Министерство образования, науки и молодежной политики
Краснодарского края
Государственное бюджетное профессиональное образовательное учреждение
Краснодарского края «Пашковский сельскохозяйственный колледж»

УТВЕРЖДАЮ
Зам директора по УМР
_____Е.П. Ольховская
«28» 09 2022 г

Комплект контрольно-оценочных средств
для проведения текущей промежуточной аттестации студентов в рамках основной профессиональной образовательной программы
по учебной дисциплине
ЭК.1 Введение в специальность

Специальность 10.02.05 Обеспечение информационной безопасности автоматизированных систем

г. Краснодар, 2022

Комплект контрольно-оценочных средств разработан на основе рабочей программы ЭК.1 Введение в специальность, требованиями ФГОС СПО по специальности 10.02.05 Обеспечение информационной безопасности автоматизированных систем, приказ Минобрнауки России от 09.12.2016.г. №1553, зарегистрировано в Минюсте России 26.121.2016 г., № 44938 (ред. 17.12.2020 г.), с учетом:

– Федерального государственного образовательного стандарта среднего общего образования (далее – ФГОС СОО) (утвержден приказом Министерства образования и науки РФ от 17.05.2012 № 413);

– Рекомендаций по организации получения среднего общего образования в пределах освоения образовательных программ среднего профессионального образования на базе основного общего образования с учетом требований федеральных государственных образовательных стандартов и получаемой профессии или специальности среднего профессионального образования (письмо Департамента государственной политики в сфере подготовки рабочих кадров и ДПО Минобрнауки России от 17.03.2015 № 06-259);

– Концепции преподавания общеобразовательных дисциплин с учетом профессиональной направленности программ среднего профессионального образования, реализуемых на базе основного общего образования, утвержденной распоряжением Министерства просвещения Российской Федерации от 30 апреля 2021 г. № Р-98.

Организация разработчик: ГБПОУ КК ПСХК

Разработчик:

Пушкарева Н.Я.	Преподаватель компьютерных дисциплин ГБПОУ КК ПСХК, высшая квалификационная категория, математик, преподаватель информатики и ИКТ

Рассмотрен на заседании методического объединения информационных технологий
Протокол № 1 от « 28 » сент 2022 г.
_____/Пушкарева Н.Я.

СОДЕРЖАНИЕ

1. Паспорт комплекта контрольно-оценочных средств

В результате освоения учебной дисциплины ЭК.1 Введение в специальность обучающийся должен обладать планируемыми результатами освоения дисциплины при формировании и развитии общих компетенций по специальности 10.02.05 Обеспечение информационной безопасности автоматизированных систем:

ОК1	Выбирать способы решения задач профессиональной деятельности, применительно к различным контекстам
ОК2	Осуществлять поиск, анализ и интерпретацию информации, необходимой для выполнения задач профессиональной деятельности
ОК3	Планировать и реализовывать собственное профессиональное и личностное развитие
ОК4	Работать в коллективе и команде, эффективно взаимодействовать с коллегами, руководством, клиентами
ОК5	Осуществлять устную и письменную коммуникацию на государственном языке с учетом особенностей социального и культурного контекста
ОК6	Проявлять гражданско-патриотическую позицию, демонстрировать осознанное поведение на основе традиционных общечеловеческих ценностей
ОК7	Содействовать сохранению окружающей среды, ресурсосбережению, эффективно действовать в чрезвычайных ситуациях
ОК8	Использовать средства физической культуры для сохранения и укрепления здоровья в процессе профессиональной деятельности и поддержание необходимого уровня физической подготовленности
ОК9	Использовать информационные технологии в профессиональной деятельности
ОК10	Пользоваться профессиональной документацией на государственном и иностранном языках

В рамках программы учебной дисциплины обучающимися должны быть освоены личностные (ЛР), метапредметные (МР) и предметные результаты базового углубленного уровней (ПРб) и (ПРу) в соответствии с требованиями ФГОС среднего общего образования:

Коды	**Планируемые результаты освоения дисциплины**
ЛР 01	сформированность основ саморазвития и самовоспитания в соответствии с общечеловеческими ценностями и идеалами гражданского общества; готовность и способность к самостоятельной, творческой и ответственной деятельности;
ЛР 02	толерантное сознание и поведение в поликультурном мире, готовность и способность вести диалог с другими людьми, достигать в нем взаимопонимания, находить общие цели и сотрудничать для их достижения, способность противостоять идеологии экстремизма, национализма, ксенофобии, дискриминации по социальным, религиозным, расовым, национальным признакам и другим негативным социальным явлениям;

ЛР 03	навыки сотрудничества со сверстниками, детьми младшего возраста, взрослыми в образовательной, общественно полезной, учебно-исследовательской, проектной и других видах деятельности;
ЛР 04	нравственное сознание и поведение на основе усвоения общечеловеческих ценностей;
ЛР 05	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;
ЛР 06	эстетическое отношение к миру, включая эстетику быта, научного и технического творчества, спорта, общественных отношений;
ЛР 07	осознанный выбор будущей профессии и возможностей реализации собственных жизненных планов; отношение к профессиональной деятельности как возможности участия в решении личных, общественных, государственных, общенациональных проблем.
МР 01	умение самостоятельно определять цели деятельности и составлять планы деятельности; самостоятельно осуществлять, контролировать и корректировать деятельность; использовать все возможные ресурсы для достижения поставленных целей и реализации планов деятельности; выбирать успешные стратегии в различных ситуациях;
МР 02	умение продуктивно общаться и взаимодействовать в процессе совместной деятельности, учитывать позиции других участников деятельности, эффективно разрешать конфликты;
МР 03	владение навыками познавательной, учебно-исследовательской и проектной деятельности, навыками разрешения проблем; способность и готовность к самостоятельному поиску методов решения практических задач, применению различных методов познания;
МР 04	готовность и способность к самостоятельной информационно-познавательной деятельности, владение навыками получения необходимой информации из словарей разных типов, умение ориентироваться в различных источниках информации, критически оценивать и интерпретировать информацию, получаемую из различных источников;
МР 05	умение использовать средства информационных и коммуникационных технологий (далее – ИКТ) в решении когнитивных, коммуникативных и организационных задач с соблюдением требований эргономики, техники безопасности, гигиены, ресурсосбережения, правовых и этических норм, норм информационной безопасности;
МР 07	умение самостоятельно оценивать и принимать решения, определяющие стратегию поведения, с учетом гражданских и нравственных ценностей;
МР 08	владение языковыми средствами – умение ясно, логично и точно излагать свою точку зрения, использовать адекватные языковые средства;
МР 09	владение навыками познавательной рефлексии как осознания совершаемых действий и мыслительных процессов, их результатов и оснований, границ своего знания и незнания, новых познавательных задач и средств их достижения.

ПРб 01	сформированность представлений о роли информации и связанных с ней процессов в окружающем мире;
ПРб 02	наличие представлений о компьютерных сетях и их роли в современном мире; об общих принципах разработки и функционирования интернет-приложений;
ПРб 03	понимание угроз информационной безопасности, использование методов и средств противодействия этим угрозам, соблюдение мер безопасности, предотвращающих незаконное распространение персональных данных; соблюдение требований техники безопасности и гигиены при работе с компьютерами и другими компонентами цифрового окружения; понимание правовых основ использования компьютерных программ, баз данных и работы в сети Интернет;
ПРб 04	понимание основных принципов дискретизации различных видов информации; умение определять информационный объем текстовых, графических и звуковых данных при заданных параметрах дискретизации;
ПРб 05	умение организовывать личное информационное пространство с использованием различных средств цифровых технологий; понимание возможностей цифровых сервисов государственных услуг, цифровых образовательных сервисов; понимание возможностей и ограничений технологий искусственного интеллекта в различных областях; наличие представлений об использовании информационных технологий в различных профессиональных сферах.
ПРу 01	наличие представлений о базовых принципах организации и функционирования компьютерных сетей;

Формой аттестации по учебной дисциплине является *дифференцированный зачет.*

2. Результаты освоения учебной дисциплины, подлежащие проверке

2.1. В результате аттестации по учебной дисциплине осуществляется комплексная проверка следующих умений и знаний, а также динамика формирования общих компетенций:

Результаты обучения: умения, знания и общие компетенции	**Показатели оценки результата**	**Форма контроля и оценивания**
Знать:		
ОК03. Планировать и реализовывать собственное профессиональное и личностное развитие	Объясняет сущность деятельности в рамках своей специальности. Воспроизводит оценки социальной значимости своей будущей профессии / специальности и объясняет основания для этих оценок.	Оформление понятийного словаря. Проверка опорных конспектов. Устный опрос
ОК05. Осуществлять устную и письменную коммуникацию	Оценивает стандартный продукт письменной	Оформление понятийного словаря.

на государственном языке с учетом особенностей социального и культурного контекста.	коммуникации простой и сложной структуры. Оценивает созданный продукт письменной коммуникации сложной структуры, содержащий сопоставление позиций и / или аргументацию за и против предъявленной для обсуждения позиции.	Проверка опорных конспектов. Тестирование
ОК06. Проявлять гражданско-патриотическую позицию, демонстрировать осознанное поведение на основе традиционных общечеловеческих ценностей	Оценивает значимость своей профессии, сущность гражданско-патриотической позиции, общечеловеческих ценностей. Соблюдает правила поведения в ходе выполнения профессиональной деятельности	Письменный контроль (тестирование) Таблица соответствия информации её свойствам.
ОК07. Содействовать сохранению окружающей среды, ресурсосбережению, эффективно действовать в чрезвычайных ситуациях	Знает правила экологической безопасности при ведении профессиональной деятельности; основные ресурсы, задействованные в профессиональной деятельности; пути обеспечения ресурсосбережения**.**	Оформление понятийного словаря. Проверка опорных конспектов. Тестирование
ОК10. Пользоваться профессиональной документацией на государственном и иностранном языках	Знает правила построения простых и сложных предложений на профессиональные темы; основные общеупотребительные глаголы (бытовая и профессиональная лексика); лексический минимум, относящийся к описанию предметов, средств и процессов профессиональной деятельности; особенности произношения; правила чтения текстов	Оформление понятийного словаря. Письменный контроль (тестирование) Таблица соответствия информации её свойствам. Проверка опорных конспектов. Тестирование

	профессиональной направленности.	
Уметь:		
ОК01. Выбирать способы решения задач профессиональной деятельности, применительно к различным контекстам	Распознает задачу и/или проблему в профессиональном и/или социальном контексте. Планирует деятельность по решению задачи в рамках известных технологий, в том числе выделяя отдельные составляющие технологии. Разбивает поставленную цель на задачи, подбирая из числа известных технологии (элементы технологий), позволяющие решить каждую из задач. Оценивает результат и последствия своих действий.	Оформление понятийного словаря. Проверка опорных конспектов, отчетов по решению задач. Тестирование.
ОК02. Осуществлять поиск, анализ и интерпретацию информации, необходимой для выполнения задач профессиональной деятельности	Определяет задачи поиска информации. Определяет необходимые источники информации. Планирует процесс поиска. Структурирует получаемую информацию; выделяет наиболее значимое в перечне информации. Оценивает практическую значимость результатов поиска. Оформляет результаты поиска.	Проверка опорных конспектов, отчетов по решению типовых ситуационных задач. Тестирование.
ОК04. Работать в коллективе и команде, эффективно взаимодействовать с коллегами, руководством, клиентами	Участвует в групповом обсуждении, высказываясь в соответствии с заданной процедурой и по заданному вопросу. Аргументировано отвергает или принимает идеи других участников группового обсуждения. Договаривается о процедуре и вопросах для обсуждения	Тестирование Поверка подготовленных самостоятельных сообщений по теме. Составление сравнительной таблицы.

