Приложение №9.4.39
к ППССЗ по специальности 09.02.03
Программирование в компьютерных системах

ФОНДОЦЕНОЧНЫХ СРЕДСТВ
ПО УЧЕБНОЙ ДИСЦИПЛИНЕ
ОП.11 ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

для специальности

09.02.03 Программирование в компьютерных системах

Уровень подготовки - базовый

Год начала подготовки-2020

2023

СОДЕРЖАНИЕ

1. Паспорт фонда оценочных средств

Фонд оценочных средств (далее - ФОС) по дисциплине ОП.11. Основы информационной безопасности предназначен для контроля и оценки образовательных достижений обучающихся, освоивших программу учебной дисциплины.

ФОС включают контрольные материалы для проведения текущего контроля и промежуточной аттестации в форме экзамена.

ФОСразработаны на основании положений:

- основнойпрофессиональнойобразовательнойпрограммыпоспециальностиСПО 09.02.03Программирование в компьютерных системах
- программы учебной дисциплины ОП.11 Основы информационнойбезопасности

Используемые в ФОС оценочные средства представлены втаблице:

Разделы (темы) дисциплины	Код контролируемой компетенции	Оценочное средство	
		Текущий контроль	Промежуточная аттестация
Раздел 1. Информационная безопасность и уровни ее обеспечения	ПК 1.1-1.4, 2.1-2.4, 3.1. -3.3, 3.6 ОК1-9	Самостоятельные работы по разделу, Практические занятия №1-9 Тест №1,2,3 Устный опрос №1	
Раздел 2. Компьютерные вирусы и защита от них	ПК 1.1-1.4, 2.1-2.4, 3.1. -3.3, 3.6 ОК1-9	Самостоятельная работа по разделу, Практические занятия №10-16 Тест №4,5	
Раздел 3. Механизмы обеспечения "информационной безопасности"	ПК 1.1-1.4, 2.1-2.4, 3.1. -3.3.3.6 ОК1-9	Самостоятельная работа по разделу, Практические занятия №17-23 Тест №6,7,8	
Промежуточная аттестация			Экзамен

В рамках программы учебной дисциплины реализуется программа воспитания, направленная на формирование следующих личностных результатов (дескриптеров):

ЛР 5. Демонстрирующий приверженность к родной культуре, исторической памяти на основе любви к Родине, родному народу, малой родине, принятию традиционных ценностей многонационального народа России.

ЛР 7.Осознающий приоритетную ценность личности человека; уважающий собственную и чужую уникальность в различных ситуациях, во всех формах и видах деятельности.

ЛР 13. Демонстрирующий готовность обучающегося соответствовать ожиданиям работодателей: ответственный сотрудник, дисциплинированный, трудолюбивый, нацеленный на достижение поставленных задач, эффективно взаимодействующий с членами команды, сотрудничающий с другими людьми, проектно мыслящий.

ЛР 17. Ценностное отношение обучающихся к своему Отечеству, к своей малой и большой Родине, уважительного отношения к ее истории и ответственного отношения к ее современности.

ЛР 18. Ценностное отношение обучающихся к людям иной национальности, веры, культуры, уважительного отношения к ихвзглядам.

ЛР 19. Уважительное отношения обучающихся к результатам собственного и чужого труда.

ЛР 22 Приобретение навыков общения и самоуправления.

ЛР 23. Получение обучающимися возможности самораскрытия и самореализация личности.

2.Результаты освоения учебной дисциплины, подлежащиепроверке

Контроль и оценка результатов освоения дисциплины осуществляется преподавателемвпроцессепроведенияпрактическихзанятийилабораторныхработ, тестирования, а также выполнения обучающимися индивидуальных заданий, проектов,исследований.

Результаты обучения (освоенные умения, усвоенные знания)	**Формы и методы контроля и оценки результатов обучения**
Умения:	
• Классифицировать защищаемую информацию по видам тайны истепеням конфиденциальности; • Применять основные правила и документы системы сертификации Российской федерации; • Классифицировать основные угрозы безопасностиинформации.	практические занятия, выполнение индивидуальных заданий
Знания	
• Сущность и понятие информационной безопасности, характеристику ее составляющих; • Место информационной безопасности в системе национальной безопасности страны; • Современные средства и способы обеспечения информационной безопасности.	выполнение контрольных заданий, тестов, домашняя работа, практические занятия, экзамен

Требования ФГОС СПО к результатам освоениядисциплины:

Код	Наименование результата обучения
ОК 1	Понимать сущность и социальную значимость своей будущей профессии, проявлять к ней устойчивый интерес.
ОК 2	Организовывать собственную деятельность, выбирать типовые методы и способы выполнения профессиональных задач, оценивать их эффективность и качество.
ОК 3	Принимать решения в стандартных и нестандартных ситуациях и нести за них ответственность.
ОК 4	Осуществлять поиск и использование информации, необходимойдля эффективного выполнения профессиональных задач,профессионального и личностного развития.
ОК 5	Использовать информационно-коммуникационные технологии в профессиональной деятельности.
ОК 6	Работать в коллективе и команде, эффективно общаться с коллегами, руководством, потребителями.

