух символов. Ввести данные в таблицу 3.

Таблица №3.

Попытка / Образ	Расстояния Хэмминга до образа "*aa*"									
	1	2	3	4	5	6	7	8	9	10
"*aa*"	1	7	0	0	3	0	0	2	0	10
"*aa*"	0	2	0	3	0	0	6	0	4	0

14. Вычислить вероятности ошибок первого рода по обычной формуле.

P1 = 9/20 = 0,45

15. Вычислите математическое ожидание расстояний Хэмминга E(h)=1.9 и по нему вычислите вероятность ошибок первого рода, пользуясь хи-квадрат распределением с 1.9 степенями свободы.
16. В связи с высоким уровнем вероятности ошибок первого рода средство аутентификации необходимо переобучить, дополнительно введя ещё 4 образа "аа". Повторить тестирование на 20 тестовых образах, данные сведите в таблицу 4.

Таблица №4.

Попытка / Образ	Расстояния Хэмминга до образа *"аа"*									
	1	2	3	4	5	6	7	8	9	10
"аа"	0	0	0	**1**	0	0	0	0	0	0
"аа"	0	0	0	0	0	**5**	0	0	0	0

17. Вычислить вероятность появления ошибки первого рода классическим методом:

$$P1 = 2/20 = 0{,}1$$

18. Вычислить вероятность появления ошибок первого рода с учётом значений расстояний Хэмминга E(h) = 6/20 = = 0.3 P1=0.09.
19. Сделать вывод, например, для рассматриваемого примера:

ВЫВОД:

1. Учёт дополнительной информации в виде математического ожидания расстояний Хэмминга при малом числе опытов позволяет получить более достоверные результаты при оценке вероятностей появления ошибок первого рода. Повышение достоверности оценки является следствием учёта большего объёма исходной информации.

2. Сложные биометрические образы (состоящие из большего числа рукописных символов) обладают большей нестабильностью по сравнению с простыми биометрическими образами. Нестабильность биометрического образа может быть скомпенсирована за счёт увеличения тестовых примеров в обучающей выборке.

Указания по выполнению заданий:

1. На компьютере должна быть установлена программа «БиоНейроАвтограф».
2. Ответить на вопросы при защите работы

Материально-техническое обеспечение занятия:

1. Компьютеры по количеству обучающихся с развёрнутой ОС MS Windows, программным пакетом MS Office v.2010 и программой «БиоНейроАвтограф».

Список литературы:

1. *Брюхомицкий, Ю.А.* Биометрические технологии идентификации личности : учебное пособие / Ю. А. Брюхомицкий ; Южный федеральный университет. – Ростов-на-Дону ; Таганрог : Издательство Южного федерального университета, 2017. – 263 с. – ISBN 978-5-9275-2454-9. – Текст : электронный. – URL: https://znanium.com/catalog/product/1021574 (дата обращения: 10.05.2021). – Режим доступа: по подписке.
2. Среда моделирования «Бионейронавтограф» [Электронный ресурс]. – Режим доступа свобод.: http://пниэи.рф/activity/science/noc.htm.
3. Материалы лекций

Практическая работа № 4 (4 ч.). Коррекция ошибок выходных кодов нейронной сети за счёт введения в эти коды избыточности – ОПК-4.1, ПК-3, ПК-9

Цели работы:

– оценить возможность коррекции ошибок выходных кодов сети за счёт введения в коды избыточности.

– закрепление навыков работы с программой «БиоНейроАвтограф».

Задания:

1. Запустить файл «бионейроавтограф.exe».
2. Задать 32-х символьный простой пароль и рукописный образ.
3. Обучить систему.
4. Для проверки качества обучения ввести контрольный рукописный образ и нажать кнопку

«Проверить». Далее ввести рукописный символ. Если средство аутентификации Вас узнает, то появится сообщение «Введён верный пароль!».

5. Воспроизвести нестабильность рукописного почерка, например, путём увеличения длины хвостика рукописной буквы "a" так, чтобы образ приближался к символу "@". При этом нейронная сеть перестаёт узнавать образ. Убедиться в этом, рассматривая данные в двоичной и символьной кодировке.
6. Рассмотреть ситуацию корректировки кода рукописного символа "a" путём выявления наиболее часто встречающегося символа в символьной кодировке. Выписать символы в последовательности по убыванию частоты их появления в последовательности:
   – символ "a" – 17 раз;
   – символ "i" – 4 раза;
   – символ " " – 4 раза;
   – символ "c" – 2 раза;
   – символ "C" – 1 раз;
   – символ "!" – 1 раз;
   – символ "m" – 1 раз.