	в группе в соответствии с поставленной целью деятельности команды (группы).	
ОК08. Использовать средства физической культуры для сохранения и укрепления здоровья в процессе профессиональной деятельности и поддержание необходимого уровня физической подготовленности	Использует физкультурно-оздоровительную деятельность для укрепления здоровья, достижения жизненных и профессиональных целей; применяет рациональные приемы двигательных функций в профессиональной деятельности; пользуется средствами профилактики перенапряжения характерными для данной специальности	Оформление понятийного словаря. Блиц-опрос Письменный контроль (тестирование)
ОК09. Использовать информационные технологии в профессиональной деятельности	Применяет средства информационных технологий для решения профессиональных задач; использовать современное программное обеспечение	

3. Оценка освоения учебной дисциплины:

3.1. Формы и методы оценивания

Предметом оценки дисциплины ЭК.1 Введение в специальность по специальности 10.02.05 Обеспечение информационной безопасности автоматизированных систем, предусмотренные с учетом:

− Федерального государственного образовательного стандарта среднего профессионального образования по специальности 10.02.05 Обеспечение информационной безопасности автоматизированных систем (приказ Минобрнауки России от 09.12.2016.г. №1553, зарегистрировано в Минюсте России 26.121.2016 г., № 44938 (ред. 17.12.2020 г.);

− Федерального государственного образовательного стандарта среднего общего образования (далее – ФГОС СОО) (утвержден приказом Министерства образования и науки РФ от 17.05.2012 № 413);

– Рекомендаций по организации получения среднего общего образования в пределах освоения образовательных программ среднего профессионального образования на базе основного общего образования с учетом требований

федеральных государственных образовательных стандартов и получаемой профессии или специальности среднего профессионального образования (письмо Департамента государственной политики в сфере подготовки рабочих кадров и ДПО Минобрнауки России от 17.03.2015 № 06-259);

– Концепции преподавания общеобразовательных дисциплин с учетом профессиональной направленности программ среднего профессионального образования, реализуемых на базе основного общего образования, утвержденной распоряжением Министерства просвещения Российской Федерации от 30 апреля 2021 г. № Р-98, по специальности 10.02.05 Обеспечение информационной безопасности автоматизированных систем базового уровня подготовки, направленные на формирование общих и профессиональных компетенций.

Типы (виды) заданий для текущего контроля

№	Тип (вид) задания	Проверяемые знания и умения	Критерии оценки
1	Тесты	Знание основ дисциплины Введение в специальность в соответствии с темой занятия	«5» - 100 – 90% правильных ответов «4» - 89 - 75% правильных ответов «3» - 74 – 55% правильных ответов «2» - 54% и менее правильных ответов
2	Устные ответы	Знание основ дисциплины Введение в специальность в соответствии с темой занятия	Устные ответа на вопросы должны соответствовать учебному материалу, изученному на уроке
3	Проверка конспектов (рефератов, докладов, сообщений, понятийных словарей, таблиц соответствия)	Умение ориентироваться в информационном пространстве, составлять конспект. Знание правил оформления рефератов,	Соответствие содержания работы, заявленной теме, правилам оформления работы.

		творческих работ.	
4	Дифференцированный зачет	Знание основ дисциплины Введение в специальность и умение применять их при решении задач	Устные ответы и демонстрация практических умений работы на компьютере в соответствии с темой занятия: «5» - 100 – 90% правильных ответов и заданий «4» - 89 - 80% правильных ответов и заданий «3» - 79 – 70% правильных ответов и заданий «2» - 69% и менее правильных ответов и заданий

Промежуточный контроль по результатам освоения обучающимися учебной дисциплины проводится в форме дифференцированных зачётов (зачёт с оценкой).

Дифференцированный зачёт проводится в форме выполнения тестового задания.

3.2. Типовые задания для оценки освоения учебной дисциплины

Раздел 1. Нормативно-правовое обеспечение образовательного процесса в образовательных организациях среднего профессионального образования

Тема 1.1. Федеральный государственный образовательный стандарт специальности среднего профессионального образования (ФГОС СПО) по специальности 10.02.05 Обеспечение информационной безопасности автоматизированных систем как совокупность требований к образованию по специальности: форма освоения, нормативный срок обучения, квалификация и профессиональная компетентность специалиста; характеристика общих и профессиональных компетенций студента по специальности среднего профессионального образования.

Учебные дисциплины специальности 10.02.05 Обеспечение информационной безопасности автоматизированных систем как процесс формирования общих

и профессиональных компетенций в процессе обучения; понимание сущности и социальной значимости своей будущей профессии и проявление к ней устойчивого интереса в процессе обучения; престижность и спрос на специальность; возможность трудоустройства и продолжения образования.

Блок заданий 1. Примерный перечень вопросов для устного и письменного опроса по теме:

1. Форма освоения, нормативный срок обучения, квалификация и профессиональная компетентность специалиста по специальности 10.02.05 Обеспечение информационной безопасности автоматизированных систем.
2. Характеристика общих и профессиональных компетенций студента по специальности среднего профессионального образования.
3. Область профессиональной деятельности выпускников.

Блок заданий 2. Самостоятельная работа обучающихся

Самостоятельная работа с научной и специальной литературой, с Интернет-ресурсами, ответы на контрольные вопросы, подготовка самостоятельных сообщений, рефератов по теме:

1. Исторические этапы формирования и развития специальности.
2. Общие требования к профессиональным знаниям, навыкам и опыту.

Тема 1.2. Закон «Об образовании в Российской Федерации» как нормативно-правовая основа образовательного процесса в системе среднего профессионального образования.

Сайт колледжа как инструмент реализации государственной политики в сфере образования, элемент единой информационно-образовательной среды. Структура сайта.

Блок заданий 1. Письменный опрос на тему: Правила внутреннего распорядка.

Вопросы:

1. Как студент обязан обращаться со студенческим билетом?
2. Студент заболел, каковы его действия и в какие сроки?
3. Порядок действий при необходимости пропустить занятия по уважительной причине
4. Какова форма и стиль одежды студента?
5. В какой одежде запрещено находиться студенту в колледже?
6. Что запрещается студентам приносить, передавать, использовать в колледже и на его территории?
7. Меры дисциплинарного воздействия за систематическую неуспеваемость, нарушение учебной дисциплины, правил внутреннего распорядка и

Устава колледжа к студентам

Ответы:

1. Как студент обязан обращаться со студенческим билетом?
   Постоянно иметь при себе, бережно хранить и не передавать другим лицам
2. Студент заболел, каковы его действия и в какие сроки?
   В трехдневный срок проинформировать классного руководителя и предоставить справку из лечебного учреждения
3. Порядок действий при необходимости пропустить занятия по уважительной причине
   Написать заявление, согласовать с классным руководителем и подписать у зав. отделением
4. Какова форма и стиль одежды студента?
   Свободная, деловой стиль
5. В какой одежде запрещено находиться студенту в колледже?
   В спортивной одежде, в шортах, в пляжной обуви
6. Что запрещается студентам приносить, передавать, использовать в колледже и на его территории?
   оружие, спиртные напитки, табачные изделия, жевательную резинку, токсические и наркотические вещества и иные предметы и вещества, способные причинить вред здоровью участников образовательных отношений и (или) деморализовать образовательный процесс; любые предметы и вещества, могущие привести к взрывам, возгораниям и отравлению
7. Меры дисциплинарного воздействия за систематическую неуспеваемость, нарушение учебной дисциплины, правил внутреннего распорядка и Устава колледжа к студентам
   Замечание, выговор, отчисление

Блок заданий 2. Письменный опрос на тему: Режим телефона во время учебных занятий. (Инструкция: тип вопроса - выбор единственно правильного ответа или множественный выбор)

Вопросы:

1. Режим телефона во время учебных, практических и внеучебных мероприятий
2. Местонахождение мобильного телефона и других портативных электронных устройств во время учебных, практических и внеучебных мероприятий

3. На перемене допускается пользование телефоном только как …
4. На занятиях физической культуры где должен находиться телефон?
5. На ком лежит ответственность за сохранность телефона?
6. Студент на занятиях использует телефон как калькулятор, как записную книжку, словарь иностранных слов, видеокамеру, видеоплеер, диктофон, игру и т.д. Когда это запрещено?
7. Как родители могут передать детям сообщения в случае форс-мажорных обстоятельствах во время учебных занятий?

Ответы:

1. Режим телефона во время учебных, практических и внеучебных мероприятий – **беззвучный или выключенный**
2. Местонахождение мобильного телефона и других портативных электронных устройств во время учебных, практических и внеучебных мероприятий – **убрать со стола в сумку, карман, портфель**
3. На перемене допускается пользование телефоном только как … - **средством связи**
4. На занятиях физической культуры где должен находиться телефон? – **складываются в место, отведенное преподавателем**
5. На ком лежит ответственность за сохранность телефона? – **только на его владельце (родителях, законных представителях владельца)**
6. Студент на занятиях использует телефон как калькулятор, как записную книжку, словарь иностранных слов, видеокамеру, видеоплеер, диктофон, игру и т.д. Когда это запрещено? – **использовать без разрешения преподавателя**
7. Как родители могут передать детям сообщения в случае форс-мажорных обстоятельствах во время учебных занятий? - **через секретаря учебной части, приемную директора, классного руководителя**

Блок заданий 3. Самостоятельная работа обучающихся

Самостоятельная работа с научной и специальной литературой, с Интернет-ресурсами, ответы на контрольные вопросы, подготовка самостоятельных сообщений, рефератов по теме:

1. Стандарты компетенций и движения Молодые профессионалы.
2. Демонстрационный экзамен.
3. Организация и проведение демонстрационного экзамена.

Тема 1.3. Специальность 10.02.05 Обеспечение информационной безопасности автоматизированных систем. Квалификация по специальности.

Объекты профессиональной деятельности. Область профессиональной деятельности. Виды профессиональной деятельности техника по защите информации.

Блок заданий 1. Примерный перечень вопросов для устного и письменного опроса по теме:

1. Объекты профессиональной деятельности.
2. Обязанности техника по защите информации. Виды профессиональной деятельности.
3. Область профессиональной деятельности выпускников.

Блок заданий 2. Устный опрос по теме.

Вопросы:

1. Назовите наименование квалификации по специальности? Чем занимается этот специалист на предприятии?
2. Назовите объекты профессиональной деятельности.
3. Назовите обязанности техника по защите информации.
4. Назовите виды деятельности техника по защите информации.

Ответы:

1. **Наименование квалификации -Техник по защите информации**
   Техник по защите информации - это специалист, который занимается обеспечением информационной безопасности предприятия и его информационной инфраструктуры, техническим обслуживанием средств защиты информации.
   Техники по защите информации проводят информационное обследование и анализ, разрабатывают правовые документы, которые максимально упорядочивают информационные потоки.
   Специалист устанавливает и настраивает средства и механизмы защиты, а также поддерживает, обновляет, модернизирует созданную систему безопасности.
2. Объекты информатизации.
   Средства защиты информации.
   Документация.
   Первичные трудовые коллективы
3.