ОК 7	Брать на себя ответственность за работу членов команды (подчиненных), результат выполнения заданий.
ОК 8	Самостоятельно определять задачи профессионального и личностного развития, заниматься самообразованием, осознанно планировать повышениеквалификации.
ОК 9	Ориентироваться в условиях частой смены технологий в профессиональной деятельности.
Профессиональные компетенции:	
ПК 1.1.	Выполнять разработку спецификаций отдельных компонент.
ПК 1.2.	Осуществлять разработку кода программного продукта на основе готовых спецификаций на уровне модуля.
ПК 1.3.	Выполнять отладку программных модулей с использованием специализированных программных средств.
ПК 1.4.	Выполнять тестирование программных модулей.
ПК.1.6	Разрабатывать компоненты проектной и технической документации с использованием графических языков спецификаций.
ПК 2.1.	Разрабатывать объекты базы данных.
ПК 2.2.	Разрабатывать и публиковать программное обеспечение и информационные ресурсы отраслевой направленности со статическим и динамическим контентом на основе готовых спецификаций и стандартов.
ПК 2.3.	Проводить отладку и тестирование программного обеспечения отраслевой направленности.
ПК 2.4.	Проводить адаптацию отраслевого программного обеспечения
ПК 3.1.	Разрешать проблемы совместимости программного обеспечения отраслевой направленности
ПК 3.2	Выполнять интеграцию модулей в программную систему.
ПК 3.3.	Проводить обслуживание, тестовые проверки, настройкупрограммного обеспечения отраслевой направленности
ПК 3.4.	Осуществлять разработку тестовых наборов и тестовых сценариев.
ПК 3.5.	Производить инспектирование компонент программного продукта на предмет соответствия стандартам кодирования.
ПК 3.6.	Разрабатывать технологическую документацию.

3.Оценка освоения учебнойдисциплины

3.1.Формы и методы оценивания

Предметом оценки освоения дисциплины являются общие компетенции, умения, знания, способность применять их в практической деятельности и повседневной жизни. Соотношение типов задания и критериев оценки представлено в таблице:

№	Тип (вид) задания	Критерии оценки
1	Тесты	Таблица 1. Шкала оценки образовательных достижений
2	Устные ответы	Таблица 2. Критерии и нормы оценки устных ответов
3	Практическая работа	Выполнение не менее 80% – положительная оценка
4	Проверка конспектов, рефератов, творческих работ, презентаций	Соответствие содержания работы, заявленной теме; правилам оформления работы.

Таблица 1. Шкала оценки образовательных достижений (тестов)

Процент результативности (правильных ответов)	Оценка уровня подготовки	
	балл (отметка)	вербальный аналог
90 ÷ 100	5	отлично
89 ÷ 80	4	хорошо
79 ÷ 70	3	удовлетворительно
мене е 70	2	неудовлетворительно

Таблица 2. Критерии и нормы оценки устных ответов

Оценка	Показатели оценки
«5»	Глубокоеиполноевладениесодержаниемучебногоматериала,вкоторомобучающийся легко ориентируется, умеет применить теоретические знания при решении практическихситуаций,высказатьиобосноватьсвоисуждения,грамотноеилогичное построение высказывания
«4»	Полное освоение учебного материала, грамотное его изложение, владение понятийным аппаратом, но содержание и/или форма ответа имеют отдельные недостатки
«3»	Знание и понимание основных положений учебного материала, неполное и/или непоследовательное его изложение, неточности в определении понятий, отсутствие обоснования высказываемых суждений
«2»	Незнание содержания учебного материала, неумение выделять главное и второстепенное,ошибкивопределениипонятий,искажающиеихсмысл,беспорядочное и неуверенное изложение материала
«1»	Полное незнание и непонимание учебного материала или отказ отвечать

Промежуточная аттестация по результатам освоения обучающимисяучебной дисциплины проводится в формеэкзамена.

3.2 Типовые задания для оценки освоения учебной дисциплины

Устный опрос№1

1. Что такое информационнаябезопасность?
2. Перечислите важнейшие аспекты информационнойбезопасности.
3. Перечислите уровни решения проблемы информационной безопасности.

Устный опрос №2

1. Перечислите уровни защитыинформации.
2. Охарактеризуйте угрозы информационной безопасности: раскрытия целостности, отказ в обслуживании.
3. Объясните причины компьютерныхпреступлений.
4. Опишите, как обнаружить компьютерное преступление или уязвимые места в системе информационнойбезопасности.
5. Опишите основные технологии компьютерныхпреступлений.

Устный опрос №3

1. Перечислите меры защиты информационнойбезопасности.
2. Перечислите меры предосторожности при работе с целью защитыинформации.
3. Опишите, какими способами можно проверить вводимые данные накорректность.
4. Опишите основные меры защиты носителейинформации.
5. ПочемуподключениекглобальнойкомпьютернойсетиИнтернетпредставляетсобойугрозу для информационнойбезопасности?
6. Опишите, как использование электронной почты создает угрозу информационной безопасности. Какие меры обеспечивают безопасное использованиее-mail?

Раздел 1. Информационная безопасность и уровни ее обеспечения

Тест №1

Инструкция: выберите один правильный ответ

1. ВкакомгодувРоссиипоявилисьпервыепреступлениясиспользованиемкомпьютернойтехники (были похищены 125,5 тыс. долларов США воВнешэкономбанке)?

1. 1988;
2. 1991;
3. 1994;
4. 1997;
5. 2002.

2. Сколько выделено основных составляющих национальных интересов Российской Федерации в информационнойсфере?

1. 2;
2. 3;
3. 4;
4. 5;
5. 6.

3. Активный перехват информации это перехват,который:

1. заключается в установке подслушивающего устройства в аппаратуру средств обработки информации;
2. основан на фиксации электромагнитных излучений, возникающих при функционировании средств компьютерной техники икоммуникаций;
3. неправомерно использует технологические отходы информационногопроцесса;
4. осуществляется путем использования оптическойтехники;
5. осуществляется с помощью подключения к телекоммуникационному оборудованию компьютера.

4. Обеспечение национальной безопасности на государственном уровне определяется следующей целью:
1. надежная защита личной и имущественнойбезопасности;
2. обеспечение научно обоснованного и гарантированного государством минимума материальных и экологическихусловий;
3. преодоление конфронтации в обществе, достижение национальногосогласия;
4. обеспечение суверенитета и территориальной целостностиРоссии.

