МИНОБРНАУКИ РОССИИ

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ «ТУЛЬСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»

Утверждено решением Ученого совета Тульского государственного университета
от «25» марта 2021 г.,
протокол № 10;

Ректор _____ М.В. Грязев
Подпись

М.П.

ПРОГРАММА ПОВЫШЕНИЯ КВАЛИФИКАЦИИ

Технологии защиты конфиденциальной информации

Срок освоения программы – 72 часа

Тула 2021 год

1 Цель и задачи программы повышения квалификации

Целью программы повышения квалификации является формирование новых компетенций обучающегося, необходимых для ведения процессов построения систем защиты конфиденциальной информации, обрабатываемой в автоматизированных системах.

Настоящая программа курсов повышения квалификации предусматривает четыре модуля дисциплин, задачами изучения которых являются:

1. Формирование базовых теоретических знаний и профессиональных навыков в области основ проектирования и эксплуатации баз данных и информационных автоматизированных систем в различных сферах общественной жизни. Модуль «Автоматизированные системы обработки конфиденциальной информации».

2. Получение теоретических знаний и профессиональных навыков в области применения Федеральных законов, постановлений правительства РФ и органов исполнительной власти РФ, ГОСТов, а также базовых методик и алгоритмов управления информационной безопасностью. Модуль «Нормативно-правовые документы РФ в сфере кибербезопасности».

3. Получение теоретических знаний и профессиональных навыков и умений в области разработки и практической реализации технологий ведения защиты конфиденциальной информации, обрабатываемой в автоматизированных системах. Модуль «Технологии защиты конфиденциальной информации».

4. Получение теоретических знаний и профессиональных навыков в области выбора, внедрения и эксплуатации программного обеспечения для анализа и моделирования систем защиты конфиденциальной информации, включая программные инструменты защиты данных в системах управления базами данных и анализаторы кода и целостности входных информационных массив. Модуль «Программные средства в области защиты конфиденциальной информации».

2 Планируемые результаты обучения

Перечень компетенций обучающегося, планируемых к формированию в результате освоения настоящей программы повышения квалификации:

- владение знаниями и навыками в области создания автоматизированных систем, обрабатывающих конфиденциальную информацию, их эксплуатации и анализа их защищенности (ПК-1);
- владение знаниями и навыками в области работы с нормативно-правовыми документами РФ в сфере защиты информации и создании автоматизированных информационных систем в защищенном исполнении (ПК-2);
- владение знаниями, навыками и умениями в области проектирования систем защиты конфиденциальной информации и автоматизированных информационных систем на основе актуальных уязвимостей, угроз и категорий нарушителей, в области разработки технологий и методов прогрессивной защиты конфиденциальной информации (ПК-3);
- владение знаниями и навыками в области применения сертифицированных программных средств для анализа действующих систем защиты и моделирования эффективных систем защиты информации и автоматизированных информационных систем (ПК-4).

В результате освоения программы повышения квалификации обучающийся должен:

знать:

- принципы создания автоматизированных систем, обрабатывающих конфиденциальную информацию, правила их эксплуатации и методики анализа их защищенности;
- нормативно-правовые документы РФ в сфере защиты информации и в области создания автоматизированных информационных систем в защищенном исполнении;
- принципы, подходы, методики и этапы проектирования систем защиты конфиденциальной информации и автоматизированных информационных систем на основе актуальных уязвимостей, угроз и категорий нарушителей, технологии и методы прогрессивной защиты конфиденциальной информации;
- перечень и принципы работы сертифицированных программных средств для анализа действующих систем защиты и моделирования эффективных систем защиты информации и автоматизированных информационных систем.

уметь:

- применить на практике знания по созданию автоматизированных систем, обрабатывающих конфиденциальную информацию, правила их эксплуатации и методики анализа их защищенности;
- использовать в профессиональной деятельности нормативно-правовые документы РФ в сфере защиты информации и в области создания автоматизированных информационных систем в защищенном исполнении;
- применить на практике принципы, подходы, методики и этапы проектирования систем защиты конфиденциальной информации и автоматизированных информационных систем на основе актуальных уязвимостей, угроз и категорий нарушителей, технологии и методы прогрессивной защиты конфиденциальной информации;
- воспользоваться знаниями принципов работы сертифицированных программных средств для анализа действующих систем защиты и моделирования эффективных систем защиты информации и автоматизированных информационных систем.