- участие в работе по обеспечению информационной безопасности предприятия, соблюдению охраняемой законом тайны (государственной, служебной, коммерческой);
- проверка технического состояния, установка, наладка и регулировка аппаратуры и приборов, их профилактические осмотры и текущий ремонт;

- эксплуатация средств защиты и контроля информации;
- ведение учета работ и объектов, подлежащих защите, установленных технических средств, журналов нарушений их работы, справочников подготовка технических средств для проведения всех видов плановых и внеплановых контрольных проверок, аттестации оборудования, а также в случае необходимости к сдаче в ремонт;
- работа по оформлению протоколов специальных измерений и другой технической документации, в том числе отчетной, связанной с эксплуатацией средств и контролем информации
- участие в планировании и организации работ по обеспечению защиты объекта;
- организация и технология работы с конфиденциальными документами;
- работа с различными системами электронного документооборота;
- применение программно-аппаратных и технических средств защиты информации;
- участие в организации комплексной системы защиты объекта;
- выполнение работ по одной или нескольким профессиям рабочих, должностям служащих

Блок заданий 3. Самостоятельная работа обучающихся

Самостоятельная работа с научной и специальной литературой, с Интернет-ресурсами, ответы на контрольные вопросы, подготовка самостоятельных сообщений, рефератов по теме:

1. Общая характеристика специальности.
2. Требования, предъявляемые к специалистам.

Профессионально ориентированное обучение

Раздел 2. Общие вопросы информационной безопасности и защиты информации

Тема 2.1. Информационная безопасность – основные понятия и определения. Современное состояние и перспективы развития защиты информации.

Блок заданий 1. Примерный перечень вопросов для устного и письменного опроса по теме:

1. Информационная безопасность – основные понятия и определения.
2. Современное состояние системы защиты информации.
3. Перспективы развития защиты информации.

Блок заданий 2. Тестовые задания по теме. (Инструкция: тип вопроса – дать письменный ответ, указать соответствие)

1. Дополните определение:

Информационная безопасность – это защита …

2. Дополните определение:

Защита информации – это комплекс …

3. Впишите варианты ответов в таблицу:

Информационные угрозы преднамеренные:						
Информационные угрозы случайные:						

а. Компьютерные вирусы
б. Отказ, сбой аппаратуры
в. Ошибки в программировании
г. Физическое воздействие на аппаратуру
д. Форс-мажорные обстоятельства
е. Хищение информации

4. Перечислите виды угроз в каждой категории (кратко, без расшифровки понятий)

Угрозы доступности:

Угрозы целостности:

Угрозы конфиденциальности:

Ответы к тесту:

1. Дополните определение:

Информационная безопасность – это защита …

целостности, доступности и конфиденциальности информации.

2. Дополните определение:

Защита информации – это комплекс …

мероприятий, направленных на обеспечение информационной безопасности.

3. Впишите варианты ответов в таблицу:

Информационные угрозы преднамеренные:	а	г	е			
Информационные угрозы случайные:	б	в	д			

ж. Компьютерные вирусы
з. Отказ, сбой аппаратуры
и. Ошибки в программировании
к. Физическое воздействие на аппаратуру
л. Форс-мажорные обстоятельства
м. Хищение информации

4. Перечислите виды угроз в каждой категории (кратко, без расшифровки понятий)

Угрозы доступности:

непреднамеренные ошибки штатных пользователей.

Повреждение или ***разрушение*** оборудования

Программные атаки на доступность:

- SYN-наводнение.
- XSS-атака.

- DDoS-атака.
- Вредоносные программы (вирусы)

Угрозы целостности

- Кражи и подлоги.
- Дублирование данных.
- Внесение дополнительных сообщений.
- Нарушение целостности программ (внедрение вредоносного кода).

Угрозы конфиденциальности

- Раскрытие паролей.
- Перехват данных.
- Кража оборудования.
- Маскарад.

Блок заданий 3. Самостоятельная работа обучающихся

Самостоятельная работа с научной и специальной литературой, с Интернет-ресурсами, ответы на контрольные вопросы, подготовка самостоятельных сообщений, рефератов по теме:

1. Понятие "информационная безопасность".
2. Проблема информационной безопасности общества.

Тема 2.2 Основы информационной безопасности. Принципы организации системы защиты, политика информационной безопасности, направления, способы и методы защиты.

Блок заданий 1. Примерный перечень вопросов для устного и письменного опроса по теме:

1. Основы информационной безопасности.
2. Принципы организации системы защиты.
3. Политика информационной безопасности.
4. Направления, способы и методы защиты.

Блок заданий 2. Самостоятельная работа обучающихся

Самостоятельная работа с научной и специальной литературой, с Интернет-ресурсами, ответы на контрольные вопросы, подготовка самостоятельных сообщений, рефератов по теме:

1. Составляющие информационной безопасности.
2. Система формирования режима информационной безопасности.
3. Задачи информационной безопасности общества.

Тема 2.3 Нормативно-правовая база информационной безопасности. Стандарты и нормативно-методические документы в области обеспечения

информационной безопасности. Государственная система обеспечения информационной безопасности.

Блок заданий 1. Примерный перечень вопросов для устного и письменного опроса по теме:

1. Нормативно-правовая база информационной безопасности
2. Стандарты и нормативно-методические документы в области обеспечения информационной безопасности.
3. Государственная система обеспечения информационной безопасности.

Блок заданий 2. Тестовые задания по теме. (Инструкция: тип вопроса - выбор единственно правильного ответа, дополнить предложение, установить соответствие)

1. Основным источником права в области обеспечения информационной безопасности в России является
   а. Уголовный кодекс
   б. Конституция
   в. государственные и отраслевые стандарты
   г. Документы Гостехкомиссии
2. Какой из типов нормативно-правовых документов регламентирует Информационную безопасность в Российской Федерации?
   а. Акты федерального законодательства
   б. Нормативно-методические документы государственных органов
   в. Стандарты информационной безопасности
3. Дополните предложение

Федеральные законы и другие нормативные акты предусматривают разделение информации на категории свободного и _____ доступа.

4. Дополните предложение

Государственная тайна относится к информации _____ доступа

5. Определение понятия "конфиденциальная информация" дано в
   а. Конституция РФ
   б. Законе "О государственной тайне"
   в. Законе "Об информации, информатизации и защите информации"
   г. УК РФ
6. Система защиты государственных секретов:
   а. основывается на Уголовном Кодексе РФ
   б. регулируется секретными нормативными документами
   в. определена Законом РФ "О государственной тайне"
7. Какие действия в Уголовном кодексе РФ классифицируются как преступления в компьютерной информационной сфере?
   а. неправомерный доступ к компьютерной информации

б. Создание, использование и распространение вредоносных программ для ЭВМ
в. умышленное нарушение правил эксплуатации ЭВМ и их сетей

8. Какой из нормативно-правовых документов определяет перечень объектов информационной безопасности личности, общества и государства и методы ее обеспечения?
а. Уголовный кодекс РФ
б. Гражданский кодекс РФ
в. Доктрина информационной безопасности РФ
г. Постановления Правительства
д. Указ Президента РФ

9. Методы обеспечения информационной безопасности делятся:
а. правовые
б. организационно-технические
в. политические
г. экономические

10. Дополните предложение:
Информация может являться объектом
_____ отношений.

11. По доступности информация классифицируется на:
а. открытую информацию и государственную тайну
б. конфиденциальную информацию и информацию свободного доступа
в. информацию с ограниченным доступом и общедоступную информацию

12. виды информации, указанные в остальных пунктах
Конфиденциальная информация это:
а. сведения, составляющие государственную тайну
б. сведения о состоянии здоровья высших должностных лиц
в. документированная информация, доступ к которой ограничивается в соответствии с законодательством РФ
д. данные о состоянии преступности в стране

13. Совокупность официальных взглядов на цели, задачи, принципы и основные направления обеспечения информационной безопасности РФ представлены в:
а. Доктрине информационной безопасности РФ
б. Концепции национальной безопасности РФ
в. ФЗ РФ "Об информации, информационных технологиях и о защите информации"

г. Конституции РФ

14. Определение понятия "конфиденциальная информация" дано в:
   а. Конституции РФ
   б. Законе "О государственной тайне"
   в. Законе "Об информации, информатизации и защите информации"
   г. УК РФ

15. Установите соответствие:

1	Органы законодательной власти (Государственная дума)
2	Органы исполнительной власти (правительство)
3	Правительство
4	Министерства и ведомства

А	разрабатывают и принимают постановления и решения, являющиеся нормативными правовыми актами
Б	издают законы, регулирующие отношения в области защиты информации
В	контролируют исполнение законов
Г	принимают соответствующие постановления в области защиты информации и издает распоряжения, являющиеся подзаконными нормативными правовыми актами

Ответы на тест на тему «Нормативно-правовая база информационной безопасности»:

1. Основным источником права в области обеспечения информационной безопасности в России является д. Уголовный кодекс е. **Конституция** ж. государственные и отраслевые стандарты з. Документы Гостехкомиссии	2. Какой из типов нормативно-правовых документов регламентирует Информационную безопасность в Российской Федерации? г. **Акты федерального законодательства** д. Нормативно-методические документы государственных органов е. Стандарты информационной безопасности
3. Дополните предложение Федеральные законы и другие нормативные акты	*4. Дополните предложение*

предусматривают разделение информации на категории свободного и _**ограниченного__** доступа.	Государственная тайна относится к информации _**ограниченного_** доступа
5. Определение понятия "конфиденциальная информация" дано в д. Конституция РФ е. Законе "О государственной тайне" ж. **Законе "Об информации, информатизации и защите информации"** з. УК РФ	6. Система защиты государственных секретов: г. основывается на Уголовном Кодексе РФ д. регулируется секретными нормативными документами е. **определена Законом РФ "О государственной тайне"**
7. Какие действия в Уголовном кодексе РФ классифицируются как преступления в компьютерной информационной сфере? а. **Неправомерный доступ к компьютерной информации** б. **Создание, использование и распространение вредоносных программ для ЭВМ** в. **Умышленное нарушение правил эксплуатации ЭВМ и их сетей**	8. Какой из нормативно-правовых документов определяет перечень объектов информационной безопасности личности, общества и государства и методы ее обеспечения? е. Уголовный кодекс РФ ж. Гражданский кодекс РФ з. **Доктрина информационной безопасности РФ** и. Постановления Правительства к. Указ Президента РФ
9. Методы обеспечения информационной безопасности делятся: а. **правовые** б. **организационно-технические** в. политические г. **экономические**	*10.Дополните предложение* Информация может являться объектом **публичных, гражданских и иных** правовых отношений.
11. По доступности информация классифицируется на: а. открытую информацию и государственную тайну	12. Конфиденциальная информация это: а. сведения, составляющие государственную тайну

б. конфиденциальную информацию и информацию свободного доступа в. **информацию с ограниченным доступом и общедоступную информацию** г. виды информации, указанные в остальных пунктах	б. сведения о состоянии здоровья высших должностных лиц в. **документированная информация, доступ к которой ограничивается в соответствии с законодательством РФ** г. данные о состоянии преступности в стране
13. Совокупность официальных взглядов на цели, задачи, принципы и основные направления обеспечения информационной безопасности РФ представлены в: а. **Доктрине информационной безопасности РФ** б. Концепции национальной безопасности РФ в. ФЗ РФ "Об информации, информационных технологиях и о защите информации" г. Конституции РФ	14. Определение понятия "конфиденциальная информация" дано в: а. Конституции РФ б. Законе "О государственной тайне" в. **Законе "Об информации, информатизации и защите информации"** г. УК РФ

15. Установите соответствие:

1	Органы законодательной власти (Государственная дума)
2	Органы исполнительной власти (правительство)
3	Правительство
4	Министерства и ведомства

А	разрабатывают и принимают постановления и решения, являющиеся нормативными правовыми актами
Б	издают законы, регулирующие отношения в области защиты информации
В	контролируют исполнение законов
Г	принимают соответствующие постановления в области защиты информации и издает распоряжения, являющиеся подзаконными нормативными правовыми актами

1	Б
2	В
3	Г
4	А

Блок заданий 3. Самостоятельная работа обучающихся

Самостоятельная работа с научной и специальной литературой, с Интернет-ресурсами, ответы на контрольные вопросы, подготовка самостоятельных сообщений, рефератов по теме:

1. Нормативно-правовые основы информационной безопасности в РФ.
2. Правовые основы информационной безопасности общества.
3. Ответственность за нарушения в сфере информационной безопасности.