5. К правовым методам защиты информациииотносится:
1. разработка нормативно правовых актов, регламентирующих отношения в информационной сфере;
2. создание и совершенствование системы обеспечения ИБРФ;
3. разработка, использование и совершенствование средств защиты процессов ипрограмм;
4. разработка программ обеспечения ИБ РФ и определение порядка ихфинансирования;
5. формирование системы мониторинга показателей и характеристик ИБРФ.

6. В стандарте «Оранжевая книга» фундаментальное требование, которое относится к группе Подотчетность:
1. управляющие доступом метки должны быть связаны собъектами;
2. необходимо иметь явную и хорошо определенную систему обеспечениябезопасности;
3. индивидуальные субъекты должныидентифицироваться;
4. вычислительная система в своем составе должна иметь аппаратные/программные механизмы, допускающие независимую оценку на предмет того, что система обеспечивает выполнение изложенныхтребований;
5. гарантированно защищенные механизмы, реализующие перечисленные требования, должны быть постоянно защищены от «взламывания» и/или несанкционированного внесенияизменений.

7. К источникам защищаемой информации относится:
1. электрическиеполя;
2. магнитныеполя;
3. электромагнитныеполя;
4. черновики и отходыпроизводства;
5. элементарныечастицы;
6. акустическиеколебания.

8. Информация, использование которой без согласия субъекта может нанести вред его чести, достоинству, деловой репутации:
1. профессиональнаятайна;
2. государственнаятайна;
3. персональныеданные;
4. коммерческаятайна;
5. служебнаятайна.

9. ВруководящемдокументеФСТЭКсистемы,вкоторыхработаетодинпользователь,допущенный ко всей обрабатываемой информации уровня государственной тайны, размещенной на носителях одного уровня конфиденциальности – относятся кгруппе:
1. 1А;
2. 1Г;
3. 2А;
4. 3А;
5.3Б.

10. Защита информации от несанкционированного воздействия это деятельность по предотвращению:
1. получения защищаемой информации заинтересованным субъектом с нарушением установленных правовыми документами или собственником, владельцем информации прав или правил доступа к защищаемойинформации;
2. воздействия с нарушением установленных прав и/или правил на изменение информации, приводящего к искажению, уничтожению, копированию, блокированию доступа к информации, а также к утрате, уничтожению или сбою функционирования носителяинформации;
3. воздействияназащищаемуюинформациюошибокпользователяинформацией,сбоятехнических и программных средств информационных систем, а также природныхявлений;
4. неконтролируемого распространения защищаемой информации от ее разглашения, несанкционированногодоступа;
5. несанкционированного доведения защищаемой информации до неконтролируемого количества получателейинформации.

ТЕСТ №2

Инструкция: выберите один правильный ответ

1. Какой процент утраты информации от действий собственных сотрудников? 1. 5;
2. 10;
3. 15;
4. 60;
5. 80.

2. Защита информацииэто:
1. процесс сбора, накопления, обработки, хранения, распределения и

поискаинформации;
2. преобразование информации, в результате которого содержание информации становится непонятным для субъекта, не имеющегодоступа;
3. получение субъектом возможности ознакомления с информацией, в том числе при помощи техническихсредств;
4. совокупность правил, регламентирующих порядок и условия доступа субъекта к информации и ееносителям;
5. деятельность по предотвращениюутечки информации, несанкционированных и непреднамеренных воздействий нанеѐ.

3. Пассивный перехват информации это перехват, который:
1. заключается в установке подслушивающего устройства в аппаратуру средств обработки информации;
2. основан на фиксации электромагнитных излучений, возникающих при функционировании средств компьютерной техники икоммуникаций;
3. неправомерно использует технологические отходы информационногопроцесса;
4. осуществляется путем использования оптическойтехники;
5. осуществляется с помощью подключения к телекоммуникационному оборудованию компьютера.

2. Обеспечениенациональнойбезопасности на государственном уровне определяется следующейцелью:
1. надежная защита личной и имущественнойбезопасности;
2. обеспечение научно обоснованного и гарантированного государством минимума материальных и экологическихусловий;
3. преодоление конфронтации в обществе, достижение национальногосогласия;
4. обеспечение социально-политической и экономической стабильностистраны;
5. обеспечение признанных международным правом интересов граждан России, проживающих в зарубежных странах.

5. К правовым методам защиты информации относится:
1. создание и совершенствование системы обеспечения ИБРФ;
2. разработка, использование и совершенствование средств защиты процессов ипрограмм;
3. внесение изменений и дополнений в законодательство РФ, регулирующие отношения в области обеспеченияИБ;
4. разработка программ обеспечения ИБ РФ и определение порядка ихфинансирования;
5. формирование системы мониторинга показателей и характеристик ИБРФ.

6. ВстандартеСША«Оранжевойкниге»фундаментальноетребование,котороеотносит сякгруппе Подотчетность:
1. управляющие доступом метки должны быть связаны собъектами;
2. необходимо иметь явную и хорошо определенную систему обеспечениябезопасности;
3. гарантированно защищенные механизмы, реализующие перечисленные требования, должны бытьпостояннозащищеныот«взламывания»и/илинесанкционированноговнесенияиз

менений;4. вычислительная система в своем составе должна иметь аппаратные/программные механизмы, допускающие независимую оценку на предмет того, что система обеспечивает выполнение изложенныхтребований;
5. контрольная информация должна храниться отдельно и защищаться так, чтобы со стороны ответственной за это группы имелась возможность отслеживать действия, влияющие на безопасность.