владеть:

- принципами создания автоматизированных систем, обрабатывающих конфиденциальную информацию, правила их эксплуатации и методики анализа их защищенности;
- нормативно-правовой базой документов РФ в сфере защиты информации и в области создания автоматизированных информационных систем в защищенном исполнении;
- принципами, подходами, методиками и этапами проектирования систем защиты конфиденциальной информации и автоматизированных информационных систем на основе актуальных уязвимостей, угроз и категорий нарушителей, технологии и методы прогрессивной защиты конфиденциальной информации;

- принципами работы сертифицированных программных средств для анализа действующих систем защиты и моделирования эффективных систем защиты информации и автоматизированных информационных систем.

Целевой аудиторией слушателей настоящей программы курсов повышения квалификации являются граждане Российской Федерации, желающие получить профессиональные знания и практические навыки в сфере ведения работ по автоматизации деловых процессов, а также по техникам обеспечения защиты конфиденциальной информации, обрабатываемой в автоматизированных системах, с учетом требований документов РФ в области обеспечения кибербезопасности.

3 Учебный план

Срок освоения программы: 72 часа.

Форма обучения: очная.

Порядок обучения: единовременно и непрерывно.

Программа повышение квалификации может быть реализована с применением дистанционных образовательных технологий.

№ п/п	Наименование модуля	Всего часов	В том числе					Форма контроля
			Виды учебных занятий и учебных работ				Самостоятельная работа	
			Лекции	Практические (семинарские) занятия	Лабораторные работы	Иные виды учебных занятий и учебных работ*		
1	Модуль «Автоматизированные системы обработки конфиденциальной информации»	16	4	-	-	4	8	Промежуточная аттестация (зачет)
2	Модуль «Нормативно-правовые документы РФ в сфере кибербезопасности»	18	4	2	-	4	8	Промежуточная аттестация (зачет)
3	Модуль «Технологии защиты конфиденциальной информации»	18	4	2	-	4	8	Промежуточная аттестация (зачет)
4	Модуль «Программные средства в области защиты конфиденциальной информации»	18	4	2	-	4	8	Промежуточная аттестация (зачет)
Итоговая аттестация		*2*						
Итого:		*72*						

** Под иными видами учебных занятий и учебных работ здесь и далее понимаются: круглые столы, мастер-классы, мастерские, деловые игры, ролевые игры, тренинги, семинары по обмену опытом, выездные занятия, консультации и др.*

4 Календарный учебный график

Реализация модулей программы курсов повышения квалификации осуществляется параллельно в соответствии с календарным учебным графиком:

Наименование модуля	1 неделя	2 неделя	Итого:
Модуль «Автоматизированные системы обработки конфиденциальной информации»	8	8	16
Модуль «Нормативно-правовые документы РФ в сфере кибербезопасности»	9	9	18
Модуль «Технологии защиты конфиденциальной информации»	9	9	18
Модуль «Программные средства в области защиты конфиденциальной информации»	9	9	18
Итоговая аттестация (экзамен)	-	2	2
Итого:	35	37	72

5 Рабочие программы дисциплин (модулей)

Рабочая программа модуля «Автоматизированные системы обработки конфиденциальной информации»

№ п/п	Наименование тем модуля	Всего часов	В том числе				
			Виды учебных занятий и учебных работ				Самостоятельная работа
			Лекции	Практические (семинарские) занятия	Лабораторные работы	Иные виды учебных занятий и учебных работ*	
1	Виды информации. Закрытая, открытая и конфиденциальная информация	4	1	-	-	1	2
2	Виды закрытой и конфиденциальной информации	2	0,5	-	-	0,5	1
3	Современные способы автоматизации деловых процессов	2	0,5	-	-	0,5	1
4	Угрозы, уязвимости, атаки, категории и модели нарушителей режима конфиденциальности	2	0,5	-	-	0,5	1
5	Понятие автоматизированной системы и автоматизированной системы в защищенном исполнении	2	0,5	-	-	0,5	1
6	Актуальные подходы к созданию автоматизированных систем	2	0,5	-	-	0,5	1
7	Способы защиты автоматизированных систем. Программная, техническая и организационно-методическая защита	2	0,5	-	-	0,5	1
	Итого	16	4	-	-	4	8

