МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ
РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное автономное образовательное учреждение
высшего образования
«ТЮМЕНСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»
Тобольский педагогический институт им. Д.И. Менделеева (филиал)
Тюменского государственного университета

УТВЕРЖДАЮ
Директор
_____ Шилов С.П

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ
учебной дисциплины ОП.15 Методы и средства защиты информации
для обучающихся по программе подготовки специалистов среднего звена
09.02.05 Прикладная информатика (по отраслям)
(базовая подготовка)
Форма обучения – очная

Маковийчук Л.Ф. ОП.15 Методы и средства защиты информации. Фонд оценочных средств дисциплины для обучающихся по программе подготовки специалистов среднего звена 09.02.05 Прикладная информатика (по отраслям) Форма обучения – очная. Тобольск, 2020.

Фонд оценочных средств разработан на основе ФГОС СПО по специальности 09.02.05 Прикладная информатика (по отраслям), утвержденного приказом Министерства образования и науки Российской Федерации от 13 августа 2014 года, № 1001.

Содержание

1. Общая характеристика фондов оценочных средств

1.1. Область применения программы

Фонд оценочных средств учебной дисциплины ОП.15 Методы и средства защиты информации является частью программы подготовки специалистов среднего звена в соответствии с ФГОС СПО в соответствии с ФГОС по специальности СПО 09.02.05 Прикладная информатика (по отраслям) базовой подготовки.

Фонд оценочных средств учебной дисциплины ОП.15 Методы и средства защиты информации может быть использован в профессиональной подготовке студентов по квалификации – техник-программист.

1.2. Место дисциплины в структуре программы подготовки специалистов среднего звена

Дисциплина ОП.15 Методы и средства защиты информации входит в профессиональный учебный цикл.

1.3. Цели и задачи дисциплины – требования к результатам освоения дисциплины.

уметь:

В результате освоения дисциплины обучающийся должен **уметь**:

У1 классифицировать защищаемую информацию по видам тайны и степеням конфиденциальности;

У2 применять основные правила и документы системы сертификации Российской Федерации;

У3 классифицировать основные угрозы безопасности информации. в результате освоения дисциплины обучающийся должен **знать**:

З1 сущность и понятие информационной безопасности, характеристику ее составляющих;

З2 место информационной безопасности в системе национальной безопасности страны;

З3 современные средства и способы обеспечения информационной безопасности.

В результате освоения дисциплины обучающийся должен обладать следующими компетенциями:

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 8. Самостоятельно определять задачи профессионального и личностного развития, заниматься самообразованием, осознанно планировать повышение квалификации.

ОК 9. Ориентироваться в условиях частой смены технологий в профессиональной деятельности.

ПК.3.4. Работать с системами управления взаимоотношениями с клиентами.

Код ОК, ПК	Умения	Знания
ОК1	У1	З1
ОК2	У2	З1, З2
ОК3	У3	З1, З2, З3
ОК8	У2	З1, З2, З3
ОК9	У3	З1, З2, З3

ПК.3.4	У1, У2, У3	З1, З2, З3

2.Паспорт фонда оценочных средств

	п/п	Темы дисциплины, МДК, разделы (этапы) практики, в ходе текущего контроля, вид промежуточной аттестации с указанием семестра	Код контролируемой компетенции (или её части), знаний, умений	Наименование оценочного средства (с указанием количество вариантов, заданий и т.п.)
1.		Раздел 1. Информационная безопасность	З1, З2, У1	Тестирование, устный опрос
2.		Раздел 2. Сущность и понятие защиты информации	З1, У1, ОК1	Тестирование, защита лабораторных работ
3.		Раздел 3. Основы защиты информации	З3, У3	Тестирование, устный опрос, защита лабораторных работ
4.		Раздел 4. Правовое обеспечение информационной безопасности	У2, З2, ОК2, ОК8	Тестирование, устный опрос
5.		Раздел. 5. Организационные основы защиты информации	У3, З3, ПК.3.4, ОК.3	Тестирование, устный опрос, защита лабораторных работ
6.		Раздел 6. Обеспечение безопасности автоматизированных систем.	У3, З3, ПК.3.4, ОК9	Тестирование, защита лабораторных работ
7.		Промежуточная аттестация	У1-У3, З1-З3, ОК1, ОК2, ОК3, ОК8, ОК9, ПК.3.4	Экзамен