7. К источникам защищаемой информации относится:
1. электрическиеполя;
2. сырье;
3. магнитныеполя;
4. электромагнитныеполя;
5. элементарныечастицы;
6. акустическиеколебания.

8. Естественные угрозы безопасности информации вызваны:
1. деятельностьючеловека;
2. ошибкамиприпроектированииАСОИ,ееэлементовилиразработкепрограммногообеспечения;
3. воздействиями объективных физических процессов или стихийных природных явлений, независящих отчеловека;
4. корыстными устремлениямизлоумышленников;
5. ошибками при действияхперсонала.

9. ВруководящемдокументеФСТЭКсистемы,вкоторыхработаетодинпользователь,допущенный ко всей обрабатываемой информации уровня не относящейся к государственной тайне, размещенной на носителях одного уровня конфиденциальности – относятся кгруппе:
1. 1А;
2. 1Г;
3. 2А;
4. 3А;
5.3Б.

10. Защита информации от непреднамеренного воздействия это деятельность попредотвращению:
1. получения защищаемой информации заинтересованным субъектом с нарушением установленных правовыми документами или собственником, владельцем информации прав или правил доступа к защищаемойинформации;
2. воздействия с нарушением установленных прав и/или правил на изменение информации, приводящего к искажению, уничтожению, копированию, блокированию доступа к информации, а также к утрате, уничтожению или сбою функционирования носителяинформации;
3. воздействияназащищаемуюинформациюошибокпользователяинформацией,сбоятехнических и программных средств информационных систем, а также природныхявлений;

4. неконтролируемого распространения защищаемой информации от ее разглашения, несанкционированногодоступа;
5. несанкционированного доведения защищаемой информации до неконтролируемого количества получателейинформации.

Тест №3

Инструкция: выберите один правильный ответ

1. КакойобщийущербподаннымИнститутаКомпьютернойБезопасностинанесликомпьютерные вирусы за последние 5 лет, (млрд. долл.США)?
1. 4;
2. 34;
3. 54;
4. 74;
5. 94.

2. Информационные процессыэто:
1. процесс сбора, накопления, обработки, хранения, распределения и поискаинформации;
2. преобразование информации, в результате которого содержание информации становится непонятным для субъекта, не имеющегодоступа;
3. получение субъектом возможности ознакомления с информацией, в том числе при помощи техническихсредств;
4. совокупность правил, регламентирующих порядок и условия доступа субъекта к информации и ееносителям;
5. деятельность по предотвращениюутечки информации, несанкционированных и непреднамеренных воздействий нанеѐ.

3. Аудиоперехват перехват информации это перехват, который:
1. заключается в установке подслушивающего устройства в аппаратуру средств обработки информации;
2. основан на фиксации электромагнитных излучений, возникающих при функционировании средств компьютерной техники икоммуникаций;
3. неправомерно использует технологические отходы информационногопроцесса;
4. осуществляется путем использования оптическойтехники;
5. осуществляется с помощью подключения к телекоммуникационному оборудованию компьютера.

4. Обеспечение национальной безопасности на государственном уровне определяется следующей целью:
1. защита и обеспечение законных прав, свобод и интересовграждан;
2. надежная защита личной и имущественнойбезопасности;
3. обеспечение научно обоснованного и гарантированного государством минимума материальных и экологическихусловий;
4. преодоление конфронтации в обществе, достижение национальногосогласия;
5.обеспечение признанных международным правом интересов граждан России,

проживающих в зарубежных странах.

5. К правовым методам защиты информации относится:
1. создание и совершенствование системы обеспечения ИБРФ;
2. разработка, использование и совершенствование средств защиты процессов ипрограмм;
3. разработка программ обеспечения ИБ РФ и определение порядка ихфинансирования;
4. законодательное разграничение полномочий в области ИБ РФ;
5.формирование системы мониторинга показателей и характеристик ИБРФ.

6. В стандарте «Оранжевая книга» фундаментальное требование, которое относится к группе Гарантии:
1. управляющие доступом метки должны быть связаны собъектами;
2. необходимо иметь явную и хорошо определенную систему обеспечениябезопасности;
3. индивидуальные субъекты должныидентифицироваться;
4. вычислительная система в своем составе должна иметь аппаратные/программные механизмы, допускающие независимую оценку на предмет того, что система обеспечивает выполнение изложенныхтребований;
5. контрольная информация должна храниться отдельно и защищаться так, чтобы со стороны ответственной за это группы имелась возможность отслеживать действия, влияющие на безопасность.

7. К носителям защищаемой информации относится:
1. люди
2. сырье;
3. черновики и отходыпроизводства;
4. документы;
5. акустическиеколебания.

8. Искусственные угрозы безопасности информации вызваны:
1. деятельностьючеловека;
2. ошибкамиприпроектированииАСОИ,ееэлементовилиразработкепрограммногообеспечения;
3. воздействиями объективных физических процессов или стихийных природных явлений, независящих отчеловека;
4. корыстными устремлениямизлоумышленников;
5. ошибками при действияхперсонала.

9. В руководящем документе ФСТЭК системы, в которых работает несколько пользователей, которые имеют одинаковые права доступа ко всей информации уровня государственной тайны, обрабатываемойи/илихранимойнаносителяхразличногоуровняконфиденциальности –относятся кгруппе:
1. 3А;
2. 2А;
3. 1А;

4.3Б;
5. 1Б.