Рабочая программа модуля «Нормативно-правовые документы РФ в сфере кибербезопасности»

№ п/п	Наименование тем модуля	Всего часов	В том числе				
			Виды учебных занятий и учебных работ				Самостоятельная работа
			Лекции	Практические (семинарские) занятия	Лабораторные работы	Иные виды учебных занятий и учебных работ	
1	Обзор Федеральных законов в области обеспечения информационной безопасности. ФЗ №152 «О персональных данных»	3	1	-	-	1	1
2	Постановления правительства РФ в области защиты данных и информации	3	1	-	-	1	1
3	Документы органов исполнительной власти (ФСБ, ФСТЭК) в области обеспечения кибербезопасности	2	0,5	-	-	0,5	1
4	Международные стандарты в сфере защиты информации	2	0,5	-	-	0,5	1
5	Отечественные стандарты в области защиты информации	4	0,5	1	-	0,5	2
6	Политики безопасности, распорядительные документы и подтверждающие акты предприятий	4	0,5	1	-	0,5	2
	Итого:	18	4	2	-	4	8

Рабочая программа модуля «Технологии защиты конфиденциальной информации»

№ п/п	Наименование тем модуля	Всего часов	В том числе				
			Виды учебных занятий и учебных работ				Самостоятельная работа
			Лекции	Практические (семинарские) занятия	Лабораторные работы	Иные виды учебных занятий и учебных работ	
1	Анализ объекта информатизации и архитектуры автоматизированной системы. Входной уровень защищенности	3	1	-	-	1	1
2	Выбор актуальных угроз. Банк угроз ФСТЭК. Экспертная оценка	3	1	-	-	1	1
3	Анализ категорий нарушителей для объекта информатизации	2	0,5	-	-	0,5	1
4	Анализ уязвимостей в действующей системе защиты. Барьеры защищенности. Усиление барьеров защищенности	2	0,5	-	-	0,5	1
5	Классы и уровни защищенности ав-	4	0,5	1	-	0,5	2

	томатизированных систем. Установление класса и уровня защищенности						
6	Средства защиты объекта информатизации и автоматизированных информационных систем. Программная, техническая (программно-аппаратная), организационно-методическая составляющая средств защиты	4	0,5	1	-	0,5	2
	Итого:	18	4	2	-	4	8

Рабочая программа модуля
«Программные средства в области защиты конфиденциальной информации»

№ п/п	Наименование тем модуля	Всего часов	В том числе				
			Виды учебных занятий и учебных работ				Самостоятельная работа
			Лекции	Практические (семинарские) занятия	Лабораторные работы	Иные виды учебных занятий и учебных работ	
1	Программные средства для анализа действующей системы защиты автоматизированных систем. Программная оценка криптографической стойкости.	3	1	-	-	1	1
2	Программные средства для моделирования более эффективной и модернизации действующей системы защиты автоматизированных систем	3	1	-	-	1	1
3	Средства журналирования работы с автоматизированными системами	2	0,5	-	-	0,5	1
4	Системы мониторинга утечки конфиденциальной информации и мониторинга функционирования механизмов контроля	2	0,5	-	-	0,5	1
5	Системы распределения ролей	4	0,5	1	-	0,5	2
6	Системы управления рисками в сфере информационной безопасности	4	0,5	1	-	0,5	2
	Итого:	18	4	2	-	4	8

6 Организационно-педагогические условия реализации программы повышения квалификации

6.1 Требования к материально-техническому обеспечению

Для проведения лекционных занятий требуется аудитория, оборудованная настенным экраном, проектором, ноутбуком и аудиосистемой.