Тема 2.4. Виды и особенности угроз информационной безопасности.

Блок заданий 1. Примерный перечень вопросов для устного и письменного опроса по теме:

1. Информационная безопасность
2. Основные определения и критерии классификации угроз
3. Угрозы информационной безопасности
4. Источники информационных угроз
5. Виды информационных угроз
6. Цели информационной безопасности
7. Объекты обеспечения информационной безопасности
8. Свойства угрозы информационной безопасности
9. Классификация угроз
10. Основные определения и критерии классификации угроз
11. Наиболее распространенные угрозы доступности
12. Меры при уличении сотрудника в промышленном шпионаже
13. Основные угрозы целостности
14. Основные угрозы конфиденциальности
15. Программные атаки на доступность
16. Классификация сетевых атак
17. Сетевые атаки

Блок заданий 2. Самостоятельная работа обучающихся

Самостоятельная работа с научной и специальной литературой, с Интернет-ресурсами, ответы на контрольные вопросы, подготовка самостоятельных сообщений по теме.

Тема 2.5 Защита информации. Методы защиты информации с использованием паролей, биометрические системы защиты, идентификация по отпечаткам пальцев, по характеристикам речи, по радужной оболочке глаза, по изображению лица, по ладони руки. Физическая защита данных на дисках.

Блок заданий 1. Примерный перечень вопросов для устного и письменного опроса по теме:

1. Несанкционированный доступ
2. Защита с использованием паролей
3. Биометрические системы защиты
4. Идентификация по отпечаткам пальцев
5. Идентификация по характеристикам речи
6. Идентификация по радужной оболочке глаза
7. Идентификация по изображению лица
8. Идентификация по ладони руки
9. Физическая защита данных на дисках
10. Способы реализации RAID-массива

Блок заданий 2. Самостоятельная работа обучающихся

Самостоятельная работа с научной и специальной литературой, с Интернет-ресурсами, ответы на контрольные вопросы, подготовка самостоятельных сообщений по теме.

Тема 2.6 Защита от вредоносных программ. Компьютерные вирусы и информационная безопасность. Воздействие на программно-аппаратные средства защиты информации.

Блок заданий 1. Примерный перечень вопросов для устного и письменного опроса по теме:

1. Защита от вредоносных программ
2. Признаки заражения компьютера
3. Действия при наличии признаков заражения компьютера
4. Антивирусные программы
5. Признаки заражения сетевым вирусом
6. Компьютерные вирусы и защита от них
7. Классификация вирусов по особенностям алгоритма
8. Загрузочные вирусы
9. Файловые вирусы
10. Макровирусы
11. Сетевые черви и защита от них
12. Межсетевой экран
13. Почтовые черви
14. Троянские программы и защита от них
15. Троянские программы – шпионы
16. Рекламные программы
17. Хакерские утилиты и защита от них
18. Утилиты взлома удалённых компьютеров

19.Руткиты

20.Защита от хакерских атак, сетевых червей и троянских программ

Блок заданий 2. Тестовые задания по теме. (Инструкция: тип вопроса - выбор одного или нескольких правильных ответов, установить соответствие)

ВАРИАНТ 1

<table>
<tr><td>1. Отличительными способностями компьютерного вируса являются:
а) способность к самостоятельному запуску и многократному копированию кода
б) значительный объем программного кода
в) легкость распознавания</td><td>2. DoS — программы:
а) реализуют распределённые атаки с разных компьютеров, причём без ведома пользователей заражённых компьютеров
б) оба варианта верны
в) реализуют атаку с одного компьютера с ведома пользователя. Эти программы обычно наносят ущерб удалённым компьютерам и сетям, не нарушая работоспособности заражённого компьютера</td></tr>
<tr><td colspan="2">3. Соотнесите соответствия терминов с описанием:
<table>
<tr><td>А. Макровирус</td><td>1. перехватывают обращения операционной системы к пораж файлам и секторам дисков и подставляют вместо своего тела незараженные объекты</td></tr>
<tr><td>Б. Троян</td><td>2. использует возможности макроязыков, встроенных в офис пакеты</td></tr>
<tr><td>В. Червь</td><td>3. маскируется под полезную программу, но выполняют разрушительные действия (например, сбор конфиденциальн информации - паролей)</td></tr>
<tr><td>Г. Стелс-вирус</td><td>4. вычисляет адреса доступных компьютеров в сети и распро по ней свои копии</td></tr>
</table></td></tr>
<tr><td>4. Компьютерные вирусы:
а) являются следствием ошибок в операционной системе
б) пишутся людьми специально для нанесения ущерба пользователем ПК
в) возникают в связи со сбоями в аппаратных средствах компьютера</td><td>5. Сетевые черви бывают:
а) Web-черви
б) черви операционной системы
в) черви MS Office</td></tr>
</table>

6. **По «среде обитания» вирусы можно разделить на:** а) не опасные б) очень опасные в) файловые	7. **Типы методов антивирусной защиты** а) теоретические б) практические в) организационные г) программные д) технические
8**. Антиспамовая программа, установленная на домашнем компьютере, служит для …** а) защиты компьютера от нежелательной и/или не запрошенной корреспонденции б) обеспечения регулярной доставки антивирусной программе новых антивирусных баз в) корректной установки и удаления прикладных программ г) защиты компьютера от хакерских атак	
9**. На чем основано действие антивирусной программы?** а) на ожидании начала вирусной атаки б) на сравнении программных кодов с известными вирусами в) на удалении зараженных файлов	10. **Какие существуют основные средства защиты данных?** а) аппаратные средства б) программные средства в) резервное копирование наиболее ценных данных
11. **Какой вирус ведет себя так же, как файловый, то есть может заражать файлы при обращении к ним компьютера?** а) Интернет-черви б) ревизоры в) загрузочные	12. **Сигнатурный метод антивирусной проверки заключается в …** а) сравнении файла с известными образцами вирусов б) анализе поведения файла в разных условиях в) анализе кода на предмет наличия подозрительных команд г) отправке файлов на экспертизу в компанию-производителя антивирусного средства

ВАРИАНТ 2

1. **Утилиты, используемые для сокрытия вредоносной активности. Они маскируют**	2**. DDos — программы:** а) реализуют атаку с одного компьютера с ведома пользователя.

<table>
<tr><td>вредоносные программы, чтобы избежать их обнаружения антивирусными программами:
а) руткит
б) бэкап
в) камбэк</td><td>Эти программы обычно наносят ущерб удалённым компьютерам и сетям, не нарушая работоспособности заражённого компьютера
б) оба варианта верны
в) реализуют распределённые атаки с разных компьютеров, причём без ведома пользователей заражённых компьютеров</td></tr>
<tr><td colspan="2">3. Соотнесите соответствия терминов с описанием:
<table>
<tr><td>А. Полифаги</td><td>1. Принцип работы основан на подсчете контрольных сум присутствующих на диске файлов</td></tr>
<tr><td>Б. Ревизоры</td><td>2. Программа, перехватывающая «Вирусоопасные» ситуа сообщающие об этом пользователю.</td></tr>
<tr><td>В. Блокировщики</td><td>3. Принцип работы основан на проверке файлов, загрузоч секторов дисков.</td></tr>
</table></td></tr>
<tr><td>4. Троянские программы бывают:
а) сетевые программы
б) программы передачи данных
в) программы — шпионы</td><td>5. Сетевые черви бывают:
а) почтовые черви
б) черви операционной системы
в) черви MS Office</td></tr>
<tr><td>6. По «среде обитания» вирусы можно разделить на:
а) загрузочные
б) очень опасные
в) опасные</td><td>7. Как называется вирус, попадающий на компьютер при работе с электронной почтой:
а) текстовый
б) сетевой
в) файловый</td></tr>
<tr><td colspan="2">8. Косвенное проявление наличия вредоносной программы на компьютере
а) неожиданно появляющееся всплывающее окно с приглашением посетить некий сайт
б) неожиданное уведомление антивирусной программы об обнаружении вируса
в) неожиданное отключение электроэнергии
г) неожиданно появляющееся всплывающее окно с текстом порнографического содержания
д) неожиданное самопроизвольное завершение работы почтового агента</td></tr>
</table>

9. **Преимущества сигнатурного метода антивирусной проверки над эвристическим** а) существенно менее требователен к ресурсам б) не требует регулярного обновления антивирусных баз в) позволяет выявлять новые, еще не описанные вирусными экспертами, вирусы г) более надежный	10. **Этапы действия программного вируса:** а) размножение, вирусная атака б) запись в файл, размножение в) запись в файл, размножение, уничтожение
11. **Свойство вируса, позволяющее называться ему загрузочным – способность …** а) вызывать перезагрузку компьютера-жертвы б) заражать загрузочные сектора жестких дисков в) подсвечивать кнопку Пуск на системном блоке г) заражать загрузочные дискеты и компакт-диски	12. **Троянская программа, троянец:** а) являются вредоносными программами, которые проникают на компьютер, используя сервисы компьютерных сетей б) являются вредоносными программами, которые могут «размножаться» и скрытно внедрять свои копии в файлы, загрузочные секторы дисков и документы в) вредоносная программа, которая выполняет несанкционированную пользователем передачу управления компьютером удалённому пользователю, а также действия по удалению, модификации, сбору и пересылке информации третьим лицам

Ответы на тесты:

ВАРИАНТ 1

1. Отличительными способностями компьютерного вируса являются: а) **способность к самостоятельному запуску и многократному копированию кода**	**2. DoS — программы:** а) реализуют распределённые атаки с разных компьютеров, причём без ведома пользователей заражённых компьютеров б) оба варианта верны в) **реализуют атаку с одного компьютера с ведома**

б) значительный объем программного кода в) легкость распознавания	**пользователя. Эти программы обычно наносят ущерб удалённым компьютерам и сетям, не нарушая работоспособности заражённого компьютера**

3. Соотнесите соответствия терминов с описанием:

А. Макровирус	1. перехватывают обращения операционной системы к пораж файлам и секторам дисков и подставляют вместо своего тела незараженные объекты
Б. Троян	2. использует возможности макроязыков, встроенных в офис пакеты
В. Червь	3. маскируется под полезную программу, но выполняют разрушительные действия (например, сбор конфиденциальн информации - паролей)
Г. Стелс-вирус	4. вычисляет адреса доступных компьютеров в сети и распро по ней свои копии
1Г, 3Б, 2А, 4В	