10. Защита информации от разглашения это деятельность попредотвращению:
1. получения защищаемой информации заинтересованным субъектом с нарушением установленных правовыми документами или собственником, владельцем информации прав или правил доступа к защищаемойинформации;
2. воздействия с нарушением установленных прав и/или правил на изменение информации, приводящего к искажению, уничтожению, копированию, блокированию доступа к информации, а также к утрате, уничтожению или сбою функционирования носителяинформации;
3. воздействияназащищаемуюинформациюошибокпользователяинформацией,сбояте хнических и программных средств информационных систем, а также природныхявлений;
4. неконтролируемого распространения защищаемой информации от ее разглашения, несанкционированного доступа; 5. несанкционированного доведения защищаемой информации до неконтролируемого количества получателейинформации.

Раздел 2. Компьютерные вирусы и защита от них

Тест №4

Инструкция: выберите один правильный ответ

1. По данным журнала «SecurityMagazine», средний размер ущерба от компьютерного мошенничества составляет (долл.США):
1. 500 000;
2. 1 000 000;
3. 1 500 000;
4. 2 000 000;
5. 2 500 000.

2. Шифрование информацииэто:
1. процесс сбора, накопления, обработки, хранения, распределения и поискаинформации;
2. преобразование информации, в результате которого содержание информации становится непонятным для субъекта, не имеющегодоступа;
3. получение субъектом возможности ознакомления с информацией, в том числе при помощи техническихсредств;
4. совокупность правил, регламентирующих порядок и условия доступа субъекта к информации и ееносителям;
5. деятельность по предотвращениюутечки информации, несанкционированных и непреднамеренных воздействий нанеѐ.

3. Просмотр мусора это перехват информации, который:
1. заключается в установке подслушивающего устройства в аппаратуру средств обработки информации;

2. основан на фиксации электромагнитных излучений, возникающих при функционировании средств компьютерной техники икоммуникаций;
3. неправомерно использует технологические отходы информационногопроцесса;
4. осуществляется путем использования оптическойтехники;
5. осуществляется с помощью подключения к телекоммуникационному оборудованию компьютера.

4. Обеспечение национальной безопасности на государственном уровне определяется следующей целью:
1. надежная защита личной и имущественнойбезопасности;
2. совершенствование федеративного государственного устройства;
3. обеспечение научно обоснованного и гарантированного государством минимума материальных и экологическихусловий;
4. преодоление конфронтации в обществе, достижение национального согласия;
5.обеспечение признанных международным правом интересов граждан России, проживающих в зарубежных странах.

5. К правовым методам защиты информациииотносится:
1. создание и совершенствование системы обеспечения ИБРФ;
2. разработка, использование и совершенствование средств защиты процессов ипрограмм;
3. разработка программ обеспечения ИБ РФ и определение порядка ихфинансирования;
4. формирование системы мониторинга показателей и характеристик ИБРФ;
5. уточнение статуса иностранных информационных агенств, СМИ ижурналистов.

6. В стандарте «Оранжевая книга» фундаментальное требование, которое относится к группе Гарантии:
1. управляющие доступом метки должны быть связаны собъектами;
2. защищенные механизмы, реализующие перечисленные требования, должны быть постоянно защищены от «взламывания» и/или несанкционированного внесения изменений; 3. индивидуальные субъекты должныидентифицироваться;
4. необходимо иметь явную и хорошо определенную систему обеспечениябезопасности;
5. контрольная информация должна храниться отдельно и защищаться так, чтобы со стороны ответственной за это группы имелась возможность отслеживать действия, влияющие на безопасность.

7. К носителям защищаемой информации относится:
1. элементарныечастицы;
2. люди;
3. сырье;
4. черновики и отходыпроизводства;
5. документы.

8. К основным непреднамеренным искусственным угрозам АСОИ относится:
1. физическое разрушение системы путем взрыва, поджога ит.п.;
2. перехват побочных электромагнитных, акустических и других излучений устройств и линий связи;

3. изменениережимовработыустройствилипрограмм,забастовка,саботажперсонала,п остановка мощных активных помех ит.п.;
4. чтение остаточной информации из оперативной памяти и с внешних запоминающихустройств;
5. неумышленные действия, приводящие к частичному или полному отказу системы или разрушению аппаратных, программных, информационных ресурсовсистемы.

9. В руководящем документе ФСТЭК системы, в которых работает несколько пользователей, которые имеют одинаковые права доступа ко всей информации не относящиеся к уровню государственной тайны, обрабатываемой и/или хранимой на носителях различного уровня конфиденциальности – относятся кгруппе:
1.2Б;
2. 2А;
3. 1А;
4. 3Б;
5. 1Б.

10. Защита информации от несанкционированного доступа это деятельность попредотвращению:
1. получения защищаемой информации заинтересованным субъектом с нарушением установленных правовыми документами или собственником, владельцем информации прав или правил доступа к защищаемойинформации;
2. воздействия с нарушением установленных прав и/или правил на изменение информации, приводящего к искажению, уничтожению, копированию, блокированию доступа к информации, а также к утрате, уничтожению или сбою функционирования носителяинформации;
3. воздействияназащищаемуюинформациюошибокпользователяинформацией,сбояте хнических и программных средств информационных систем, а также природныхявлений;
4. неконтролируемого распространения защищаемой информации от ее разглашения, несанкционированногодоступа;
5. несанкционированного доведения защищаемой информации до неконтролируемого количества получателейинформации.

Тест №5
Инструкция: выберите один правильныйответ

1. По данным Главного информационного центра МВД России количество компьютерных преступлений ежегодно увеличивается в (раза):
1. 2;
2. 2,5;
3. 3;
4. 3,5;
5. 4.

2. Доступ к информацииэто:
1. процесс сбора, накопления, обработки, хранения, распределения и поискаинформации;
2. преобразование информации, в результате которого содержание информации становится непонятным для субъекта, не имеющегодоступа;
3. получение субъектом возможности ознакомления с информацией, в том числе при помощи техническихсредств;
4. совокупность правил, регламентирующих порядок и условия доступа субъекта к информации и ееносителям;
5. деятельность по предотвращениюутечки информации, несанкционированных и непреднамеренных воздействий нанеѐ.