Для проведения практических (семинарских) и лабораторных занятий требуется компьютерный класс, в котором компьютеры оснащены операционной системой Windows, Linux, стандартными офисными пакетами Мой офис, Microsoft Office, Open Office, Libre Office.

Для проведения итоговой аттестации требуется компьютерный класс с программным обеспечением и средствами проведения тестирования, в том числе on-line тестирования.

6.2 Перечень учебно-методического и информационного обеспечения

1. Федеральный закон «О персональных данных» от 27.07.2006 N 152-ФЗ
2. Постановление Правительства РФ от 01.11.2012 N 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»
3. Приказ ФСТЭК России от 18.02.2013 N 21 (ред. от 23.03.2017) «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных».
4. Гостехкомиссия России – Руководящий документ. Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации – Москва, 1992.
5. Гостехкомиссия России – Руководящий документ. Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от НСД к информации – Москва, 1992.
6. ГОСТ Р 53114-2008 Защита информации. Обеспечение информационной безопасности в организации. Основные термины и определения.
7. Бабаш А. В. Криптографические методы защиты информ.: Уч.пос.: Т.1/А.В.Бабаш-2изд.-ИЦ РИОР, НИЦ ИНФРА-М,2016-413с(/ А.В. Бабаш. - Москва: Мир, 2016. - 597 с.
8. Баранова Е. К. Информационная безопасность и защита. Учебное пособие / Е.К. Баранова, А.В. Бабаш. - М.: РИОР, Инфра-М, 2016. - 324 с.
9. Борисов М. А. Основы организационно-правовой защиты информации / М.А. Борисов, О.А. Романов. - М.: Ленанд, 2014. - 248 с.
10. Гвоздева В. А. Основы построения автоматизированных информационных систем / В.А. Гвоздева, И.Ю. Лаврентьева. - М.: Форум, Инфра-М, 2016. - 320 с.
11. Зегжда Д.П. Основы безопасности информационных систем / Д.П. Зегжда, А.М. Ивашко. - М.: Горячая линия - Телеком, 2013. - 452 с.
12. Петраков А. В. Основы практической защиты информации / А.В. Петраков. - М.: РадиоСофт, 2015. - 504 с.

6.3 Требования к кадровому обеспечению

Реализация программы повышения квалификации осуществляется профессорско-преподавательским составом института Прикладной математики и компьютерных наук Тульского государственного университета.

7 Формы аттестаций и оценочные материалы

Промежуточная аттестация обучающегося по каждому модулю осуществляется в виде зачета в форме тестирования (on-line тестирования). В ходе зачета обучающемуся предлагается ответить на ряд вопросов по тематике текущего модуля. Обучающийся, давший удовлетворительные ответы более, чем на 50% вопросов, получает оценку «Зачтено».

Итоговая аттестация обучающегося по программе повышения квалификации осуществляется в виде экзамена в форме тестирования (on-line тестирования). К итоговой аттестации допускается обучающийся, не имеющий задолженности и в полном объеме выполнивший учебный план настоящей программы.

Итоговая аттестация считается успешно пройденной в случае получения обучающимся на экзамене одной из следующих оценок: «Отлично», «Хорошо», «Удовлетворительно». Оценка формируется в зависимости от количества набранных обучающимся правильных ответов:

- от 40 до 60% правильных ответов – оценка «Удовлетворительно»;
- от 61 до 80% правильных ответов – оценка «Хорошо»;
- от 81 до 100% правильных ответов – оценка «Отлично». Если обучающийся набрал от 0 до 39% правильных ответов (оценка «Неудовлетворительно»), ему предлагается пройти повторной тестирование после соответствующей подготовки.

В случае успешного прохождения итоговой аттестации обучающемуся выдается документ о квалификации установленного образца – удостоверение о повышении квалификации.

В приложении к программе повышения квалификации приводятся оценочные материалы для проведения промежуточных и итоговой аттестаций обучающегося.

8 Методические материалы по проведению итоговой аттестации

При планировании процедуры итоговой аттестации обучающихся целесообразно использовать соответствующие методические рекомендации Минобрнауки России (Письмо Минобрнауки России от 30 марта 2015 г. «О направлении методических рекомендаций по итоговой аттестации слушателей»).