4. Компьютерные вирусы: а) являются следствием ошибок в операционной системе б) **пишутся людьми специально для нанесения ущерба пользователем ПК** в) возникают в связи со сбоями в аппаратных средствах компьютера	**5. Сетевые черви бывают:** а) **Web-черви** б) черви операционной системы в) черви MS Office
6. По «среде обитания» вирусы можно разделить на: а) не опасные б) очень опасные в) **файловые**	7. Типы методов антивирусной защиты а) теоретические б) практические в**) организационные** г) программные д) **технические**

8. Антиспамовая программа, установленная на домашнем компьютере, служит для …

а) защиты компьютера от нежелательной и/или не запрошенной корреспонденции

б) обеспечения регулярной доставки антивирусной программе новых антивирусных баз

в) корректной установки и удаления прикладных программ

г) защиты компьютера от хакерских атак	
9. На чем основано действие антивирусной программы? а) на ожидании начала вирусной атаки б) **на сравнении программных кодов с известными вирусами** в) на удалении зараженных файлов	**10. Какие существуют основные средства защиты данных?** а) аппаратные средства б) программные средства в) **резервное копирование наиболее ценных данных**
11. Какой вирус ведет себя так же, как файловый, то есть может заражать файлы при обращении к ним компьютера? а) Интернет-черви б) ревизоры в) **загрузочные**	12. Сигнатурный метод антивирусной проверки заключается в … **а) сравнении файла с известными образцами вирусов** б) анализе поведения файла в разных условиях в) анализе кода на предмет наличия подозрительных команд г) отправке файлов на экспертизу в компанию-производителя антивирусного средства

ВАРИАНТ 2

1. Утилиты, используемые для сокрытия вредоносной активности. Они маскируют вредоносные программы, чтобы избежать их обнаружения антивирусными программами: а) р**уткит** б) бэкап в) камбэк	**2. DDos — программы**: а) реализуют атаку с одного компьютера с ведома пользователя. Эти программы обычно наносят ущерб удалённым компьютерам и сетям, не нарушая работоспособности заражённого компьютера б) оба варианта верны в) **реализуют распределённые атаки с разных компьютеров, причём без ведома пользователей заражённых компьютеров**

3. Соотнесите соответствия терминов с описанием:

А. Полифаги	1. Принцип работы основан на подсчете контрольных сум присутствующих на диске файлов
Б. Ревизоры	2. Программа, перехватывающая «Вирусоопасные» ситуа сообщающие об этом пользователю.
В. Блокировщики	3. Принцип работы основан на проверке файлов, загрузоч секторов дисков.

<table>
<tr><td colspan="2">А3, Б1, В2</td></tr>
<tr><td>4. Троянские программы бывают:
а) сетевые программы
б) программы передачи данных
в) программы — шпионы</td><td>5. Сетевые черви бывают:
а) почтовые черви
б) черви операционной системы
в) черви MS Office</td></tr>
<tr><td>6. По «среде обитания» вирусы можно разделить на:
а) загрузочные
б) очень опасные
в) опасные</td><td>7. Как называется вирус, попадающий на компьютер при работе с электронной почтой:
а) текстовый
б) сетевой
в) файловый</td></tr>
<tr><td colspan="2">8. Косвенное проявление наличия вредоносной программы на компьютере
а) неожиданно появляющееся всплывающее окно с приглашением посетить некий сайт
б) неожиданное уведомление антивирусной программы об обнаружении вируса
в) неожиданное отключение электроэнергии
г) неожиданно появляющееся всплывающее окно с текстом порнографического содержания
д) неожиданное самопроизвольное завершение работы почтового агента</td></tr>
<tr><td>9. Преимущества сигнатурного метода антивирусной проверки над эвристическим
а) существенно менее требователен к ресурсам
б) не требует регулярного обновления антивирусных баз
в) позволяет выявлять новые, еще не описанные вирусными экспертами, вирусы
г) более надежный</td><td>10. Этапы действия программного вируса:
а) размножение, вирусная атака
б) запись в файл, размножение
в) запись в файл, размножение, уничтожение.</td></tr>
<tr><td>11. Свойство вируса, позволяющее называться ему загрузочным – способность …
а) вызывать перезагрузку компьютера-жертвы</td><td>12. Троянская программа, троянец:
а) являются вредоносными программами, которые проникают на компьютер, используя сервисы компьютерных сетей</td></tr>
</table>

б) **заражать загрузочные сектора жестких дисков** в) подсвечивать кнопку Пуск на системном блоке г) заражать загрузочные дискеты и компакт-диски	б) являются вредоносными программами, которые могут «размножаться» и скрытно внедрять свои копии в файлы, загрузочные секторы дисков и документы в) **вредоносная программа, которая выполняет несанкционированную пользователем передачу управления компьютером удалённому пользователю, а также действия по удалению, модификации, сбору и пересылке информации третьим лицам**

Блок заданий 3. Самостоятельная работа обучающихся

Самостоятельная работа с научной и специальной литературой, с Интернет-ресурсами, ответы на контрольные вопросы, подготовка самостоятельных сообщений, рефератов по теме.

Тема 2.7 Защита информации в компьютерных сетях. Объекты защиты информации в сети.

Блок заданий 1. Примерный перечень вопросов для устного и письменного опроса по теме:

1. Цели и задачи защиты
2. Угрозы безопасности
3. Компьютерная и сетевая безопасность
4. Брандмауэр
5. Механизм виртуальных частных сетей
6. Безопасная информационная система
7. Конфиденциальность, доступность, целостность данных
8. Сервисы сетевой безопасности
9. Шифрование
10. Криптографическая защита информации
11. Электронная цифровая подпись
12. Аутентификация
13. Идентификация
14. Авторизация
15. Аудит
16. Технология защищенного канала

Блок заданий 2. Тестовые задания по теме. (Инструкция: тип вопроса - выбор одного или нескольких правильных ответов, установить соответствие)

1. Какой аспект информационной безопасности был нарушен, если при передаче по сети файла, информация в нем была прочитана злоумышленником? а. конфиденциальность б. доступность в. целостность г. аутентичность	2. Какой аспект информационной безопасности был нарушен, если при передаче по сети файла, информация в нем была модифицирована злоумышленником? а. конфиденциальность б. доступность в. целостность г. аутентичность
3. Какой аспект информационной безопасности был нарушен, если в результате атаки на сайт авторизованные пользователи не могут получить доступ к необходимым данным? а. конфиденциальность б. доступность в. целостность г. аутентичность	4. Какие угрозы направлены на создание ситуаций, когда определенные действия либо снижают работоспособность информационной системы, либо блокируют доступ к некоторым ее ресурсам? а. угрозы нарушения конфиденциальности б. угрозы нарушения целостности в. угрозы нарушения доступности
5. Как называется процедура проверки идентификационных данных пользователя при доступе к информационной системе? а. идентификация б. аутентификация в. авторизация	6. Как называется процедура предоставления определенному пользователю прав на выполнение некоторых действий? а. идентификация б. аутентификация в. авторизация
7. Какие из нижеперечисленных угроз относятся к внешним угрозам? а. атаки из Интернета б. распространение вредоносного программного обеспечения	8. Какие из нижеперечисленных угроз относятся к случайным воздействиям? а. ошибки в программном обеспечении б. распространение вредоносного программного обеспечения

в. использование сотрудниками слабых паролей для доступа к информационным системам г. передача сотрудниками конфиденциальной информации конкурентам д. перехват информации с использованием радиоприемных устройств е. преднамеренное удаление конфиденциальной информации сотрудниками	в. нежелательные рассылки (спам) г. отказы в работе оборудования д. ошибки в работе персонала е. изменение таблицы маршрутизации для внедрения ложного объекта в сеть

Ключи к тесту:

1	2	3	4	5	6	7	8
а	в	б	в	б	в	а б д	а г д

Блок заданий 3. Самостоятельная работа обучающихся

Самостоятельная работа с научной и специальной литературой, с Интернет-ресурсами, ответы на контрольные вопросы, подготовка самостоятельных сообщений, рефератов по теме:

1. Сервисы безопасности в вычислительных сетях.
2. Механизмы безопасности.
3. Администрирование средств безопасности.

Тема 2.8 Сети и облачные технологии. Использование облачных вычислений и сетей. Ключевые возможности облачных сервисов. Классификация облачных сервисов. Дата-центры для обработки данных. Преимущества облачных сервисов. Модели облачных технологий.

Блок заданий 1. Примерный перечень вопросов для устного и письменного опроса по теме:

1. Облако. Облачные технологии.
2. Облачные хранилища данных.
3. Примеры использования облачных хранилищ.
4. Облачные вычисления.
5. Виды облачных сервисов.
6. Частные облака.
7. Публичные облака.
8. Гибридные облака.
9. Общественное облако.
10. Модели развертывания облачных вычислений.

11. Преимущества и недостатки облачных технологий.
12. Популярные облачные хранилища данных.
13. Популярные бесплатные облачные сервисы.
14. Пример использования облачных технологий в образовании.

Блок заданий 2. Самостоятельная работа обучающихся

Самостоятельная работа с научной и специальной литературой, с Интернет-ресурсами, ответы на контрольные вопросы, подготовка самостоятельных сообщений, рефератов по теме.

Раздел 3. Информационная безопасность цифровой экономики

Тема 3.1. Модели информационной экономики. Разновидности моделей цифровой экономики, сфера их применения.

Блок заданий 1. Примерный перечень вопросов для устного и письменного опроса по теме:

1. Понятие и исторические аспекты цифровизации экономики
2. Особенности цифровой экономики Инструменты цифровой экономики
3. Инструменты цифровой экономики
4. Направления цифровой экономики
5. Национальная программа – «Цифровая экономика РФ»
6. Значение цифровой экономики
7. Риски и проблемы цифровой экономики
8. Информационная безопасность как необходимое условие развития экономики цифрового типа
9. Основные правила безопасного использования и распоряжения информацией сотрудниками
10. Основные инструменты обеспечения информационной безопасности цифровой экономики
11. Зашита серверов от атак хакеров
12. Биометрическая защита
13. Зашита с использованием ЭЦП
14. Зашита с использованием искусственного интеллекта (ИИ)
15. Программно-технические средства защиты

Блок заданий 2. Самостоятельная работа обучающихся

Самостоятельная работа с научной и специальной литературой, с Интернет-ресурсами, ответы на контрольные вопросы, подготовка самостоятельных сообщений, рефератов по теме:

1. Угрозы информационной безопасности в условиях цифровой экономики.
2. Защита внутренней политики информационной безопасности России.

3. Объекты защиты в сфере обеспечения безопасности РФ.
4. угрозам информационной безопасности внутренней политики
5. Мероприятия для обеспечения информационной безопасности РФ в сфере внутренней политики.
6. Технические методы и средства защиты информации.
7. Основные меры по обеспечению информационной безопасности Российской Федерации.

Тема 3.2 Технология «Умный город». Концепция «умного города». Основные функции и принципы, сфера деятельности.

Блок заданий 1. Примерный перечень вопросов для устного и письменного опроса по теме:

1. Концепция «Умный город», цели и принципы ее реализации.
2. Интеллектуальная сеть
3. Умные технологии.
4. Умный учет
5. Интеллектуальная сеть
6. Энергоэффективность.
7. Возможность присоединения распределенной генерации.
8. Основные функции «Умный город».
9. Преимущества системы автоматизации контроля и учета «Умный город».
10. Экономическая эффективность.
11. Примеры умных городов.

Блок заданий 2. Самостоятельная работа обучающихся

Самостоятельная работа с научной и специальной литературой, с Интернет-ресурсами, ответы на контрольные вопросы, подготовка самостоятельных презентаций по теме:

1. Концепция «Умный город».
2. Реализация смарт сити.
3. Умный город – технологии и перспективы.