3. Перехват, который заключается в установке подслушивающего устройства в аппаратуру средств обработки информации называется:
1. активныйперехват;
2. пассивныйперехват;
3. аудиоперехват;
4. видеоперехват;
5. просмотрмусора.

4. Обеспечение национальной безопасности на государственном уровне определяется следующей целью:
1. надежная защита личной и имущественнойбезопасности;
2. обеспечение научно обоснованного и гарантированного государством минимума материальных и экологическихусловий;
3. повышение эффективности защиты конституционного строя, правопорядка, борьбы с орг. преступностью икоррупцией;
4. преодоление конфронтации в обществе, достижение национальногосогласия;
5. обеспечение признанных международным правом интересов граждан России, проживающих в зарубежных странах.

5. К организационно-техническим методам защиты информации относится:
1. создание и совершенствование системы обеспечения ИБРФ;
2. разработка программ обеспечения ИБ РФ и определение порядка их финансирования; 3. формирование системы мониторинга показателей и характеристик ИБРФ;
4. уточнение статуса иностранных информационных агентств, СМИ ижурналистов.

6. В международном стандарте «Оранжевая книга» минимальная защита этогруппа:
1. A;
2. B;
3. C;
4. D;
5. E.

7. К носителям защищаемой информации относится:

1. люди;
2. электрическоеполе;
3. сырье;
4. черновики и отходыпроизводства;
5. документы.

8. К основным непреднамеренным искусственным угрозам АСОИ относится:
1. физическое разрушение системы путем взрыва, поджога ит.п.;
2. неправомерное отключение оборудования или изменение режимов работы устройств и программ;
3. изменениережимовработыустройствилипрограмм,забастовка,саботажперсонала,п остановка мощных активных помех ит.п.;
4. чтение остаточной информации из оперативной памяти и с внешних запоминающихустройств;
5. перехват побочных электромагнитных, акустических и других излучений устройств и линий связи.

9. В руководящем документе ФСТЭК многопользовательские системы, в которых одновременно обрабатывается и/или хранится информация разных уровней конфиденциальностидо грифа
«Особо важно» включительно, причем различные пользователи имеют различные права на доступ к информации – относятся к группе:
1.1Б;
2.2Б;
3. 3А;
4. 1А;
5.1В.

10. По характеру воздействия удаленные атаки делятсяна:
1. условные ибезусловные;
2. атаки с обратной связью и без обратнойсвязи;
3. внутрисегментные имежсегментные;
4. пассивные иактивные;
5. атаки, которые могут реализовываться на всех семи уровнях – физическом, канальном, сетевом, транспортном, сеансовом, представительном иприкладном.

Раздел 3. Механизмы обеспечения "информационной

Тест №6
Инструкция: выберите один правильный ответ

1. По данным Главного информационного центра МВД России ежегодный размер материального ущерба от компьютерных преступлений составляет около (млн.рублей):
1. 6;
2. 60;
3. 160;

4. 600;
5. 1600.

2. Субъект доступа к информацииэто:
1. физическое лицо, или материальный объект, в том числе физическое поле, в которых информация находит свое отображение в виде символов, образов, сигналов, технических решений ипроцессов;
2. субъект,осуществляющийпользованиеинформациейиреализующийполномочиярас поряжения в пределах прав, установленных законом и/или собственником информации; 3. субъект, пользующийся информацией, полученной от ее собственника, владельца или посредника в соответствии с установленными правами и правилами доступа к информации либо с их нарушением;
4. субъект, в полном объеме реализующий полномочия владения, пользования, распоряжения информацией в соответствии с законодательнымиактами;
5. участник правоотношений в информационныхпроцессах.

3. Перехват, который осуществляется путем использования оптической техники, называется: 1. активный перехват;
2. пассивныйперехват;
3. аудиоперехват;
4. видеоперехват;
5. просмотрмусора.

4. Обеспечение национальной безопасности на уровне гражданского общества определяется следующей целью:
1. надежная защита личной и имущественнойбезопасности;
2. обеспечение научно обоснованного и гарантированного государством минимума материальных и экологическихусловий;
3. повышение эффективности защиты конституционного строя, правопорядка, борьбы с орг. преступностью икоррупцией;
4. преодоление конфронтации в обществе, достижение национальногосогласия.

5. К организационно-техническим методам защиты информациииотносится:
1. разработка программ обеспечения ИБ РФ и определение порядка ихфинансирования;
2. формирование системы мониторинга показателей и характеристик ИБРФ;
3. уточнение статуса иностранных информационных агентств, СМИ ижурналистов;
4. усиление правоприменительной деятельности федеральных органов исполнительной власти в информационнойсфере.

6. В международном стандарте «Оранжевая книга» индивидуальная защита это группа:
1. A;
2. B;
3. C;
4. D;
5. E.

7. К носителям защищаемой информации относится:
1. люди;
2. сырье;
3. черновики и отходыпроизводства;
4. магнитноеполе;
5. документы.

8. К основным непреднамеренным искусственным угрозам АСОИ относится:
1. физическое разрушение системы путем взрыва, поджога ит.п.;
2. чтение остаточной информации из оперативной памяти и с внешних запоминающихустройств;
3. измененирежимовработыустройствилипрограмм,забастовка,саботажперсонала,п остановка мощных активных помех ит.п.;
4. неумышленная порча носителейинформации;
5. перехват побочных электромагнитных, акустических и других излучений устройств и линий связи.