9 Лист согласования программы повышения квалификации

Разработчики программы повышения квалификации:

Баранов Андрей Николаевич, к.т.н., доц. _____
Фамилия, имя, отчество, ученая степень, ученое звание, должность разработчика — Подпись

Баранова Елизавета Михайловна, к.т.н., доц. _____
Фамилия, имя, отчество, ученая степень, ученое звание, должность разработчика — Подпись

Сычугов Алексей Алексеевич, к.т.н., доц. _____
Фамилия, имя, отчество, ученая степень, ученое звание, должность разработчика — Подпись

Программа согласована с дирекцией Института прикладной математики и компьютерных наук

Директор ИПМКН _____ А.А. Сычугов
Аббревиатура наименования института — Подпись

Согласовано с УМУ:

Специалист по УМР УМУ _____ С.В. Моржова
Подпись

Начальник УМУ _____ А.В. Моржов
Подпись

Программа планируется к реализации Институтом прикладной математики и компьютерных наук
Наименование реализующего подразделения

Согласовано:

Директор ИПМКН _____ А.А. Сычугов
Должность руководителя реализующего подразделения — Подпись

«22» 03 2021 г.

ПРИЛОЖЕНИЕ

Оценочные материалы для проведения промежуточной аттестации по модулю «Автоматизированные системы обработки конфиденциальной информации»

1. Языком создания запросов для систем управления базами данных является:
а) HTML
б) Pascal
в) Java
г) SQL
д) C ++

2. Структура таблицы реляционной базы данных (БД) изменится, если…
а) добавить или удалить поле
б) удалить все записи
в) добавить одну или нескольких записей
г) изменить имя записи

3. Какие свойства информации натолкнули разработчиков на внедрение баз данных в информационные системы?
а) старение
б) кумулятивность
в) повторяемость и многократность использования
г) рост объема информации

4. Соотнесите понятия со связью типа один ко многим в реляционных базах данных:
а) односторонняя (читается только в одном направлении)
б) раскладывается на две связи типа один к одному
в) двусторонняя (читается в двух направлениях – слева направо и справа налево)
г) записи таблиц, объединенные этой связью, могут быть объединены в одну таблицу
д) записи таблиц, объединенные этой связью, НЕ могут быть объединены в одну таблицу

5. Как называется технология обработки данных, при которой сервер обрабатывает часть пользовательских команд:
а) клиент-серверная
б) распределенная
в) файл-серверная
г) иерархическая
д) однораноговая

6. Сервер, который выполняет часть абонентских запросов это:
а) глобальный сервер
б) архивационный сервер
в) сервер печати
г) сервер приложений

7. Укажите свойства реляционной связи баз данных типа многие ко многим:
а) двусторонняя (читается справа налево и с лева направо)
б) может быть разделена на две связи типа один ко многим
в) может быть разделена на две связи типа один к одному
г) состоит из трех таблиц

д) всегда строится только при помощи вторичных ключей

8. Укажите управляемые уровни защиты информации, хранящейся в базах данных (на компьютерах):
а) организационный
б) программный
в) правовой
г) технический
д) аппаратный

9. Если злоумышленник уничтожил логические связи между сущностями в базе данных, то он нарушил
а) конфиденциальность информации
б) кумулятивность информации
в) семантику информации
г) целостность информации
д) методы доступа к информации

10. Система защиты информации должна быть рассмотрена как состоящая из следующих подсистем:
а) подсистемы управления доступом
б) подсистемы, анализирующей угрозы и уязвимости
в) подсистемы регистрации и учета
г) криптографической подсистемы
д) подсистемы обеспечения целостности

Оценочные материалы для проведения промежуточной аттестации по модулю «Нормативно-правовые документы РФ в сфере кибербезопасности»

1. Обработка биометрических данных регламентируется Федеральным законом:
а) 251-ФЗ;
б) 215-ФЗ;
в) 52-ФЗ;
г) 152-ФЗ;
д) 125-ФЗ.