Тема 3.3 Технология блокчейн. Понятие электронных денег, сферы их использования, их виды. Криптовалюта. Биткоины.

Блок заданий 1. Примерный перечень вопросов для устного и письменного опроса по теме:

1. Технология блокчейн.
2. История понятия «блокчейн»
3. Как блокчейн связан с понятием биткоин.
4. Сферы применения блокчейна: криптовалюта

5. Сферы применения блокчейна: банковское дело
6. Сферы применения блокчейна: кибербезопасность
7. Сферы применения блокчейна: удостоверения личности
8. Как работают платежные средства на блокчейне.
9. Критика блокчейна: минусы технологии
10. Будущее технологии в России и за рубежом

Блок заданий 2. Самостоятельная работа обучающихся

Самостоятельная работа с научной и специальной литературой, с Интернет-ресурсами, ответы на контрольные вопросы, подготовка самостоятельных презентаций по теме:

1. Технология блокчейн.
2. Сферы применения блокчейна
3. Криптовалюта. Биткоины.

Тема 3.4 Интеллектуальные системы. Искусственный интеллект.

Направление исследований в искусственном интеллекте. Основные задачи искусственного интеллекта.

Блок заданий 1. Примерный перечень вопросов для устного и письменного опроса по теме:

1. Понятие об искусственном интеллекте.
2. Направления развития искусственного интеллекта
3. Интеллектуальные информационные системы
4. Разработка естественно-языковых интерфейсов и машинный перевод.
5. Генерация и распознавание речи.
6. Обработка визуальной информации.
7. Обучение и самообучение.
8. Распознавание образов.
9. Игры и машинное творчество.
10. Автоматические рассуждения и доказательства теорем.
11. Новые архитектуры компьютеров.
12. Интеллектуальные роботы.

Блок заданий 2. Самостоятельная работа обучающихся

Самостоятельная работа с научной и специальной литературой, с Интернет-ресурсами, ответы на письменные контрольные вопросы:

1. В чем заключается суть направления развития искусственного интеллекта, основанного на попытке создать нейронную модель мозга?
2. Каковы современные аспекты применения нейросистем?
3. Каковы недостатки нейронных сетей?
4. В чем заключаются преимущества нейронных сетей?

5. Из каких элементов состоит модель искусственного нейрона?
6. Как работает искусственный нейрон?
7. Как строятся нейронные сети?
8. Какие задачи решаются с помощью нейронных сетей?
9. Как производится обучение нейронной сети?
10. Какие типы правил обучения нейросетей вы знаете?

Тема 3.5 Технология Интернет вещей. Области применения в цифровой экономике. Перспективы технологии вещей.

Блок заданий 1. Примерный перечень вопросов для устного и письменного опроса по теме:

1. Основные понятия Интернета вещей (IoT, Internet of Things). История Интернета вещей.
2. Сферы для реализации IoT технологий.
3. Интернет вещей - конкурентные преимущества.
4. Программно-аппаратные средства Интернета вещей. Средства идентификации
5. Средства измерения. Средства подачи данных. Средства обработки данных
6. Архитектура Интернета вещей
7. Умная парковка
8. Умная теплица
9. «Умный дом». Схема «Умного дома».

Блок заданий 2. Самостоятельная работа обучающихся

Самостоятельная работа с научной и специальной литературой, с Интернет-ресурсами, ответы на контрольные вопросы, подготовка самостоятельных презентаций по теме:

1. Сферы для реализации IoT технологий.

Тема 3.6 Технология Роботизированной Автоматизации (RPA). Области применения технологии RPA. Преимущества RPA. Перспективы RPA-технологий.

Блок заданий 1. Примерный перечень вопросов для устного и письменного опроса по теме:

1. Интеллектуальные программные роботы (RPA).
2. Преимущества технологии RPA.
3. История роботизации.
4. Эффективность применения RPA.
5. Жизненный цикл робота.

6. Развитие технологии.
7. OCR & NLP. Распознование структурированных и неструктурированных документов.
8. ML & конвейр.

Блок заданий 2. Самостоятельная работа обучающихся

Самостоятельная работа с научной и специальной литературой, с Интернет-ресурсами, ответы на контрольные вопросы, подготовка самостоятельных презентаций по теме:

1. Робот вместо человека.
2. Какие бывают роботы: цифровой работник, цифровой читатель, цифровой диктор, цифровой интеллект.

4. Контрольно-оценочные материалы для промежуточной аттестации по учебной дисциплине

4.1 Пакет экзаменатора

Промежуточный контроль по результатам освоения обучающимися учебной дисциплины проводится в форме дифференцированного зачёта (зачёт с оценкой).

Дифференцированный зачёт проводится в форме тестовых заданий.

Количество вариантов заданий – 1 вариант теста.

Форма оценки: оценка продукта практической деятельности (заполненные бланки ответов теста);

Методы проверки: сопоставление с эталоном;

Требования к процедуре оценки: особых требований нет

Помещение: особых требований нет,

Оборудование: особых требований нет

Инструменты: особых требований нет,

Расходные материалы: бланк ответов

Доступ к дополнительным инструкциям и справочным материалам: не предусмотрен

Норма времени: 1 академический час

Инструмент проверки (модельный ответ)

Сравнение с эталоном, набор критериев для экспертной оценки

Критерии оценки	Количество правильных ответов	Оценка
«5» - 100 – 90% правильных ответов «4» - 89 - 75% правильных ответов	52-47 46-39 38-29	5 отлично 4 хорошо

«3» - 74 – 55% правильных ответов «2» - 54% и менее правильных ответов	28 и менее	3 удовлетворительно 2 неудовлетворительно

Ключи к тесту:

1. Как студент обязан обращаться со студенческим билетом?
   Постоянно иметь при себе, бережно хранить и не передавать другим лицам
2. Порядок действий при необходимости пропустить занятия по уважительной причине
   Написать заявление, согласовать с классным руководителем и подписать у зав. отделением
3. В какой одежде запрещено находиться студенту в колледже?
   В спортивной одежде, в шортах, в пляжной обуви
4. Назовите наименование квалификации по специальности? Чем занимается этот специалист на предприятии?
   Наименование квалификации -Техник по защите информации
   Техник по защите информации — это специалист, который занимается обеспечением информационной безопасности предприятия и его информационной инфраструктуры, техническим обслуживанием средств защиты информации.
   Техники по защите информации проводят информационное обследование и анализ, разрабатывают правовые документы, которые максимально упорядочивают информационные потоки.
   Специалист устанавливает и настраивает средства и механизмы защиты, а также поддерживает, обновляет, модернизирует созданную систему безопасности.
5. Назовите объекты профессиональной деятельности.
   а. **Объекты информатизации.**
   б. **Средства защиты информации.**
   в. **Документация.**
   г. **Первичные трудовые коллективы**
6. Назовите виды деятельности техника по защите информации
   - **участие в планировании и организации работ по обеспечению защиты объекта;**
   - **организация и технология работы с конфиденциальными документами;**
   - **работа с различными системами электронного документооборота;**

- **применение программно-аппаратных и технических средств защиты информации;**
- **участие в организации комплексной системы защиты объекта;**
- **выполнение работ по одной или нескольким профессиям рабочих, должностям служащих**

7. ***Дополните определение:***

Информационная безопасность – это защита …

целостности, доступности и конфиденциальности информации.

8. ***Дополните определение:***

Защита информации – это комплекс …

мероприятий, направленных на обеспечение информационной безопасности.

9. ***Впишите варианты ответов в таблицу:***

Информационные угрозы преднамеренные:	а	д	ж			
Информационные угрозы случайные:	б	в	г	е		

а. Компьютерные вирусы
б. Отказ, сбой аппаратуры
в. Ошибки в программировании
г. Ошибки пользователя
д. Физическое воздействие на аппаратуру
е. Форс-мажорные обстоятельства
ж. Хищение информации

10.Отличительными способностями компьютерного вируса являются:

а) способность к самостоятельному запуску и многократному копированию кода

б) значительный объем программного кода

в) легкость распознавания

11.**DoS — программы:**

а) реализуют распределённые атаки с разных компьютеров, причём без ведома пользователей заражённых компьютеров

б) оба варианта верны

в) **реализуют атаку с одного компьютера с ведома пользователя. Эти программы обычно наносят ущерб удалённым компьютерам и сетям, не нарушая работоспособности заражённого компьютера**

12.**DDos — программы**:

а) реализуют атаку с одного компьютера с ведома пользователя. Эти программы обычно наносят ущерб удалённым компьютерам и сетям, не нарушая работоспособности заражённого компьютера

б) оба варианта верны

в) **реализуют распределённые атаки с разных компьютеров, причём без ведома пользователей заражённых компьютеров**

13. **Утилиты, используемые для сокрытия вредоносной активности. Они маскируют вредоносные программы, чтобы избежать их обнаружения антивирусными программами**:

а) р**уткит**

б) бэкап

в) камбэк

14. **Соотнесите соответствия терминов с описанием:**

А. Полифаги	1. Принцип работы основан на подсчете контрольных сумм для присутствующих на диске файлов
Б. Ревизоры	2. Программа, перехватывающая «Вирусоопасные» ситуации и сообщающие об этом пользователю.
В. Блокировщики	3. Принцип работы основан на проверке файлов, загрузочных секторов дисков.
А3, Б1, В2	

15. **Соотнесите соответствия терминов с описанием:**

А. Макровирус	1. перехватывают обращения операционной системы к пораженным файлам и секторам дисков и подставляют вместо своего тела незараженные объекты
Б. Троян	2. использует возможности макроязыков, встроенных в офисные пакеты
В. Червь	3. маскируется под полезную программу, но выполняют разрушительные действия (например, сбор конфиденциальной информации - паролей)
Г. Стелс-вирус	4. вычисляет адреса доступных компьютеров в сети и распространяе по ней свои копии
1Г, 3Б, 2А, 4В	

16. **Сетевые черви бывают:**

а) **Web-черви**

б) черви операционной системы

в) черви MS Office

17. **Троянские программы бывают:**

а) сетевые программы

б) программы передачи данных

в) **программы — шпионы**

18.. Типы методов антивирусной защиты

а) теоретические

б) практические

в**) организационные**

г) программные

д) **технические**

19. **На чем основано действие антивирусной программы?**

а) на ожидании начала вирусной атаки

б) **на сравнении программных кодов с известными вирусами**

в) на удалении зараженных файлов

20. **Какие существуют основные средства защиты данных?**

а) аппаратные средства

б) программные средства

в) **резервное копирование наиболее ценных данных**

21. Преимущества сигнатурного метода антивирусной проверки над эвристическим

а) существенно менее требователен к ресурсам

б) не требует регулярного обновления антивирусных баз

в) позволяет выявлять новые, еще не описанные вирусными экспертами, вирусы

г) **более надежный**

22. **Этапы действия программного вируса:**

а) размножение, вирусная атака

б) запись в файл, размножение

в**) запись в файл, размножение, уничтожение.**

23. Свойство вируса, позволяющее называться ему загрузочным – способность …

а) вызывать перезагрузку компьютера-жертвы

б) **заражать загрузочные сектора жестких дисков**

в) подсвечивать кнопку Пуск на системном блоке

г) заражать загрузочные дискеты и компакт-диски

24. **Какой вирус ведет себя так же, как файловый, то есть может заражать файлы при обращении к ним компьютера?**

а) Интернет-черви

б) ревизоры

в) **загрузочные**

25. Сигнатурный метод антивирусной проверки заключается в …

а) сравнении файла с известными образцами вирусов

б) анализе поведения файла в разных условиях

в) анализе кода на предмет наличия подозрительных команд

г) отправке файлов на экспертизу в компанию-производителя антивирусного средства

26. Троянская программа, троянец:

а) являются вредоносными программами, которые проникают на компьютер, используя сервисы компьютерных сетей

б) являются вредоносными программами, которые могут «размножаться» и скрытно внедрять свои копии в файлы, загрузочные секторы дисков и документы

в) **вредоносная программа, которая выполняет несанкционированную пользователем передачу управления компьютером удалённому пользователю, а также действия по удалению, модификации, сбору и пересылке информации третьим лицам**

27. К биометрическим системам защиты информации относятся системы идентификации по:

а) **отпечаткам пальцев**

б) **характеристикам речи**

в) радужной оболочке глаза

г) изображению лица

д) геометрии ладони руки

е) росту

ж) весу

з) цвету глаз

и) цвету волос

28. Если узор … не совпадает с узором допущенного к информации пользователя, то доступ к информации невозможен. Как называется этот критерий?