Типовые задания для оценки дисциплины

	п/п	Темы дисциплины, МДК, разделы (этапы) практики, в ходе текущего контроля, вид промежуточной аттестации с указанием семестра	Код контролируемой компетенции (или её части), знаний, умений	Наименование оценочного средства (с указанием количество вариантов, заданий и т.п.)
1.		Раздел 1. Информационная безопасность	З1, З2, У1	Тестирование, устный опрос

Устный опрос

1. Что такое информационная безопасность?
2. Перечислите важнейшие аспекты информационной безопасности.
3. Перечислите уровни решения проблемы информационной безопасности.

Таблица Критерии и нормы оценки устных ответов

Оценка	Показатели оценки
«5»	Глубокое и полное владение содержанием учебного материала, в котором обучающийся легко ориентируется, умеет применить теоретические знания при решении практических ситуаций, высказать и обосновать свои суждения, грамотное и логичное по- строение 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, ошибки в определении понятий, искажающие их смысл, беспорядочное и неуве ренное изложение материала
«1»	Полное незнание и непонимание учебного материала или отказ отвечать

Тестирование

Инструкция: выберите один правильный ответ

1. В каком году в России появились первые преступления с использованием компьютерной техники (были похищены 125,5 тыс. долларов США во Внешэкономбанке)?

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

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

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 и коммуникаций;
3. неправомерно использует технологические отходы информационного процесса;
4. осуществляется путем использования оптической техники;
5. осуществляется с помощью подключения к телекоммуникационному оборудованию компьютера.

4. Обеспечение национальной безопасности на государственном уровне определяется следующей целью:
1. надежная защита личной и имущественной безопасности;
2. обеспечение научно обоснованного и гарантированного государством минимума материальных и экологических условий;
3. преодоление конфронтации в обществе, достижение национального согласия;
4. обеспечение суверенитета и территориальной целостности России.

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

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

7. К источникам защищаемой информации относится:
1. электрические поля;
2. магнитные поля;
3. электромагнитные поля;
4. черновики и отходы производства;
5. элементарные частицы;
6. акустические колебания.

8. Информация, использование которой без согласия субъекта может нанести вред его чести, достоинству, деловой репутации:
1. профессиональная тайна;
2. государственная тайна;
3. персональные данные;
4. коммерческая тайна;
5. служебная тайна.

9. В руководящем документе ФСТЭК системы, в которых работает один пользователь, допущенный ко всей обрабатываемой информации уровня государственной тайны, размещенной на носителях одного уровня конфиденциальности – относятся к группе:
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 защищаемой информации;
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 носителя информации;
3. воздействия на защищаемую информацию ошибок пользователя информацией, сбоя технических и программных средств информационных систем, а также природных явлений;
4. неконтролируемого распространения защищаемой информации от ее разглашения, несанкционированного доступа;
5. несанкционированного доведения защищаемой информации до неконтролируемого количества получателей информации.

Таблица. 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
менее 70	2	неудовлетворительно

	п/п	Темы дисциплины, МДК, разделы (этапы) практики, в ходе текущего контроля, вид промежуточной аттестации с указанием семестра	Код контролируемой компетенции (или её части), знаний, умений	Наименование оценочного средства (с указанием количество вариантов, заданий и т.п.)
1.		Раздел 2. Сущность и понятие защиты информации	З1, У1	Тестирование, защита лабораторных работ

Тестирование №1

1. Какой процент утраты информации от действий собственных сотрудников?

1. 5;
2. 10;
3. 15;
4. 60;
5. 80.