2. В качестве оператора по обработке биометрических данных может выступать (на основе действующего законодательства):
а) государственный орган;
б) муниципальный орган;
в) образовательное учреждение;
г) юридическое лицо;
д) физическое лицо.

3. Коэффициент FAR – это:
а) коэффициент ложного отказа в пропуске систем СКУД;
б) коэффициент ложного пропуска систем СКУД;
в) усредненный коэффициент сбоев формирования биометрического шаблона;
г) коэффициент похищений биометрических шаблонов;
д) коэффициент атак на сервер, хранящих биометрические шаблоны.

4. Система СКУД – это:
а) Система контроля удаленного доступа;

б) Система качественного управления документооборотом;
в) Система квалифицированного управления делопроизводством;
г) Система контроля и управления доступом;
д) Система контроля и управления данными.

5. Какие два класса биометрических технологий существуют:
а) одномерные и многомерные;
б) основанные на плоской и трехмерной идентификации;
в) аутентифицирующие и идентифицирующие;
г) телевизионные и радиочастотные;
д) статические и динамические?

6. Укажите технологии биометрической идентификации:
а) дактилоскопия;
б) идентификация на основе рисунка вен;
в) идентификация на основе костей позвоночника;
г) идентификация на основе геометрии ладони;
д) идентификация на основе сетчатки глаза.

7. Каким коэффициентом может быть оценена биометрическая система идентификации:
а) коэффициент выхода из строя серверов;
б) коэффициент человеко-потока;
в) коэффициент безуспешных попыток создать шаблон из входных данных (при низком качестве последних);
г) коэффициент регулярного изменения алгоритма биометрической идентификации;
д) коэффициент, показывающий то, что автоматизированная система не способна определить биометрические входные данные, когда они представлены корректно?

8. Для какой технологии биометрической идентификации фальсификация данных безуспешна:
а) распознавание лица 3D;
б) распознавание радужной оболочки глаза;
в) распознавание геометрии ладони;
г) распознавание рисунка вен;
д) распознавание сетчатки глаза?

9. Как называются действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность персональных данных конкретному субъекту персональных данных:
а) обезвреживание ПД;
б) отвержение ПД;
в) обезличивание ПД
г) олицетворение ПД;
д) обесценивание ПД?

10. Укажите технологии, наиболее чувствительные к внешним факторам:
а) распознавание лица 3D;
б) распознавание радужной оболочки глаза;
в) распознавание лица 2D;
г) дактилоскопия;
д) распознавание сетчатки глаза.

Оценочные материалы для проведения промежуточной аттестации по модулю «Технологии защиты конфиденциальной информации»

1. Биометрическая идентификация может применяться в процессах:

а) идентификации при доступе к локальным рабочим станциям;

б) идентификации при работе систем «умный дом»;

в) идентификации при доступе к объектам общего пользования (повышенной социальной активности);

г) идентификации при доступе к защищаемым объектам;

д) идентификации при доступе к серверам.

2.Форма согласия субъекта на обработку ПД:

а) устанавливается для отрасли;

б) произвольна;

в) регламентирована ФЗ;

г) устанавливается для определенного возрастного класса субъектов;

д) устанавливается в зависимости от целей обработки ПД.

3. Как называется идентификация, осуществляемая на базе нескольких биометрических параметров:

а) многомерная;

б) многопользовательская;

в) многомодульная;

г) многофакторная;

д) мульти-идентификация?

4. Для какой технологии биометрической идентификации фальсификация данных проблематична:

а) распознавание лица 3D;

б) распознавание радужной оболочки глаза;

в) распознавание геометрии ладони;

г) распознавание рисунка вен;

д) распознавание сетчатки глаза?

5. Строгая идентификация – это:

а) использование одного алгоритма для биометрического распознавания;

б) использование одного параметра (например, только голос) для биометрического распознавания;

в) использование одной системы СКУД для биометрического распознавания;

г) использование одного критерия биометрического распознавания;

д) использование одной отличительной особенности для биометрического распознавания.