9. В руководящем документе ФСТЭК многопользовательские системы, в которых одновременно обрабатывается и/или хранится информация разных уровней конфиденциальностидо грифа
«Совершенно секретно» включительно, причем различные пользователи имеют различные права на доступ к информации – относятся к группе:
1.1Б;
2.2Б;
3. 3А;
4. 1А;
5.1В.

10. По цели воздействия удаленные атаки делятсяна:
1. условные ибезусловные;
2. атаки с обратной связью и без обратнойсвязи;
3. внутрисегментные имежсегментные;
4. пассивные иактивные;
5. атаки в зависимости от нарушения конфиденциальности, целостности идоступности.

Тест №7

Инструкция: выберите один правильный ответ

1. По данным Главного информационного центра МВД России средний ущерб, причиняемый потерпевшему от 1 компьютерного преступления, равен (млн.рублей):
1. 7;
2. 1,7;
3. 2,7;
4. 3,7;

5. 4,7.

2. Носитель информацииэто:
1. физическоелицо,илиматериальныйобъект,втомчислефизическоеполе,вкоторыхин формация находит свое отображение в виде символов, образов, сигналов, технических решений ипроцессов;
2. субъект,осуществляющийпользованиеинформациейиреализующийполномочиярас поряжения в пределах прав, установленных законом и/или собственником информации; 3. субъект, пользующийся информацией, полученной от ее собственника, владельца или посредника в соответствии с установленными правами и правилами доступа к информации либо с их нарушением;
4. субъект, в полном объеме реализующий полномочия владения, пользования, распоряжения информацией в соответствии с законодательнымиактами;
5. участник правоотношений в информационныхпроцессах.

3. Перехват, который основан на фиксации электромагнитных излучений, возникающих при функционировании средств компьютерной техники и коммуникаций называется:
1. активныйперехват;
2. пассивныйперехват;
3. аудиоперехват;
4. видеоперехват;
5. просмотрмусора.

4. Обеспечение национальной безопасности на уровне гражданского общества определяется следующей целью:
1. надежная защита личной и имущественнойбезопасности;
2. обеспечение научно обоснованного и гарантированного государством минимума материальных и экологическихусловий;
3. обеспечение признанных международным правом интересов граждан России, проживающих в зарубежных странах;
4. повышение эффективности защиты конституционного строя, правопорядка, борьбы с орг. преступностью икоррупцией;

5. К организационно-техническим методам защиты информациииотносится:
1. разработка программ обеспечения ИБ РФ и определение порядка ихфинансирования;
2. формирование системы мониторинга показателей и характеристик ИБРФ;
3. уточнение статуса иностранных информационных агентств, СМИ ижурналистов;
4. внесение изменений и дополнений в законодательство РФ, регулирующие отношения в области обеспеченияИБ;
5. формирование системы мониторинга показателей и характеристик ИБРФ.

6. В международном стандарте «Оранжевая книга» мандатная защита этогруппа:
1. А;
2. В;
3. С;

4. D;
5. E.

7. Защищаемые государством сведения, распространение которых может нанести ущерб РФ, это:
1. профессиональнаятайна;
2. государственнаятайна;
3. персональныеданные;
4. коммерческаятайна;
5. служебнаятайна.

8. К основным непреднамеренным искусственным угрозам АСОИ относится:
1. запуск технологических программ, способных при некомпетентном использовании вызывать потерю работоспособности системы;
2. чтение остаточной информации из оперативной памяти и с внешних запоминающихустройств;
3. изменениережимовработыустройствилипрограмм,забастовка,саботажперсонала,п остановка мощных активных помех ит.п.;
4. физическое разрушение системы путем взрыва, поджога ит.п.;
5. перехват побочных электромагнитных, акустических и других излучений устройств и линий связи.

9. В руководящем документе ФСТЭК многопользовательские системы, в которых одновременно обрабатывается и/или хранится информация разных уровней конфиденциальности до грифа «Секретно» включительно, причем различные пользователи имеют различные права на доступ к информации – относятся к группе:
1.1Б;
2.2Б;
3. 3А;
4. 1А;
5.1В.

10. По условию начала осуществления воздействия удаленные атаки делятсяна:
1. условные ибезусловные;
2. атаки с обратной связью и без обратнойсвязи;
3. внутрисегментные имежсегментные;
4. пассивные иактивные;
5. атаки в зависимости от нарушения конфиденциальности, целостности идоступности.

Тест №8
Инструкция: выберите один правильный ответ
1. Сколько процентов электронных писем являютсяСпамом? 1. 10;
2. 30;
3. 50;

4. 70;
5. 90.

2. Собственник информацииэто:
1. физическоелицо,илиматериальныйобъект,втомчислефизическоеполе,вкоторыхин формация находит свое отображение в виде символов, образов, сигналов, технических решений ипроцессов;
2. субъект,осуществляющийпользованиеинформациейиреализующийполномочиярас поряжения в пределах прав, установленных законом и/или собственникоминформации;
3. субъект, пользующийся информацией, полученной от ее собственника, владельца или посредника в соответствии с установленными правами и правилами доступа к информации либо с ихнарушением;
4. субъект, в полном объеме реализующий полномочия владения, пользования, распоряжения информацией в соответствии с законодательнымиактами;
5. участник правоотношений в информационныхпроцессах.

3. Перехват, который осуществляется с помощью подключения к телекоммуникационному оборудованию компьютера называется:
1. активныйперехват;
2. пассивныйперехват;
3. аудиоперехват;
4. видеоперехват;
5. просмотрмусора.