2. Защита информации это:

1. процесс сбора, накопления, обработки, хранения, распределения и поиска информации;
2. преобразование информации, в результате которого содержание информации становится непонятным для субъекта, не имеющего доступа;
3. получение субъектом возможности ознакомления с информацией, в том числе при помощи технических средств;
4. совокупность правил, регламентирующих порядок и условия доступа субъекта к информации и ее носителям;
5. деятельность по предотвращению утечки информации, несанкционированных и непреднамеренных воздействий на неѐ.

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 и коммуникаций;
3. неправомерно использует технологические отходы информационного процесса;
4. осуществляется путем использования оптической техники;
5. осуществляется с помощью подключения к телекоммуникационному оборудованию компьютера.

4. Обеспечение национальной безопасности на государственном уровне определяется следующей целью:

1. надежная защита личной и имущественной безопасности;
2. обеспечение научно обоснованного и гарантированного государством минимума материальных и экологических условий;
3. преодоление конфронтации в обществе, достижение национального согласия;
4. обеспечение социально-политической и экономической стабильности страны;
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 ИБ РФ;

2. разработка, использование и совершенствование средств защиты процессов и программ;
3. внесение изменений и дополнений в законодательство РФ, регулирующие отношения в области обеспечения ИБ;
4. разработка программ обеспечения ИБ РФ и определение порядка их финансирования;
5. формирование системы мониторинга показателей и характеристик ИБ РФ.

6. В стандарте США «Оранжевой книге» фундаментальное требование, которое относится к группе Подотчетность:
1. управляющие доступом метки должны быть связаны с объектами;
2. необходимо иметь явную и хорошо определенную систему обеспечения безопасности;
3. гарантированно защищенные механизмы, реализующие перечисленные требования, должны быть постоянно защищены от «взламывания» и/или несанкционированного внесения изменений;
4. вычислительная система в своем составе должна иметь аппаратные/программные механизмы, допускающие независимую оценку на предмет того, что система обеспечивает выполнение изложенных требований;
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. электрические поля;
2. сырье;
3. магнитные поля;
4. электромагнитные поля;
5. элементарные частицы;
6. акустические колебания.

8. Естественные угрозы безопасности информации вызваны:
1. деятельностью человека;
2. ошибками при проектировании АСОИ, ее элементов или разработке программного обеспечения;
3. воздействиями объективных физических процессов или стихийных природных явлений, независящих от человека;
4. корыстными устремлениями злоумышленников;
5. ошибками при действиях персонала.

9. В руководящем документе ФСТЭК системы, в которых работает один пользователь, допущенный ко всей обрабатываемой информации уровня не относящейся к государственной тайне, размещенной на носителях одного уровня конфиденциальности – относятся к группе:
1. 1А;
2. 1Г;
3. 2А;
4. 3А;
5. 3Б.

10. Защита информации от непреднамеренного 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 защищаемой информации;

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 носителя информации;
3. воздействия на защищаемую информацию ошибок пользователя информацией, сбоя технических и программных средств информационных систем, а также природных явлений;
4. неконтролируемого распространения защищаемой информации от ее разглашения, несанкционированного доступа;
5. несанкционированного доведения защищаемой информации до неконтролируемого количества получателей информации.

Тестирование №2

1. Какой общий ущерб по данным Института Компьютерной Безопасности нанесли компьютерные вирусы за последние 5 лет, (млрд. долл. США)?

1. 4;
2. 34;
3. 54;
4. 74;
5. 94.

2. Информационные процессы это:

1. процесс сбора, накопления, обработки, хранения, распределения и поиска информации;
2. преобразование информации, в результате которого содержание информации становится непонятным для субъекта, не имеющего доступа;
3. получение субъектом возможности ознакомления с информацией, в том числе при помощи технических средств;
4. совокупность правил, регламентирующих порядок и условия доступа субъекта к информации и ее носителям;
5. деятельность по предотвращению утечки информации, несанкционированных и непреднамеренных воздействий на неѐ.