6. Обработка биометрических персональных данных может осуществляться без согласия субъекта персональных данных в связи:

а) с реализацией международных договоров Российской Федерации о реадмиссии;

б) с осуществлением правосудия и исполнением судебных актов;

в) с проведением обязательной государственной дактилоскопической регистрации;

г) с законодательством Российской Федерации об обороне, о безопасности, о противодействии терроризму, о транспортной безопасности, о противодействии коррупции, об оперативно-розыскной деятельности, о государственной службе,

д) с уголовно-исполнительным законодательством Российской Федерации, законодательством Российской Федерации о порядке выезда из Российской Федерации и въез-

да в Российскую Федерацию, о гражданстве Российской Федерации.

7. Для какой технологии биометрической идентификации фальсификация данных невозможна:

а) распознавание лица 3D;

б) распознавание радужной оболочки глаза;

в) распознавание геометрии ладони;

г) распознавание рисунка вен;

д) распознавание сетчатки глаза?

8. Уполномоченным органом по защите прав субъектов персональных, в том числе биометрических, данных является:

а) федеральный орган законодательной власти;

б) федеральный орган судебной власти;

в) федеральный орган исполнительной власти;

г) муниципалитет;

д) орган, образованный в структуре предприятия, работающего с применением систем биометрической идентификации.

9. Финансирование уполномоченного органа по защите прав субъектов персональных данных осуществляется за счет:

а) средств муниципального бюджета.

б) активов предприятий;

в) средств субъектов обработки ПД;

г) банков;

д) средств Федерального бюджета.

10. Субъект ПД может запросить у оператора следующую информацию относительно ПД:

а) подтверждение факта обработки персональных данных оператором;

б) сроки обработки персональных данных, в том числе сроки их хранения;

в) наименование или фамилию, имя, отчество и адрес лица, осуществляющего обработку персональных данных по поручению оператора, если обработка поручена или будет поручена такому лицу;

г) алгоритмы обработки ПД и авторов разработанных алгоритмов;

д) правовые основания и цели обработки персональных данных.

Оценочные материалы для проведения промежуточной аттестации по модулю «Программные средства в области защиты конфиденциальной информации»

1. Максимальный интервал времени от даты выпуска и/или записи в базу данных самого раннего документа до настоящего времени – это…

а) актуальность базы данных

б) мощность базы данных

в) ценность базы данных

г) глубина ретроспективы базы данных

д) итерация базы данных

2. Относительное число изменяемых описаний объектов к общему числу записей в БД за некоторый интервал времени, определяемый периодичностью издания версий БД

а) детерминированность БД

б) дидактичность БД

в) дедукция БД
г) динамичность БД
д) деструктуризация БД

3. Управление доступом к ресурсам БД обязательно затрагивает:
а) операционную систему
б) сервер баз данных
в) клиентскую часть
г) каналы передачи данных при распределенной обработке информации
д) прикладные программные продукты, установленные на клиенте

4. Сервер – это… (укажите несколько подходящих определений)
а) вспомогательный компьютер в сети, управляющий всеми сетевыми процессами
б) единица коммуникационной сети
в) компьютер, который только хранит базу данных при файл-серверной архитектуре
г) логический процесс, отвечающий за обработку запросов к базам данных
д) единица абонентской подсети

5. Толстый клиент – это…
а) вариант файл-серверной архитектуры, когда вся база данных с сервера транслируется на рабочую станцию
б) вариант клиент-серверной архитектуры, когда клиенту недоступна вся база данных, а доступна лишь некоторая ее часть для модификации
в) вариант файл-серверной архитектуры, когда часть базы данных с сервера транслируется на рабочую станцию
г) локальный подход к эксплуатации базы данных
д) небольшое количество клиентов, обычно до 5, подключенных к серверу с БД

6. Перечислите внутренние по отношению к процессу эксплуатации БД источники угроз:
а) искажение в каналах передачи информации
б) ошибки проектирования БД
в) вирусы
г) ошибки проектирования информационной системы, на основании которой работает БД
д) умышленные деструктивные действия субъектов

