Краевое государственное бюджетное профессиональное образовательное учреждение
«Приморский индустриальный колледж»

СОГЛАСОВАНО
Руководитель МО
профессиональных
дисциплин
_____И.В. Мироненко
«08» 06 2020 г.

УТВЕРЖДАЮ
Зам. директора по УПР
_____Е.Н. Золотарева
«09» июня 2020 г.

КОМПЛЕКТ КОНТРОЛЬНО-ОЦЕНОЧНЫХ СРЕДСТВ
для оценки результатов освоения профессиональной дисциплины

ОП. 14 ЗАЩИТА ИНФОРМАЦИИ

Программа подготовки специалистов среднего звена
по специальности среднего профессионального образования технологического профиля
09.02.04 Информационные системы (по отраслям)

г. Арсеньев

Комплекс контрольно-оценочных средств по дисциплине ОП. 14 Защита информации разработан на основе Федерального государственного образовательного стандарта (далее – ФГОС) среднего профессионального образования (далее СПО) по специальности 09.02.04. Информационные системы (по отраслям), утвержденного приказом Министерства образования и науки Российской Федерации от 14 мая 2014 г. № 525, рабочей программы учебной дисциплины.

Комплекс контрольно - оценочных средств предназначен для определения качества освоения обучающимися учебного материала, является частью программы подготовки специалистов среднего звена (ППССЗ) в целом и учебно-методического комплекса (УМК) дисциплины.

Разработчик: А.Ю. Сережкина, преподаватель общепрофессиональных и профессиональных дисциплин технологического профиля.

1. ПАСПОРТ КОНТРОЛЬНО-ОЦЕНОЧНЫХ СРЕДСТВ УЧЕБНОЙ ДИСЦИПЛИНЫ

Контрольно-оценочные средства (КОС) предназначены для контроля и оценки образовательных достижений обучающихся, освоивших программу учебной дисциплины ОП.14 «Защита информации» по специальности 09.02.04 «Информационные системы (по отраслям)».

Контрольно-оценочные средства включают контрольные материалы для проведения текущего, рубежного контроля и итоговой аттестации в форме дифференцированного зачета.

Контрольно-оценочные средства разработаны:

1. На основе Федерального государственного образовательного стандарта специальности среднего профессионального образования 09.04.02 Информационные системы (по отраслям)
2. в соответствии с основной профессиональной образовательной программой по специальности среднего профессионального образования 09.04.02 Информационные системы (по отраслям) и программы учебной дисциплины ОП. 14 «Защита информации»

В результате освоения учебной дисциплины обучающийся должен:

уметь:

- применять организационно-правовые методы защиты информации в информационных системах;
- обеспечивать антивирусную защиту информации;
- использовать криптостойкие алгоритмы защиты данных;
- выполнять аутентификацию информации.

знать:

• сущность информационной безопасности информационных систем;

• состав и методы организационно-правовой защиты информации;

• источники возникновения информационных угроз;

• методы антивирусной защиты информации;

• алгоритмы традиционных методов шифрования данных;

• современные методы криптозащиты информации;

• протоколы идентификации и проверки подлинности пользователя;

• процедуры аутентификации данных и постановки электронной цифровой подписи.

В результате изучения учебной дисциплины «Защита информации» формируются следующие компетенции:

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, необходимой для 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 повышение квалификации.

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

Техник по информационным системам должен обладать профессиональными компетенциями, соответствующими видам деятельности:

ПК 1.1. Собирать данные для анализа использования и функционирования информационной системы, участвовать в составлении отчетной документации, принимать участие в разработке проектной документации на модификацию информационной системы.

ПК 1.5 Разрабатывать фрагменты документации по эксплуатации информационной системы.

ПК 1.10 Обеспечивать организацию доступа пользователей информационной системы в рамках своей компетенции.

ПК 2.6 Использовать критерии оценки качества и надёжности функционирования информационной системы.

Процесс изучения дисциплины направлен на формирование личностных результатов реализации программы воспитания:

ЛР 1. Осознающий себя гражданином и защитником великой страны.