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 и коммуникаций;
3. неправомерно использует технологические отходы информационного процесса;
4. осуществляется путем использования оптической техники;
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 интересов граждан;
2. надежная защита личной и имущественной безопасности;
3. обеспечение научно обоснованного и гарантированного государством минимума материальных и экологических условий;
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 информации относится:
1. создание и совершенствование системы обеспечения ИБ РФ;
2. разработка, использование и совершенствование средств защиты процессов и программ;
3. разработка программ обеспечения ИБ РФ и определение порядка их финансирования;
4. законодательное разграничение полномочий в области ИБ РФ; 5.формирование системы мониторинга показателей и характеристик ИБ РФ.

6. В стандарте «Оранжевая книга» фундаментальное требование, которое относится к группе Гарантии:
1. управляющие доступом метки должны быть связаны с объектами;
2. необходимо иметь явную и хорошо определенную систему обеспечения безопасности;
3. индивидуальные субъекты должны идентифицироваться;
4. вычислительная система в своем составе должна иметь аппаратные/программные механизмы, допускающие независимую оценку на предмет того, что система обеспечивает выполнение изложенных требований;
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 отходы производства;
4. документы;
5. акустические колебания.

8. Искусственные угрозы безопасности информации вызваны:
1. деятельностью человека;
2. ошибками при проектировании АСОИ, ее элементов или разработке программного обеспечения;
3. воздействиями объективных физических процессов или стихийных природных явлений, независящих от человека;
4. корыстными устремлениями злоумышленников;
5. ошибками при действиях персонала.

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

10. Защита информации от разглашения это деятельность по предотвращению:
1. получения защищаемой информации заинтересованным субъектом с нарушением установленных правовыми документами или собственником, владельцем информации прав или правил доступа к защищаемой информации;
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 носителя информации;
3. воздействия на защищаемую информацию ошибок пользователя информацией, сбоя технических и программных средств информационных систем, а также природных явлений;
4. неконтролируемого распространения защищаемой информации от ее разглашения, несанкционированного доступа; 5. несанкционированного доведения защищаемой информации до неконтролируемого количества получателей информации.

Таблица. 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
менее 70	2	неудовлетворительно

	п/п	Темы дисциплины, МДК, разделы (этапы) практики, в ходе текущего контроля, вид промежуточной аттестации с указанием семестра	Код контролируемой компетенции (или её части), знаний, умений	Наименование оценочного средства (с указанием количество вариантов, заданий и т.п.)
1.		Раздел 3. Основы защиты информации	З3, У3	Тестирование, устный опрос, защита лабораторных работ

Тестирование
Инструкция: выберите один правильный ответ

1. По данным журнала «Security Magazine», 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 информации это:
1. процесс сбора, накопления, обработки, хранения, распределения и поиска информации;
2. преобразование информации, в результате которого содержание информации становится непонятным для субъекта, не имеющего доступа;
3. получение субъектом возможности ознакомления с информацией, в том числе при помощи технических средств;
4. совокупность правил, регламентирующих порядок и условия доступа субъекта к информации и ее носителям;
5. деятельность по предотвращению утечки информации, несанкционированных и непреднамеренных воздействий на неѐ.

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 и коммуникаций;
3. неправомерно использует технологические отходы информационного процесса;
4. осуществляется путем использования оптической техники;
5. осуществляется с помощью подключения к телекоммуникационному оборудованию компьютера.

4. Обеспечение национальной безопасности на государственном уровне определяется следующей целью:
1. надежная защита личной и имущественной безопасности;
2. совершенствование федеративного государственного устройства;
3. обеспечение научно обоснованного и гарантированного государством минимума материальных и экологических условий;
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 информации относится:

1. создание и совершенствование системы обеспечения ИБ РФ;
2. разработка, использование и совершенствование средств защиты процессов и программ;
3. разработка программ обеспечения ИБ РФ и определение порядка их финансирования;
4. формирование системы мониторинга показателей и характеристик ИБ РФ;
5. уточнение статуса иностранных информационных агенств, СМИ и журналистов.

6. В стандарте «Оранжевая книга» фундаментальное требование, которое относится к группе Гарантии:
1. управляющие доступом метки должны быть связаны с объектами;
2. защищенные механизмы, реализующие перечисленные требования, должны быть постоянно защищены от «взламывания» и/или несанкционированного внесения изменений; 3. индивидуальные субъекты должны идентифицироваться;
4. необходимо иметь явную и хорошо определенную систему обеспечения безопасности;
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. элементарные частицы;
2. люди;
3. сырье;
4. черновики и отходы производства;
5. документы.