7. Угрозы, вызванные воздействием на систему баз данных и ее компоненты объективных физических процессов или стихийно развивающихся природных явлений – это…
а) наиболее вероятностные угрозы
б) неидентифицируемые угрозы
в) искусственные угрозы
г) случайные угрозы
д) естественные угрозы

8. Перечислите угрозы, непосредственным источником которых являются штатные программно-аппаратные средства информационной системы:
а) неквалифицированное использование или ошибочный ввод параметров программ
б) аварийное завершение системных процессов
в) инициализация баз данных
г) отказы и сбои в работе операционной системы, СУБД и прикладных программ
д) форматирование или реструктуризацию носителей информации, удаление данных

9. Укажите угрозы, непосредственным источником которых является среда, в которой эксплуатируется информационная система на основе базы данных

а) деструктивные функции программного обеспечения, функционирующего параллельно с эксплуатируемой информационной системой

б) внезапное и длительное отключение систем электропитания

в) природные катастрофы

г) техногенные катастрофы

д) всплески природных электромагнитных излучений

10. К угрозам нарушения информационной безопасности данных, отображаемой на терминале пользователя или принтере следует отнести:

а) изменение информации в оперативной памяти, используемой СУБД для кэширования данных

б) изменение информации в оперативной памяти, используемой операционной системой для кэширования данных

в) ложная сессия

г) изменение информации в оперативной памяти, используемой прикладными программами в процессе организации и выполнения сессии взаимодействия с сервером баз данных и прослушивающим процессом

д) изменение элементов данных, выводимых на терминал или принтер пользователя за счет перехвата потока

Оценочные материалы для проведения итоговой аттестации

1. Составить схему, демонстрирующую классы защищенности государственных информационных систем, обрабатывающей информацию, не составляющую государственную тайну.

Литература: Приказ ФСТЭК России от 11 февраля 2013 г. N 17

2. Предприятие выделило:

- n уровней угроз;
- m уровней уязвимостей;
- к уровней ценности информационных активов.

Разработать систему оценки вероятности возникновения инцидента в области информационной безопасности.

Использовать количественные и качественные шкалы значений.

Литература: ГОСТ Р ИСО/МЭК 27005-2010

3. Информационная система работает с 2 информационными активами, ценность одного из них очень высокая, другого — очень низкая. Установлено, что каждый из информационных активов имеет 3 незначительных (средних) угрозы, каждая из которых подкреплена очень высокой уязвимостью системы. Пользуясь шкалой, разработанной в задании 2, определить степень вероятности возникновения инцидента для каждого информационного актива и для всей системы в целом.

Литература: ГОСТ Р ИСО/МЭК 27005-2010

4. Обзор (краткий, схематичный) Федерального закона «О безопасности критической информационной инфраструктуры Российской Федерации» от 26.07.2017 № 187-ФЗ

5. Привести примеры несоблюдения законодательства в сфере персональных данных ФЗ №152 «О персональных данных» от 27.07.2006 г.

6. Составить схему, демонстрирующую требования к защите персональных данных при их обработке в информационных системах персональных данных.

Литература: Постановление правительства РФ от 1 ноября 2012 г. N 1119

7. Предприятие выделило:

- n уровней угроз;
- m уровней уязвимостей;
- к уровней ценности информационных активов.

Разработать систему оценки вероятности возникновения инцидента в области информационной безопасности.

Использовать количественные и качественные шкалы значений.

Литература: ГОСТ Р ИСО/МЭК 27005-2010

8. Информационная система работает с 3 информационными активами, ценность одного из них очень высокая, второго — очень низкая, третьего — выше среднего. Установлено, что каждый из информационных активов имеет 2 незначительных (средних) угрозы, каждая из которых подкреплена средней уязвимостью системы. Пользуясь шкалой, разработанной в задании 2, определить степень вероятности возникновения инцидента для каждого информационного актива и для всей системы в целом.

Литература: ГОСТ Р ИСО/МЭК 27005-2010

9. Обзор (краткий, схематичный) Федерального закона «О техническом регулировании» от 27 декабря 2002 г. № 184-ФЗ

10. Привести примеры соблюдения законодательства в сфере персональных данных ФЗ №152 «О персональных данных» от 27.07.2006 г.