а) идентификация по радужной оболочке глаза

б) идентификация по ладони руки

в**) идентификация по отпечаткам пальцев**

29. Межсетевой экран (брандмауэр) -

а) являются вредоносными программами, которые могут "размножаться" и скрытно внедрять свои копии в файлы, загрузочные секторы дисков и документы. Активизация компьютерного вируса может вызывать уничтожение программ и данных.

б) являются вредоносными программами, которые проникают на компьютер, используя сервисы компьютерных сетей. Их активизация может вызывать уничтожение программ и данных, а также похищение персональных данных пользователя.

в) вредоносная программа, которая выполняет несанкционированную пользователем передачу управления компьютером удалённому пользователю, а также действия по удалению, модификации, сбору и пересылке информации третьим лицам.

г) **это программное или аппаратное обеспечение, которое проверяет информацию, входящую в компьютер из локальной сети или Интернета, а затем либо отклоняет её, либо пропускает в компьютер, в зависимости от параметров.**

д) программа или набор программ для скрытого взятия под контроль взломанной системы. Это утилиты, используемые для сокрытия вредоносной активности. Они маскируют вредоносные программы, чтобы избежать их обнаружения антивирусными программами

30.Межсетевой экран позволяет:

а) **блокировать хакерские DoS - атаки, не пропуская на защищаемый компьютер сетевые пакеты с определённых серверов**

б) не допускать проникновение на защищаемый компьютер сетевых червей

в) препятствовать троянским программам отправлять конфиденциальную информацию о пользователе и компьютере

г) видеть действия которые выполняет пользователь на другом компьютере

д) использовать принтер подключённый к другому компьютеру

31. **Соотнесите соответствия терминов с описанием:**

А. DDos - программы	1. реализуют распределённые атаки с разных компьютеров, причём без ведома пользователей заражённых компьютеров
Б. DoS - программы	2. реализуют атаку с одного компьютера с ведома пользователя. Эти программы обычно наносят ущерб удалённым компьютерам и сетям, не нарушая работоспособности заражённого компьютера.
А1, Б2	

32.Какой аспект информационной безопасности был нарушен, если при передаче по сети файла, информация в нем была прочитана злоумышленником?

а) **конфиденциальность**

б) доступность

в) целостность

г) аутентичность

33.Какой аспект информационной безопасности был нарушен, если в результате атаки на сайт авторизованные пользователи не могут получить доступ к необходимым данным?

а) конфиденциальность

б) доступность

в) целостность

г) аутентичность

34. Какой аспект информационной безопасности был нарушен, если при передаче по сети файла, информация в нем была модифицирована злоумышленником?

а) конфиденциальность

б) доступность

в) целостность

г) аутентичность

35. Какие угрозы направлены на создание ситуаций, когда определенные действия либо снижают работоспособность информационной системы, либо блокируют доступ к некоторым ее ресурсам?

а) угрозы нарушения конфиденциальности

б) угрозы нарушения целостности

в) **угрозы нарушения доступности**

36. Какие из нижеперечисленных угроз относятся к внешним угрозам?

а) **атаки из Интернета**

б) распространение вредоносного программного обеспечения

в) использование сотрудниками слабых паролей для доступа к информационным системам

г) передача сотрудниками конфиденциальной информации конкурентам

д) **перехват информации с использованием радиоприемных устройств**

е) преднамеренное удаление конфиденциальной информации сотрудниками

37. Какие из нижеперечисленных угроз относятся к случайным воздействиям?

а) **ошибки в программном обеспечении**

б) распространение вредоносного программного обеспечения

в) нежелательные рассылки (спам)

г**) отказы в работе оборудования**

д) ошибки в работе персонала

е) изменение таблицы маршрутизации для внедрения ложного объекта в сеть

38. Какая система может контролировать возможность выполнения пользователями системных функций: локальный доступ к серверу, установка системного времени, создание резервных копий данных, выключение сервера?	система авторизации
39. Последовательность символов, полученная в результате криптографического преобразования исходного сообщения с использованием закрытого ключа и позволяющая определять целостность сообщения и принадлежность его автору при помощи открытого ключа	электронная цифровая подпись

40. Процедура контроля доступа легальных пользователей к ресурсам системы с предоставлением каждому из них именно тех прав, которые определены ему администратором, называется …	авторизация
41. Процедура предотвращения доступа к сети нежелательных лиц и разрешения входа для легальных пользователей называется…	аутентификация
42. Процедура сообщения пользователем системе своего идентификатора называется…	идентификация
43. Процедуры шифрования и дешифрирования называются…	криптосистемой
44. Фиксация в системном журнале событий, связанных с доступом к защищаемым системным ресурсам называется…	аудит

45. Какие действия в Уголовном кодексе РФ классифицируются как преступления в компьютерной информационной сфере?
    г. **Неправомерный доступ к компьютерной информации**
    д. **Создание, использование и распространение вредоносных программ для ЭВМ**
    е. **Умышленное нарушение правил эксплуатации ЭВМ и их сетей**
46. Какой из нормативно-правовых документов определяет перечень объектов информационной безопасности личности, общества и государства и методы ее обеспечения?
    а) Уголовный кодекс РФ
    б) Гражданский кодекс РФ
    в) Доктрина информационной безопасности РФ
    г) Постановления Правительства
    д) Указ Президента РФ
47. Основным источником права в области обеспечения информационной безопасности в России является
    а) Уголовный кодекс
    б) Конституция
    в) государственные и отраслевые стандарты
    г) Документы Гостехкомиссии
48. Методы обеспечения информационной безопасности делятся:
    а) правовые
    б) организационно-технические
    в) политические
    г) экономические

49. Определение понятия "конфиденциальная информация" дано в:

а) Конституции РФ

б) Законе "О государственной тайне"

в) Законе "Об информации, информатизации и защите информации"

г) УК РФ

50. Установите соответствие:

1	Органы законодательной власти (Государственная дума)
2	Органы исполнительной власти (правительство)
3	Правительство
4	Министерства и ведомства

А	разрабатывают и принимают постановления и решения, являющиеся нормативными правовыми актами
Б	издают законы, регулирующие отношения в области защиты информации
В	контролируют исполнение законов
Г	принимают соответствующие постановления в области защиты информации и издает распоряжения, являющиеся подзаконными нормативными правовыми актами

1	Б
2	В
3	Г
4	А

4.1 Пакет экзаменующегося

Промежуточный контроль по результатам освоения обучающимися учебной дисциплины проводится в форме дифференцированного зачёта (зачёт с оценкой).

Дифференцированный зачёт проводится в форме тестовых заданий.

Количество вариантов заданий – 1 вариант теста.

Форма оценки: оценка продукта практической деятельности (заполненные бланки ответов теста);

Помещение: особых требований нет,

Оборудование: особых требований нет

Инструменты: особых требований нет,

Расходные материалы: бланки ответов

Доступ к дополнительным инструкциям и справочным материалам: не предусмотрен

Норма времени: 1 академический час

ТЕСТОВЫЕ ЗАДАНИЯ

Тест промежуточной аттестации (дифференцированный зачет)

По дисциплине ВВЕДЕНИЕ В СПЕЦИАЛЬНОСТЬ

для специальности 10.02.05 Обеспечение информационной безопасности автоматизированных систем

1. Как студент обязан обращаться со студенческим билетом?
2. Порядок действий при необходимости пропустить занятия по уважительной причине
3. В какой одежде запрещено находиться студенту в колледже?
4. Назовите наименование квалификации по специальности? Чем занимается этот специалист на предприятии?
5. Назовите объекты профессиональной деятельности.
6. Назовите виды деятельности техника по защите информации.
7. ***Дополните определение:***

Информационная безопасность – это защита …

8. ***Дополните определение:***

Защита информации – это комплекс …

9. **Соотнесите соответствия терминов с описанием:**

1) Информационные угрозы преднамеренные:	з. Компьютерные вирусы и. Отказ, сбой аппаратуры к. Ошибки в программировании л. Ошибки пользователя м. Физическое воздействие на аппаратуру н. Форс-мажорные обстоятельства о. Хищение информации
2) Информационные угрозы случайные:	

10. **Отличительными способностями компьютерного вируса являются**:

а) способность к самостоятельному запуску и многократному копированию кода

б) значительный объем программного кода

в) легкость распознавания

11. **DoS — программы:**

а) реализуют распределённые атаки с разных компьютеров, причём без ведома пользователей заражённых компьютеров

б) оба варианта верны

в) реализуют атаку с одного компьютера с ведома пользователя. Эти программы обычно наносят ущерб удалённым компьютерам и сетям, не нарушая работоспособности заражённого компьютера

12. **DDos — программы**:

а) реализуют атаку с одного компьютера с ведома пользователя. Эти программы обычно наносят ущерб удалённым компьютерам и сетям, не нарушая работоспособности заражённого компьютера

б) оба варианта верны

в) реализуют распределённые атаки с разных компьютеров, причём без ведома пользователей заражённых компьютеров

13. **Утилиты, используемые для сокрытия вредоносной активности. Они маскируют вредоносные программы, чтобы избежать их обнаружения антивирусными программами**:

а) руткит

б) бэкап

в) камбэк

14. **Соотнесите соответствия терминов с описанием:**

А) Полифаги	1) Принцип работы основан на подсчете контрольных сумм для присутствующих на диске файлов 2) Программа, перехватывающая «Вирусоопасные» ситуации и сообщающие об этом пользователю. 3) Принцип работы основан на проверке файлов, загрузочных секторов дисков.
Б) Ревизоры	
В) Блокировщики	

15. **Соотнесите соответствия терминов с описанием:**

А) Макровирус	1) перехватывают обращения операционной системы к пораженным файлам и секторам дисков и подставляют вместо своего тела незараженные объекты 2) использует возможности макроязыков, встроенных в офисные пакеты 3) маскируется под полезную программу, но выполняют разрушительные действия (например, сбор конфиденциальной информации - паролей) 4) вычисляет адреса доступных компьютеров в сети и распространяет по ней свои копии
Б) Троян	
В) Червь	
Г) Стелс-вирус	

16. **Сетевые черви бывают:**

а) Web-черви

б) черви операционной системы

в) черви MS Office

17. **Троянские программы бывают:**

а) сетевые программы

б) программы передачи данных

в) программы — шпионы

18. **Типы методов антивирусной защиты**

а) теоретические
б) практические
в**)** организационные
г) программные
д) технические