4. Обеспечение национальной безопасности на уровне гражданского общества определяется следующей целью:
1. надежная защита личной и имущественнойбезопасности;
2. ускорение процессов формирования институтов самоорганизации гражданскогообщества;
3. обеспечение научно обоснованного и гарантированного государством минимума материальных и экологическихусловий;
4. повышение эффективности защиты конституционного строя, правопорядка, борьбы с орг. преступностью икоррупцией;
5. обеспечение суверенитета и территориальной целостностиРоссии.

5. К экономическим методам защиты информации относится:
1. разработка программ обеспечения ИБ РФ и определение порядка ихфинансирования;
2. уточнение статуса иностранных информационных агентств, СМИ ижурналистов;
3. внесение изменений и дополнений в законодательство РФ, регулирующие отношения в области обеспеченияИБ;
4. формирование системы мониторинга показателей и характеристик ИБРФ.

6. В международном стандарте «Оранжевая книга» верифицированная защита это группа: 1. A;
2. B;

3. C;
4. D;
5. E.

7. Информация представляющая секрет производства(ноу-хау), это:
1. профессиональнаятайна;
2. государственнаятайна;
3. персональныеданные;
4. коммерческаятайна;
5. служебнаятайна.

8. К основным непреднамеренным искусственным угрозам АСОИ относится:
1. физическое разрушение системы путем взрыва, поджога ит.п.;
2. чтение остаточной информации из оперативной памяти и с внешних запоминающихустройств;
3. изменениережимовработыустройствилипрограмм,забастовка,саботажперсонала,п остановка мощных активных помех ит.п.;
4. нелегальное внедрение и использование неучтенныхпрограмм игровых, обучающих, технологических и др., не являющихся необходимыми для выполнения служебныхобязанностей;
5. перехват побочных электромагнитных, акустических и других излучений устройств и линий связи.

9. В руководящем документе ФСТЭК многопользовательские системы, в которых одновременно обрабатывается и/или хранится информация разных уровней конфиденциальности в том числе Персональные данные, причем различные пользователи имеют различные права на доступ к информации – относятся кгруппе:
1.1Б;
2. 1Г;
3. 3А;
4. 1А;
5. 1В.

10. По наличию обратной связи с атакуемым объектом удаленные атаки делятсяна:
1. условные ибезусловные;
2. атаки с обратной связью и без обратнойсвязи;
3. внутрисегментные имежсегментные;
4. пассивные иактивные;
5. атаки в зависимости от нарушения конфиденциальности, целостности идоступности.

Литература:

1. Литвиненко, В.И. Основы информационной безопасности : учебное пособие / Литвиненко В.И., Козлов Е.С. — Москва : КноРус, 2020. — 199 с. — ISBN 978-5-406-00904-8. — URL: https://book.ru/book/934627

2. Гультяева, Т. А. Основы информационной безопасности : учебное пособие / Т. А. Гультяева. — Новосибирск : НГТУ, 2018. — 79 с. — ISBN 978-5-7782-3640-0. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/118233

3. Мызникова, Т. А. Основы информационной безопасности : учебное пособие / Т. А. Мызникова. — Омск :ОмГУПС, 2017. — 82 с. — ISBN 978-5-949-41160-5. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/129192

4.Контрольно-оценочные материалы для итоговой аттестации по учебнойдисциплине

МИНИСТЕРСТВО ТРАНСПОРТА РОССИЙСКОЙ ФЕДЕРАЦИИ
ФЕДЕРАЛЬНОЕ АГЕНТСТВО ЖЕЛЕЗНОДОРОЖНОГО ТРАНСПОРТА
ФИЛИАЛ ФЕДЕРАЛЬНОГО ГОСУДАРСТВЕННОГО БЮДЖЕТНОГО ОБРАЗОВАТЕЛЬНОГО УЧРЕЖДЕНИЯВЫСШЕГО ОБРАЗОВАНИЯ
«САМАРСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ПУТЕЙ СООБЩЕНИЯ» в г. Алатыре

Рассмотрено цикловой комиссией специальности 09.02.03 Председатель _____Р.В.Пасюнина «_____»_____20г.	Экзамен по дисциплине Основы информационной безопасности Специальность 09.02.03 Экзаменационный билет №1	УТВЕРЖДАЮ: Заместитель директора по учебной работе _____Т.Ю.Базилевич «_____»_____20 г.

Коды проверяемых компетенций: ОК1-ОК9.
Место проведения экзамена — кабинет № 303
Инструкция:

1. Внимательно прочитайте задание.
2. Экзамен состоит из двух частей:
   - Часть А – ответы на вопросы
   - Часть Б – выполнение практического задания.
3. Время выполнения задания – 30 минут.

Задание 1.Информационная безопасность человека и общества. Уровни защиты информационных ресурсов. Признаки, свидетельствующие о наличии уязвимых мест в информационной безопасности.

Задание 2.Компьютерные преступления. Основные технологии, использующиеся при совершении компьютерных преступлений. Ответьте на вопрос: Понятие информации. Виды информации.

Задание 3. Перейдите от двоичного кода к десятичному и декодируйте следующий текст:01000101

01101110 01110100 01100101 01110010.

Критерии оценок:

Оценка «5»:	- Выполнены полностью части А и Б
Оценка «4»	- Выполнена часть Б, часть А выполнена не полностью
Оценка «3»	- Выполнена только часть Б
Оценка «2»	- Работа не выполнена

Преподаватель:_____Т.Ю. Самкина

5. Лист согласования

Дополнения и изменения к комплекту ФОС на учебный год Дополнения и изменения к комплектуФОСна_____учебный год по дисциплине _____

ВкомплектФОСвнесеныследующиеизменения:

_____
_____
_____
_____
_____
_____
_____
_____

Дополнения и изменения в комплекте ФОСобсуждены на заседании ЦК_ «_____»_____20____г. (протокол№ _____).

ПредседательЦК_____/ /