8. К основным непреднамеренным искусственным угрозам АСОИ относится:
1. физическое разрушение системы путем взрыва, поджога и т.п.;
2. перехват побочных электромагнитных, акустических и других излучений устройств и линий связи;
3. изменение режимов работы устройств или программ, забастовка, саботаж персонала, постановка мощных активных помех и т.п.;
4. чтение остаточной информации из оперативной памяти и с внешних запоминающих устройств;
5. неумышленные действия, приводящие к частичному или полному отказу системы или разрушению аппаратных, программных, информационных ресурсов системы.

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 к группе:
1. 2Б;
2. 2А;
3. 1А;
4. 3Б;
5. 1Б.

10. Защита информации от несанкционированного доступа это деятельность по предотвращению:
1. получения защищаемой информации заинтересованным субъектом с нарушением установленных правовыми документами или собственником, владельцем информации прав или правил доступа к защищаемой информации;
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 носителя информации;
3. воздействия на защищаемую информацию ошибок пользователя информацией, сбоя технических и программных средств информационных систем, а также природных явлений;
4. неконтролируемого распространения защищаемой информации от ее разглашения, несанкционированного доступа;
5. несанкционированного доведения защищаемой информации до неконтролируемого количества получателей информации.

Таблица. 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
менее 70	2	неудовлетворительно

	п/п	Темы дисциплины, МДК, разделы (этапы) практики, в ходе текущего контроля, вид промежуточной аттестации с указанием семестра	Код контролируемой компетенции (или её части), знаний, умений	Наименование оценочного средства (с указанием количество вариантов, заданий и т.п.)
1.		Раздел 4. Правовое обеспечение информационной безопасности	У2, З2	Тестирование, устный опрос

Устный опрос

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

Таблица Критерии и нормы оценки устных ответов

Оценка	Показатели оценки
«5»	Глубокое и полное владение содержанием учебного материала, в котором обучающийся легко ориентируется, умеет применить теоретические знания при решении практических ситуаций, высказать и обосновать свои суждения, грамотное и логичное по- строение 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, ошибки в определении понятий, искажающие их смысл, беспорядочное и неуве ренное изложение материала
«1»	Полное незнание и непонимание учебного материала или отказ отвечать

Тестирование

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 информации это:

1. процесс сбора, накопления, обработки, хранения, распределения и поиска информации;

2. преобразование информации, в результате которого содержание информации становится непонятным для субъекта, не имеющего доступа;
3. получение субъектом возможности ознакомления с информацией, в том числе при помощи технических средств;
4. совокупность правил, регламентирующих порядок и условия доступа субъекта к информации и ее носителям;
5. деятельность по предотвращению утечки информации, несанкционированных и непреднамеренных воздействий на неѐ.

3. Перехват, который заключается в установке подслушивающего устройства в аппаратуру средств обработки информации называется:
1. активный перехват;
2. пассивный перехват;
3. аудиоперехват;
4. видеоперехват;
5. просмотр мусора.

4. Обеспечение национальной безопасности на государственном уровне определяется следующей целью:
1. надежная защита личной и имущественной безопасности;
2. обеспечение научно обоснованного и гарантированного государством минимума материальных и экологических условий;
3. повышение эффективности защиты конституционного строя, правопорядка, борьбы с орг. преступностью и коррупцией;
4. преодоление конфронтации в обществе, достижение национального согласия;
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 ИБ РФ;
2. разработка программ обеспечения ИБ РФ и определение порядка их финансирования; 3. формирование системы мониторинга показателей и характеристик ИБ РФ;
4. уточнение статуса иностранных информационных агентств, СМИ и журналистов.

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

7. К носителям защищаемой информации относится:
1. люди;
2. электрическое поле;
3. сырье;
4. черновики и отходы производства;
5. документы.