19. **На чем основано действие антивирусной программы?**

а) на ожидании начала вирусной атаки
б) на сравнении программных кодов с известными вирусами
в) на удалении зараженных файлов

20. **Какие существуют основные средства защиты данных?**

а) аппаратные средства
б) программные средства
в) резервное копирование наиболее ценных данных

21. **Преимущества сигнатурного метода антивирусной проверки над эвристическим**

а) существенно менее требователен к ресурсам
б) не требует регулярного обновления антивирусных баз
в) позволяет выявлять новые, еще не описанные вирусными экспертами, вирусы
г) более надежный

22. **Этапы действия программного вируса:**

а) размножение, вирусная атака
б) запись в файл, размножение
в**)** запись в файл, размножение, уничтожение

23. **Свойство вируса, позволяющее называться ему загрузочным – способность …**

а) вызывать перезагрузку компьютера-жертвы
б) заражать загрузочные сектора жестких дисков
в) подсвечивать кнопку Пуск на системном блоке
г) заражать загрузочные дискеты и компакт-диски

24. **Какой вирус ведет себя так же, как файловый, то есть может заражать файлы при обращении к ним компьютера?**

а) Интернет-черви
б) ревизоры
в) загрузочные

25. **Сигнатурный метод антивирусной проверки заключается в …**

а) сравнении файла с известными образцами вирусов
б) анализе поведения файла в разных условиях
в) анализе кода на предмет наличия подозрительных команд

г) отправке файлов на экспертизу в компанию-производителя антивирусного средства

26. **Троянская программа, троянец:**

а) являются вредоносными программами, которые проникают на компьютер, используя сервисы компьютерных сетей

б) являются вредоносными программами, которые могут «размножаться» и скрытно внедрять свои копии в файлы, загрузочные секторы дисков и документы

в) вредоносная программа, которая выполняет несанкционированную пользователем передачу управления компьютером удалённому пользователю, а также действия по удалению, модификации, сбору и пересылке информации третьим лицам

27. **К биометрическим системам защиты информации относятся системы идентификации по:**

а) отпечаткам пальцев

б) характеристикам речи

в) радужной оболочке глаза

г) изображению лица

д) геометрии ладони руки

е) росту

ж) весу

з) цвету глаз

и) цвету волос

28. **Если узор … не совпадает с узором допущенного к информации пользователя, то доступ к информации невозможен. Как называется этот критерий?**

а) идентификация по радужной оболочке глаза

б) идентификация по ладони руки

в**)** идентификация по отпечаткам пальцев

29. **Межсетевой экран (брандмауэр) -**

а) являются вредоносными программами, которые могут "размножаться" и скрытно внедрять свои копии в файлы, загрузочные секторы дисков и документы. Активизация компьютерного вируса может вызывать уничтожение программ и данных

б) являются вредоносными программами, которые проникают на компьютер, используя сервисы компьютерных сетей. Их активизация может вызывать уничтожение программ и данных, а также похищение персональных данных пользователя

в) вредоносная программа, которая выполняет несанкционированную пользователем передачу управления компьютером удалённому пользователю, а также действия по удалению, модификации, сбору и пересылке информации третьим лицам

г) это программное или аппаратное обеспечение, которое проверяет информацию, входящую в компьютер из локальной сети или Интернета, а затем либо отклоняет её, либо пропускает в компьютер, в зависимости от параметров

д) программа или набор программ для скрытого взятия под контроль взломанной системы. Это утилиты, используемые для сокрытия вредоносной активности. Они маскируют вредоносные программы, чтобы избежать их обнаружения антивирусными программами

30. **Межсетевой экран позволяет:**

а) блокировать хакерские DoS - атаки, не пропуская на защищаемый компьютер сетевые пакеты с определённых серверов

б) не допускать проникновение на защищаемый компьютер сетевых червей

в) препятствовать троянским программам отправлять конфиденциальную информацию о пользователе и компьютере

г) видеть действия которые выполняет пользователь на другом компьютере

д) использовать принтер подключённый к другому компьютеру

31. **Соотнесите соответствия терминов с описанием:**

А) DDos - программы	1) реализуют распределённые атаки с разных компьютеров, причём без ведома пользователей заражённых компьютеров
Б) DoS - программы	2) реализуют атаку с одного компьютера с ведома пользователя. Эти программы обычно наносят ущерб удалённым компьютерам и сетям, не нарушая работоспособности заражённого компьютера.
	3) реализуют атаку с одного компьютера без ведома пользователя. Эти программы обычно наносят ущерб удалённым компьютерам и сетям, не нарушая работоспособности заражённого компьютера.

32. **Какой аспект информационной безопасности был нарушен, если при передаче по сети файла, информация в нем была прочитана злоумышленником?**

а) конфиденциальность

б) доступность

в) целостность

г) аутентичность

33. **Какой аспект информационной безопасности был нарушен, если в результате атаки на сайт авторизованные пользователи не могут получить доступ к необходимым данным?**

а) конфиденциальность

б) доступность

в) целостность

г) аутентичность

34. **Какой аспект информационной безопасности был нарушен, если при передаче по сети файла, информация в нем была модифицирована злоумышленником?**

а) конфиденциальность

б) доступность

в) целостность

г) аутентичность

35. **Какие угрозы направлены на создание ситуаций, когда определенные действия либо снижают работоспособность информационной системы, либо блокируют доступ к некоторым ее ресурсам?**

а) угрозы нарушения конфиденциальности

б) угрозы нарушения целостности

в) угрозы нарушения доступности

36. **Какие из нижеперечисленных угроз относятся к внешним угрозам?**

а) атаки из Интернета

б) распространение вредоносного программного обеспечения

в) использование сотрудниками слабых паролей для доступа к информационным системам

г) передача сотрудниками конфиденциальной информации конкурентам

д) перехват информации с использованием радиоприемных устройств

е) преднамеренное удаление конфиденциальной информации сотрудниками

37. **Какие из нижеперечисленных угроз относятся к случайным воздействиям?**

а) ошибки в программном обеспечении

б) распространение вредоносного программного обеспечения

в) нежелательные рассылки (спам)

г**)** отказы в работе оборудования

д) ошибки в работе персонала

е) изменение таблицы маршрутизации для внедрения ложного объекта в сеть

38. Какая система может контролировать возможность выполнения пользователями системных функций: локальный доступ к серверу,

установка системного времени, создание резервных копий данных, выключение сервера?

Дополните определения:

39. Последовательность символов, полученная в результате криптографического преобразования исходного сообщения с использованием закрытого ключа и позволяющая определять целостность сообщения и принадлежность его автору при помощи открытого ключа называется …
40. Процедура контроля доступа легальных пользователей к ресурсам системы с предоставлением каждому из них именно тех прав, которые определены ему администратором, называется …
41. Процедура предотвращения доступа к сети нежелательных лиц и разрешения входа для легальных пользователей называется…
42. Процедура сообщения пользователем системе своего идентификатора называется…
43. Процедуры шифрования и дешифрирования называются…
44. Фиксация в системном журнале событий, связанных с доступом к защищаемым системным ресурсам называется…

46. **Какие действия в Уголовном кодексе РФ классифицируются как преступления в компьютерной информационной сфере?**
    ж. неправомерный доступ к компьютерной информации
    з. создание, использование и распространение вредоносных программ для ЭВМ
    и. умышленное нарушение правил эксплуатации ЭВМ и их сетей
47. **Какой из нормативно-правовых документов определяет перечень объектов информационной безопасности личности, общества и государства и методы ее обеспечения?**
    а) Уголовный кодекс РФ
    б) Гражданский кодекс РФ
    в) Доктрина информационной безопасности РФ
    г) Постановления Правительства
    д) Указ Президента РФ
48. **Основным источником права в области обеспечения информационной безопасности в России является**
    а) Уголовный кодекс
    б) Конституция
    в) государственные и отраслевые стандарты
    г) Документы Гостехкомиссии
49. **Методы обеспечения информационной безопасности делятся:**

а) правовые

б) организационно-технические

в) политические

г) экономические

51. **Определение понятия "конфиденциальная информация" дано в:**

а) Конституции РФ

б) Законе "О государственной тайне"

в) Законе "Об информации, информатизации и защите информации"

г) УК РФ

52. ***Установите соответствие:***

1) Органы законодательной власти (Государственная дума)	А) разрабатывают и принимают постановления и решения, являющиеся нормативными правовыми актами
2) Органы исполнительной власти (правительство)	Б) издают законы, регулирующие отношения в области защиты информации
3) Правительство	В) контролируют исполнение законов
4) Министерства и ведомства	Г) принимают соответствующие постановления в области защиты информации и издает распоряжения, являющиеся подзаконными нормативными правовыми актами

5. Перечень материалов, оборудования и информационных ресурсов, используемых для подготовки и проведения текущей и промежуточной аттестации

Оборудование учебного кабинета:

- посадочные места по количеству обучающихся;
- рабочее место преподавателя;
- комплект электронных видеоматериалов;
- задания для проверочных работ;
- профессионально ориентированные задания;
- материалы промежуточной аттестации.

Технические средства обучения:

- персональный компьютер с лицензионным программным обеспечением;
- проектор с экраном.

Залы:

Библиотека, читальный зал с выходом в сеть Интернет.

Информационное обеспечение обучения.

Основные источники:

1. Ищейнов В.Я. Основные положения информационной безопасности: - М.: Форум, НИЦ ИНФРА-М, 2021. ЭР Znanium.com
2. Партыка Т.Л. Информационная безопасность. -М: ИНФРА,2021. ЭР Znanium.com
3. Шаньгин В.Ф. Информационная безопасность компьютерных систем и сетей: - М.: ИД ФОРУМ: НИЦ ИНФРА-М, 2018.

Дополнительные источники:

1. Мельников В.П., Клейменов С.А., Петраков А.М. Информационная безопасность. – М.: Издательский центр «Академия», 2018.
2. Партыка Т.Л., Попов И.И. Информационная безопасность: учебное пособие – М.: ФОРУМ, 2020.
3. Попов В.Б. Основы информационных и телекоммуникационных технологий. Основы информационной безопасности: Учебное пособие – М.: Финансы и статистика, 2018.
4. Расторгуев С.П. Основы информационной безопасности – М.: Академия, 2014.
5. Степанов Е.А., Корпев И.К. Информационная безопасность и зашита информации. - М.-ИНФРА-М, 2019.
6. Цирлов В.Л. Основы информационной безопасности: краткий курс/Профессиональное образование. – М.: Феникс, 2019.

Интернет - ресурсы:

1. http://fcior.edu.ru/ - Федеральный центр информационно- образовательных ресурсов
2. http://www.edu.ru/ - Федеральные образовательные ресурсы
3. https://www.kaspersky.ru/– Web-сайт разработчиков антивируса Касперский.
4. http:// www.dials.ru – сервер антивирусной лаборатории.
5. www.fcior.edu.ru (Федеральный центр информационно-образовательных ресурсов).
6. wwww.dic.academic.ru (Академик. Словари и энциклопедии).
7. www.booksgid.com (Books Gid. Электронная библиотека).
8. www.window.edu.ru (Единое окно доступа к образовательным ресурсам).
9. www.st-books.ru (Лучшая учебная литература).
10. www.school.edu.ru (Российский образовательный портал. Доступность, качество, эффективность).
11. www.ru/book (Электронная библиотечная система).

12. www.school-collection.edu.ru (Единая коллекция цифровых образовательных ресурсов).