ЛР 2. Проявляющий активную гражданскую позицию, демонстрирующий приверженность принципам честности, порядочности, открытости, экономически активный

и участвующий в студенческом и территориальном самоуправлении, в том числе на условиях добровольчества, продуктивно взаимодействующий и участвующий в деятельности общественных организаций.

ЛР 3. Соблюдающий нормы правопорядка, следующий идеалам гражданского общества, обеспечения безопасности, прав и свобод граждан России. Лояльный к установкам и проявлениям представителей субкультур, отличающий их от групп с деструктивным и девиантным поведением. Демонстрирующий неприятие и предупреждающий социально опасное поведение окружающих.

ЛР 4. Проявляющий и демонстрирующий уважение к людям труда, осознающий ценность собственного труда. Стремящийся к формированию в сетевой среде личностно и профессионального конструктивного «цифрового следа».

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 6. Проявляющий уважение к людям старшего поколения и готовность к участию в социальной поддержке и волонтерских движениях.

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

ЛР 8. Проявляющий и демонстрирующий уважение к представителям различных этнокультурных, социальных, конфессиональных и иных групп. Сопричастный к сохранению, преумножению и трансляции культурных традиций и ценностей многонационального российского государства.

ЛР 9. Соблюдающий и пропагандирующий правила здорового и безопасного образа жизни, спорта; предупреждающий либо преодолевающий зависимости от алкоголя, табака, психоактивных веществ, азартных игр и т.д. Сохраняющий психологическую устойчивость в ситуативно сложных или стремительно меняющихся ситуациях.

ЛР 10. Заботящийся о защите окружающей среды, собственной и чужой безопасности, в том числе цифровой.

ЛР 11. Проявляющий уважение к эстетическим ценностям, обладающий основами эстетической культуры.

ЛР 12. Принимающий семейные ценности, готовый к созданию семьи и воспитанию детей; демонстрирующий неприятие насилия в семье, ухода от родительской ответственности, отказа от отношений со своими детьми и их финансового содержания.

Личностные результаты реализации программы воспитания, определенные отраслевыми требованиями к деловым качествам личности:

ЛР 13. Демонстрирующий умение эффективно взаимодействовать в команде, вести диалог, в том числе с использованием средств коммуникации.

ЛР 14. Демонстрирующий навыки анализа и интерпретации информации из различных источников с учетом нормативно-правовых норм.

ЛР 15. Демонстрирующий готовность и способность к образованию, в том числе самообразованию, на протяжении всей жизни; сознательное отношение к непрерывному образованию как условию успешной профессиональной и общественной деятельности.

2. ОСНОВНЫЕ ПОКАЗАТЕЛИ ОЦЕНКИ РЕЗУЛЬТАТОВ

Результаты обучения (освоенные умения, усвоенные знания)	**Основные показатели оценки результата**	**Формы и методы контроля и оценки результатов обучения**
Умения: • применять организационно-правовые методы защиты информации в информационных системах; • обеспечивать антивирусную защиту информации; • использовать криптостойкие алгоритмы защиты данных; • выполнять аутентификацию информации.	умение применять организационно-правовые методы защиты информации в информационных системах; обеспечение антивирусной защиты информации; использование криптостойких алгоритмов защиты данных; выполнение аутентификации информации.	практические занятия
Знания: • сущность информационной безопасности информационных систем; • состав и методы организационно-правовой защиты информации; • источники возникновения информационных угроз; • методы антивирусной защиты информации; • алгоритмы традиционных методов шифрования данных; • современные методы криптозащиты информации; • протоколы идентификации и проверки подлинности пользователя; • процедуры аутентификации данных и постановки электронной цифровой подписи.	Понимание сущности информационной безопасности информационных систем; Знание состава и методов организационно-правовой защиты информации; Определение источников возникновения информационных угроз; Знание методов антивирусной защиты информации, алгоритмов традиционных методов шифрования данных, современных методов криптозащиты информации,	тест, устный опрос, внеаудиторная самостоятельная работа, дифференцированный зачёт

	протоколов идентификации и проверки подлинности пользователя, а также процедуры аутентификации данных и постановки электронной цифровой подписи	