   Очевидно, что 32-х кратное повторение кодировки символа "a" позволяет корректировать случайные ошибки, возникающие из-за нестабильности рукописного почерка человека.
7. Увеличить длину хвостика буквы "a", так чтобы искажения кода появились во всех двоичных кодировках символов цифровой последовательности. Убедиться, что правильно распознанного символа "a" вообще нет в полученной последовательности.
8. Пользуясь двоичной кодировкой символов, восстановите каждый из разрядов восьмибитного кода, выявляя наиболее часто появляющееся состояние в каждом двоичном разряде. Данные сведите в таблицу 1, например:

   Таблица 1.

N	Отображён	Знак	Кодировка		N	Отображён	Знак	Кодировка
1	*1*0**01	э	11001101		17	0110*0**	j	01101000
2	*110*001	å	11101001		18	*1100011	ǿ	11100011
3	*1100*01	Ì	11100101		19	0110*011	i	01101011
4	*110*0*1	K	11101011		20	0110**11	m	01101111
5	01*0*0*1	“	01001011		21	0110001*	“	01100010
6	0110000*	°	01100000		22	01*000*1	C	01000001
7	01*000*1	C	01000011		23	*1100011	ǔ	11100011
8	01*0*0*1	K	01001011		24	**100011	C	10100011
9	011*000*	p	01110000		25	01000**1	g	01100101
10	*1**0001	ë	11010001		26	*1000**1	Ξ	11100101
11	*1100001	ê	11100001		27	*1000011	ь	11100001
12	*1***0**	±	11011010		28	01100*0*	d	01100100
13	0110***1	o	01101111		29	01*00001	A	01000001
14	*1**0001	ë	11010001		30	*1*0*0*1	ы	11010101
15	01*0*001	I	01001001		31	011000*1	c	01100001
16	01*000*1	C	01000011		32	011000*1	i	01101001

   Кодировка символов в таблице No1 находится путём инвертирования верного кода символа "a" – "0110001" в разрядах помеченных символом "*".
9. Подсчитать число состояний "0" в первом разряде кодировок, а так же число состояний "1". Вывод: верное состояние первого разряда кода "0", т.к. "0" появляется 18 раз, а "1" встречается 14 раз.
10. Подсчитать число состояний "0" во втором разряде кодировок, а так же число состояний "1". Вывод: верное состояние второго разряда кода "1", т.к. "0" – 1 раз, "1" – 31 раз.
11. Аналогично подсчитать число состояний "0" и "1"в третьем ри последующих разрядах кодировок. Сделать соответствующие выводы.
12. Сделать общий вывод, например для рассматриваемого варианта:

ВЫВОД:
32-х кратная избыточность кодировки символа "а" в выходном коде нейронной сети позволяет корректировать незначительные естественные отклонения динамики рукописного почерка человека и верно распознавать, воспроизводимые его рукой символы.
Указания по выполнению заданий:
1. На компьютере должна быть установлена программа «БиоНейроАвтограф».
2. Ответить на вопросы при защите работы
Материально-техническое обеспечение занятия:
1. Компьютеры по количеству обучающихся с развёрнутой ОС MS Windows, программным пакетом MS Office v.2010 и программой «БиоНейроАвтограф».
Список литературы:
1. *Брюхомицкий, Ю.А.* Биометрические технологии идентификации личности : учебное пособие / Ю. А. Брюхомицкий ; Южный федеральный университет. – Ростов-на-Дону ; Таганрог : Издательство Южного федерального университета, 2017. – 263 с. – ISBN 978-5-9275-2454-9. – Текст : электронный. – URL: https://znanium.com/catalog/product/1021574 (дата обращения: 10.05.2021). – Режим доступа: по подписке.
2. Среда моделирования «Бионейронавтограф» [Электронный ресурс]. – Режим доступа свобод.: http://пниэи.рф/activity/science/noc.htm.
3. Материалы лекций

Практическая работа № 5 (6 ч.). Работа с USB-сканером отпечатков пальцев – ОПК-4.1, ПК-3, ПК-9