8. К основным непреднамеренным искусственным угрозам АСОИ относится:
1. физическое разрушение системы путем взрыва, поджога и т.п.;
2. неправомерное отключение оборудования или изменение режимов работы

устройств и программ;
3. изменение режимов работы устройств или программ, забастовка, саботаж персонала, постановка мощных активных помех и т.п.;
4. чтение остаточной информации из оперативной памяти и с внешних запоминающих устройств;
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
«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 делятся на:
1. условные и безусловные;
2. атаки с обратной связью и без обратной связи;
3. внутрисегментные и межсегментные;
4. пассивные и активные;
5. атаки, которые могут реализовываться на всех семи уровнях – физическом, канальном, сетевом, транспортном, сеансовом, представительном и прикладном.

Таблица. 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
менее 70	2	неудовлетворительно

	п/п	Темы дисциплины, МДК, разделы (этапы) практики, в ходе текущего контроля, вид промежуточной аттестации с указанием семестра	Код контролируемой компетенции (или её части), знаний, умений	Наименование оценочного средства (с указанием количество вариантов, заданий и т.п.)
1.		Раздел. 5. Организационные основы защиты информации	У3, З3, ПК.3.4	Тестирование, устный опрос, защита лабораторных работ

Тестирование

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 информации это:
1. физическое лицо, или материальный объект, в том числе физическое поле, в которых информация находит свое отображение в виде символов, образов, сигналов, технических решений и процессов;
2. субъект, осуществляющий пользование информацией и реализующий полномочия распоряжения 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 законодательными актами;
5. участник правоотношений в информационных процессах.

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

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

5. К организационно-техническим методам защиты информации относится:
1. разработка программ обеспечения ИБ РФ и определение порядка их финансирования;
2. формирование системы мониторинга показателей и характеристик ИБ РФ;

3. уточнение статуса иностранных информационных агентств, СМИ и журналистов;
4. усиление правоприменительной деятельности федеральных органов исполнительной власти в информационной сфере.

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 отходы производства;
4. магнитное поле;
5. документы.

8. К основным непреднамеренным искусственным угрозам АСОИ относится:
1. физическое разрушение системы путем взрыва, поджога и т.п.;
2. чтение остаточной информации из оперативной памяти и с внешних запоминающих устройств;
3. изменение режимов работы устройств или программ, забастовка, саботаж персонала, постановка мощных активных помех и т.п.;
4. неумышленная порча носителей информации;
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
«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 делятся на:
1. условные и безусловные;
2. атаки с обратной связью и без обратной связи;
3. внутрисегментные и межсегментные;
4. пассивные и активные;
5. атаки в зависимости от нарушения конфиденциальности, целостности и доступности.

Таблица. 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

менее 70	2	неудовлетворительно

Устный опрос

1. Перечислите меры защиты информационной безопасности.
2. Перечислите меры предосторожности при работе с целью защиты информации.
3. Опишите, какими способами можно проверить вводимые данные на корректность.
4. Опишите основные меры защиты носителей информации.
5. Почему подключение к глобальной компьютерной сети Интернет представляет собой угрозу для информационной безопасности?
6. Опишите,как использование электронной почты создает угрозу информационной безопасности. Какие меры обеспечивают безопасное использование e-mail?

Таблица Критерии и нормы оценки устных ответов

Оценка	Показатели оценки
«5»	Глубокое и полное владение содержанием учебного материала, в котором обучающийся легко ориентируется, умеет применить теоретические знания при решении практических ситуаций, высказать и обосновать свои суждения, грамотное и логичное по- строение 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, ошибки в определении понятий, искажающие их смысл, беспорядочное и неуве ренное изложение материала
«1»	Полное незнание и непонимание учебного материала или отказ отвечать

	п/п	Темы дисциплины, МДК, разделы (этапы) практики, в ходе текущего контроля, вид промежуточной аттестации с указанием семестра	Код контролируемой компетенции (или её части), знаний, умений	Наименование оценочного средства (с указанием количество вариантов, заданий и т.п.)
1.		Раздел 6. Обеспечение безопасности автоматизированных систем.	У3, З3, ПК.3.4	Тестирование, защита лабораторных работ

Тестирование №1

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 информации это:
1. физическое лицо, или материальный объект, в том числе физическое поле, в которых информация находит свое отображение в виде символов, образов, сигналов, технических решений и процессов;
2. субъект, осуществляющий пользование информацией и реализующий полномочия распоряжения 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 законодательными актами;
5. участник правоотношений в информационных процессах.