Результаты (освоенные общие компетенции)	**Основные показатели оценки результата**	**Формы и методы контроля и оценки**
ОК 1 Понимать сущность и социальную значимость своей будущей профессии, проявлять к ней устойчивый интерес	– демонстрация интереса к будущей профессии	Интерпретация результатов наблюдений за деятельностью обучающегося в процессе освоения учебной дисциплины
ОК 2 Организовывать собственную деятельность, выбирать типовые методы и способы выполнения профессиональных задач, оценивать их эффективность и качество	– выбор и применение методов и способов решения профессиональных задач в области информационных систем; – оценка эффективности и качества выполнения профессиональных задач;	
ОК 3 Принимать решения в стандартных и нестандартных ситуациях и нести за них ответственность	– решение стандартных и нестандартных профессиональных задач в области информационных систем;	
ОК 4 Осуществлять поиск и использование информации, необходимой для эффективного выполнения профессиональных задач, профессионального и личностного развития	– использование различных источников для поиска информации, включая электронные; – использование найденной информации для эффективного выполнения профессиональных задач;	
ОК 5 Использовать информационно-коммуникационные технологии в профессиональной деятельности	– использование информационно-коммуникационных технологий в области информационных систем;	

ОК 6 Работать в коллективе и команде, эффективно общаться с коллегами, руководством, потребителями	– взаимодействие с обучающимися, преподавателями и мастерами в ходе обучения;	
ОК 7 Брать на себя ответственность за работу членов команды (подчиненных), за результат выполнения заданий	– самоанализ и коррекция результатов собственной работы и работы членов команды (подчиненных);	
ОК 8 Самостоятельно определять задачи профессионального и личностного развития, заниматься самообразованием, осознанно планировать повышение квалификации	– организация самостоятельных занятий при изучении дисциплины; – осознанное планирование повышения квалификации; – получение знаний, умений и навыков вне учебного заведения;	
ОК 9 Ориентироваться в условиях частой смены технологий в профессиональной деятельности	- анализ инноваций в области информационных систем в организациях (подразделениях) различных сфер деятельности.	

3. ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ДЛЯ АТТЕСТАЦИИ ПО УЧЕБНОЙ ДИСЦИПЛИНЕ

3.1 Вопросы для устного опроса по темам

Устный опрос №1

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

Устный опрос №2

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

Устный опрос №3

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?

3.2 Тестирование

Тест №1
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.

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 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.

Тест №3
Инструкция: выберите один правильный ответ
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.

Тест №4
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 неё.

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.

Тест №5
Инструкция: выберите один правильный ответ
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 взарубежных 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.

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 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.

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 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.

Тест №8
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.

Критерии оценки для проведения экзамена по дисциплине

Оценка «отлично» выставляется, если:

- полно раскрыто содержание вопросов в объеме программы и рекомендованной литературы;

- четко и правильно даны определения и раскрыто содержание концептуальных понятий, закономерностей, корректно использованы научные термины;
- для доказательства использованы различные теоретические знания, выводы из наблюдений и опытов;
- ответ самостоятельный, исчерпывающий, без наводящих дополнительных вопросов, с опорой на знания, приобретенные в процессе изучения дисциплины;
- полное соответствие отчета на экзамене требованиям стандарта.

Оценка «хорошо»:

- раскрыто основное содержание вопросов;
- в основном правильно даны определения понятий и использованы научные термины;
- ответ самостоятельный;
- определения понятий неполные, допущены нарушения последовательности изложения, небольшие неточности при использовании научных терминов или в выводах и обобщениях;
- незначительные отклонения в оформлении отчета на экзамене.

Оценка «удовлетворительно»:

- усвоено основное содержание учебного материала, но изложено фрагментарно, не всегда последовательно;
- определение понятий недостаточно четкое;
- не использованы в качестве доказательства выводы из наблюдений и опытов или допущены ошибки при их изложении;
- допущены ошибки и неточности в использовании научной терминологии, определении понятий;
- имеются значительные отклонения в оформлении отчета на экзамене.

Оценка «неудовлетворительно»:

- ответ неправильный, не раскрыто основное содержание программного материала;
- допущены грубые ошибки в определении понятий, при использовании терминологии;

- оформление отчета на экзамене полностью не удовлетворяет требованиям стандарта.