Цели работы:
– получение навыков работы с устройствами сканирования отпечатков пальцев.
Задания:
1. Запустить виртуальную машину с установленной операционной системой Windows 8 и Windows 10.
2. Вставить в USB-разъём сканер отпечатков пальцев типа Espada E-FR10W-2G.
3. Настроить программу Windows Hello и ввести изображения папиллярных узоров своих и двух-трёх сокурсников.
4. Разграничить доступ к разным файлам и папкам.
Указания по выполнению заданий:
1. На компьютере должна быть установлена программа «БиоНейроАвтограф».
2. Ответить на вопросы при защите работы
Материально-техническое обеспечение занятия:
1. Компьютеры по количеству обучающихся с развёрнутой ОС MS Windows, программным пакетом MS Office v.2010 и программой «БиоНейроАвтограф».
Список литературы:
1. *Брюхомицкий, Ю.А.* Биометрические технологии идентификации личности : учебное пособие / Ю. А. Брюхомицкий ; Южный федеральный университет. – Ростов-на-Дону ; Таганрог : Издательство Южного федерального университета, 2017. – 263 с. – ISBN 978-5-9275-2454-9. – Текст : электронный. – URL: https://znanium.com/catalog/product/1021574 (дата обращения: 10.05.2021). – Режим доступа: по подписке.
2. Материалы лекций

По результатам практических занятий обучающиеся составляют отчёты. Отчёт составляется в электронной форме с использованием ПКП MS Office и выше и передаётся преподавателю посредством оговорённой формы связи.

Приложение 1

АННОТАЦИЯ ДИСЦИПЛИНЫ

Дисциплина «Биометрические системы аутентификации» реализуется на факультете Информационных систем и безопасности для студентов 3-го курса, обучающихся по программе бакалавриата по направлению подготовки 10.03.01 Информационная безопасность (профиль подготовки – Безопасность автоматизированных систем) кафедрой комплексной защиты информации.

Цель дисциплины: профессиональная подготовка студентов, необходимая для освоения методов и технологий, связанных с обеспечением безопасности объекта охраны от физического доступа посторонних лиц.
Задачи:

- получение систематизированных знаний о современных концепциях, методах и технологиях обеспечения безопасности объекта охраны от физического доступа посторонних лиц;
- изучение теоретических основ обеспечения безопасности объекта охраны от физического доступа посторонних лиц;
- формирование умений использовать современные достижения в области обеспечения безопасности объекта охраны от физического доступа посторонних лиц при реализации своей профессиональной деятельности;
- владение практическими навыками, применения современных методами, сил и средств в обеспечении безопасности объекта охраны от физического доступа посторонних лиц;
- развитие аналитического мышления, умения строго излагать свои мысли, развитие способностей к обобщению и анализу информации, постановке целей и выбору путей ее достижения.

Дисциплина направлена на формирование следующих компетенций:
ПК-3 - Способен управлять защитой информации в автоматизированных системах
В результате освоения дисциплины (модуля) обучающийся должен:

- Знает основные методы управления защитой информации, информационные ресурсы автоматизированных систем, подлежащие защите; основные угрозы безопасности информации, модели нарушителя в автоматизированных системах
- Умеет разрабатывать предложения по совершенствованию системы управления защиты информации автоматизированных систем; классифицировать и оценивать угрозы безопасности информации; оценивать информационные риски в автоматизированных системах
- Владеет навыками составления комплекса правил, процедур, практических приёмов, принципов и методов, средств обеспечения защиты информации в автоматизированной системе

ОПК-4.1 - Способен проводить организационные мероприятия по обеспечению безопасности информации в автоматизированных системах
В результате освоения дисциплины (модуля) обучающийся должен:

- Знает нормативные, руководящие и методические документы уполномоченных федеральных органов исполнительной власти по защите информации
- Умеет разрабатывать документы в области обеспечения безопасности информации в автоматизированной системе при ее эксплуатации (включая управление инцидентами информационной безопасности)
- Владеет навыками планирования мероприятий по обеспечению защиты информации и организацию работы персонала автоматизированной системы с учётом требований по защите информации

ПК-9 - Способен осуществлять подбор, изучение и обобщение научно-технической литературы, нормативных и методических материалов, составлять обзор по вопросам обеспечения информационной безопасности по профилю своей профессиональной деятельности

В результате освоения дисциплины (модуля) обучающийся должен:

- Знает нормативные правовые акты в области защиты информации, национальные, межгосударственные и международные стандарты в области защиты информации, руководящие и методические документы уполномоченных федеральных органов исполнительной власти по защите информации
- Владеет организационными мерами по защите информации
- Умеет работать с программным обеспечением с соблюдением действующих требований по защите информации

По дисциплине предусмотрена промежуточная аттестация в форме зачёта.

Общая трудоёмкость освоения дисциплины составляет 2 зачётные единицы.