3. Перехват, который основан на фиксации электромагнитных излучений, возникающих при функционировании средств компьютерной техники и коммуникаций называется:
1. активный перехват;
2. пассивный перехват;
3. аудиоперехват;
4. видеоперехват;
5. просмотр мусора.

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

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

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

7. Защищаемые государством сведения, распространение которых может нанести ущерб РФ, это:
1. профессиональная тайна;
2. государственная тайна;
3. персональные данные;
4. коммерческая тайна;
5. служебная тайна.

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 запоминающих устройств;
3. изменение режимов работы устройств или программ, забастовка, саботаж персонала, постановка мощных активных помех и т.п.;
4. физическое разрушение системы путем взрыва, поджога и т.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 делятся на:
1. условные и безусловные;
2. атаки с обратной связью и без обратной связи;
3. внутрисегментные и межсегментные;
4. пассивные и активные;
5. атаки в зависимости от нарушения конфиденциальности, целостности и доступности.

Тестирование №2

Инструкция: выберите один правильный ответ

1. Сколько процентов электронных писем являются Спамом? 1. 10;
2. 30;
3. 50;
4. 70;
5. 90.

2. Собственник информации это:

1. физическое лицо, или материальный объект, в том числе физическое поле, в которых информация находит свое отображение в виде символов, образов, сигналов, технических решений и процессов;
2. субъект, осуществляющий пользование информацией и реализующий полномочия распоряжения 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 законодательными актами;
5. участник правоотношений в информационных процессах.

3. Перехват, который осуществляется с помощью подключения к телекоммуникационному оборудованию компьютера называется:

1. активный перехват;
2. пассивный перехват;
3. аудиоперехват;
4. видеоперехват;
5. просмотр мусора.

4. Обеспечение национальной безопасности на уровне гражданского общества определяется следующей целью:

1. надежная защита личной и имущественной безопасности;
2. ускорение процессов формирования институтов самоорганизации гражданского общества;
3. обеспечение научно обоснованного и гарантированного государством минимума материальных и экологических условий;
4. повышение эффективности защиты конституционного строя, правопорядка, борьбы с орг. преступностью и коррупцией;
5. обеспечение суверенитета и территориальной целостности России.

5. К экономическим методам защиты информации относится:

1. разработка программ обеспечения ИБ РФ и определение порядка их финансирования;
2. уточнение статуса иностранных информационных агентств, СМИ и журналистов;
3. внесение изменений и дополнений в законодательство РФ, регулирующие отношения в области обеспечения ИБ;
4. формирование системы мониторинга показателей и характеристик ИБ РФ.

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. профессиональная тайна;
2. государственная тайна;
3. персональные данные;
4. коммерческая тайна;
5. служебная тайна.

8. К основным непреднамеренным искусственным угрозам АСОИ относится:
1. физическое разрушение системы путем взрыва, поджога и т.п.;
2. чтение остаточной информации из оперативной памяти и с внешних запоминающих устройств;
3. изменение режимов работы устройств или программ, забастовка, саботаж персонала, постановка мощных активных помех и т.п.;
4. нелегальное внедрение и использование неучтенных программ игровых, обучающих, технологических и др., не являющихся необходимыми для выполнения служебных обязанностей;
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 к группе:
1. 1Б;
2. 1Г;
3. 3А;
4. 1А;
5. 1В.

10. По наличию обратной связи с атакуемым объектом удаленные атаки делятся на:
1. условные и безусловные;
2. атаки с обратной связью и без обратной связи;
3. внутрисегментные и межсегментные;
4. пассивные и активные;
5. атаки в зависимости от нарушения конфиденциальности, целостности и доступности.

Таблица. Шкала оценки образовательных достижений (тестов)

6.

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

п/п	Темы дисциплины, МДК, разделы (этапы) практики, в ходе текущего контроля, вид промежуточной аттестации с указанием семестра	Код контролируемой компетенции (или её части), знаний, умений	Наименование оценочного средства (с указанием количество вариантов, заданий и т.п.)
1.	Промежуточная аттестация	У1-У3, З1-З3, ОК1, ОК2, ОК3, ОК8, ОК9, ПК.3.4	Экзамен

Перечень теоретических вопросов для подготовки к экзамену:

1. Информационная безопасность человека и общества. Уровни защиты информационных ресурсов. Признаки, свидетельствующие о наличии уязвимых мест в информационной безопасности.
2. Компьютерные преступления. Основные технологии, использующиеся при совершении компьютерных преступлений.
3. Объекты защиты информации. Защита информации ограниченного доступа: государственная тайна, коммерческая тайна.
4. Основные каналы утечки информации. Защита от утечки информации по техническим каналам.
5. Методы и средства защиты информации. Содержание способов и средств обеспечения безопасности информации.
6. Реализация методов и средств защиты информации.
7. Средства опознания и разграничения доступа к информации.
8. Криптография. Симметричные криптосистемы.
9. Криптография. Асимметричные криптосистемы.
10. Обзор и классификация методов шифрования информации.
11. Электронно-цифровая подпись.
12. Основные алгоритмы шифрования данных: ГОСТ.
13. Правовые средства защиты информации. Защита программных продуктов. Авторское право.
14. Защита данных в автономном компьютере.
15. Защита данных в вычислительных сетях. Разработка сетевых аспектов политики безопасности.
16. Защита данных в вычислительных сетях. Межсетевые экраны. Сканеры.
17. Показатели оценки достоверности (безошибочности) передачи данных в сетях.
18. Методы взлома компьютерных систем: атаки на уровне операционных систем, атаки на уровне программного обеспечения, атаки на уровне систем управления базами данных.
19. Парольная защита операционных систем. Парольные взломщики.
20. Понятие угрозы. Анализ угроз информационной безопасности. Виды «нарушителей».
21. Структуризация методов обеспечения информационной безопасности. Основные методы реализации угроз информационной безопасности.
22. Основные принципы обеспечения информационной безопасности в автоматизированной системе.
23. Причины, виды и каналы утечки информации.
24. Методы построения защищенных автоматизированных систем.
25. Политика безопасности. Основные типы политики безопасности.
26. Политика безопасности. Модели безопасности.
27. Стандарты информационной безопасности.

28. Правовое обеспечение защиты информации. Нормативные документы.
29. Разрушающие программные воздействия: вирусы и закладки. Антивирусные средства.
30. Психологические аспекты информационной безопасности организации.

Примерный перечень практических заданий для экзамена:

1. Создание шифрованных пользовательских виртуальных дисков.
2. Анализ программных средств криптографической защиты информации.
3. Анализ программно-аппаратных средств усиленной аутентификации
4. Методы и средства привязки программного обеспечения к аппаратному окружению и физическим носителям
5. Настройка политики безопасности операционной системы.
6. Анализ защищенности изолированной программной среды.
7. Исследование систем идентификации.
8. Обзор средств построения виртуальных частных сетей.
9. Изучение средств межсетевого экранирования
10. Исследование технологий доверенной загрузки операционной системы
11. Методы сокрытия программных закладок.
12. Средства идентификации и аутентификации объектов баз данных, управление доступом
13. Средства контроля целостности информации, организация аудита
14. Типы контроля безопасности: потоковый, контроль вывода, контроль доступа.
15. Использование програмных средств для изолирования действий пользователей

Критерии оценивания экзамена

Оценка «2» ставится, если правильно выполнено менее 1 задания экзаменационной работы. Оценка «3» ставится за правильное выполнение 1 задания экзаменационной работы.
Оценка «4» ставится за правильное выполнение 2 задания экзаменационной работы.
Оценка «5» ставится за правильное выполнение всех заданий экзаменационной работы.