Негосударственное аккредитованное некоммерческое частное образовательное учреждение высшего образования
«Академия маркетинга и социально-информационных технологий – ИМСИТ»
г. Краснодар

Академический колледж

УТВЕРЖДАЮ
Проректор по учебной работе,
доцент Н. И. Севрюгина
28 марта 2022 г.

ПМ.03 Программно-аппаратные и технические средства защиты информации

рабочая программа профессионального модуля

для студентов специальности

10.02.01 Организация и технология защиты информации

Технический профиль

Квалификация выпускника -Техник по защите информации

г. Краснодар 2022

Рассмотрено
на заседании предметно цикловой комиссии
Протокол № 8 от 21 марта 2022г.
Председатель ПЦК А.А. Куценко
Зав. ИИО Академического колледжа
Ю.А. Худына

Принято
педагогическим советом
Академического колледжа
Протокол № 7
от 22 марта 2022 г.

Рабочая программа разработана на основе основной профессиональной образовательной программы среднего профессионального образования программы подготовки специалистов среднего звена, специальности 10.02.01 Организация и технология защиты информации, Федерального закона Российской Федерации от 29 декабря 2012 г. № 273- ФЗ Об образовании в Российской Федерации (редакция от 25.12.2018 г.) и требований ФГОС среднего профессионального образования (приказ от 28.07.2014 г. № 805 Об утверждении федерального государственного образовательного стандарта среднего профессионального образования по специальности 10.02.01 Организация и технология защиты информации (Зарегистрировано в Минюсте России 21.08.2014 г. № 33750) технического профиля профессионального образования.

Содержание программы реализуется в процессе освоения студентами основной профессиональной образовательной программы по специальности 10.02.01 Организация и технология защиты информации технического профиля (на базе основного общего образования) в соответствии с требованиями ФГОС СПО на 3 курсе (ах) в 5-6 семестре (ах).

Рецензенты:

Заместитель директора по учебно-методической работе ЧУ ПОО КТУИС г. Краснодар, Бондаренко Н. А.

Директор ООО «Вектор» г. Краснодар,
Бромберг Е. М.

Советник директора ООО «Аэро-тревел», г. Краснодар,
Коробенко Я.В.

СОДЕРЖАНИЕ

1 Паспорт программы учебной дисциплины

1.1 Цели и задачи дисциплины

Учебная дисциплина «Программно-аппаратные средства защиты информации» является дисциплиной федерального компонента цикла общепрофессиональных дисциплин специальности 10.02.01 «Организация и технология защиты информации».

Целью дисциплины «Программно-аппаратные средства защиты информации» является ознакомление студентов с современными средствами защиты информации в компьютерных системах, овладение методами решения профессиональных задач.

Предмет курса «Программно-аппаратные средства защиты информации» - механизмы и практические методы защиты информации в компьютерах. Изучение дисциплины «Программно-аппаратные средства защиты информации» должно способствовать воспитанию у них профессиональной компетентности и профессионального кругозора, умению ориентироваться в продуктах и тенденциях развития средств защиты информационных технологий.

Целью дисциплины является приобретение студентами знаний, навыков и умений, связанных с правовыми и программно-техническими проблемами защиты информации государственных и негосударственных организаций и учреждений, осуществляющих взаимодействие и обмен данными посредством электронных коммуникаций.

Основными задачами дисциплины являются:

ознакомить будущих специалистов с проблемными вопросами, решаемыми в области защиты компьютерной информации

показать роль современных программно-аппаратных средств защиты информации в обеспечении ее целостности конфиденциальности и доступности

показать необходимость усвоения знаний о методах и средствах защиты компьютерной информации

осветить круг вопросов касающихся персональной ответственности должностных лиц за обеспечение безопасности информации, обрабатываемой в современных компьютерных системах

создать условия для качественного овладения студентами теоретическими знаниями и практическими навыками при решении типовых задач по обеспечению безопасности информационных технологий

подготовить студентов для самостоятельного использования полученных знаний для правильного выбора решений при применении комплексных систем защиты компьютерной информации.

1.2 Требования к уровню освоения содержания дисциплины

В результате обучения студенты должны овладеть следующими

компетенциями:

ОК 1. Понимать сущность и социальную значимость своей будущей профессии, обладать высокой мотивацией к выполнению профессиональной деятельности в области обеспечения информационной безопасности.

ОК 2. Организовывать собственную деятельность, выбирать типовые методы и способы выполнения профессиональных задач, оценивать их эффективность и качество.

ОК 3. Принимать решения в стандартных и нестандартных ситуациях и нести за них ответственность.

ОК 4. Осуществлять поиск и использование информации, необходимой для эффективного выполнения профессиональных задач, профессионального и личностного развития.

ОК 5. Использовать информационно-коммуникационные технологии в профессиональной деятельности.

ОК 6. Работать в коллективе и команде, эффективно общаться с коллегами, руководством, потребителями.

ОК 7. Брать на себя ответственность за работу членов команды (подчиненных), результат выполнения заданий.

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

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

ОК 10. Применять математический аппарат для решения профессиональных задач.

ОК 11. Оценивать значимость документов, применяемых в профессиональной деятельности.

ОК 12. Ориентироваться в структуре федеральных органов исполнительной власти, обеспечивающих информационную безопасность.

ПК 3.1. Применять программно-аппаратные и технические средства защиты информации на защищаемых объектах.

ПК 3.2. Участвовать в эксплуатации систем и средств защиты информации защищаемых объектов.

ПК 3.3. Проводить регламентные работы и фиксировать отказы средств защиты.

ПК 3.4. Выявлять и анализировать возможные угрозы информационной безопасности объектов.

В результате изучения дисциплины студенты должны:

иметь представление:

- об основных направлениях и перспективах развития программно-аппаратных средств защиты информации и управления правами использования информационных ресурсов при передаче конфиденциальной информации по каналам связи, установлении подлинности передаваемых сообщений, хранении информации (документов, баз данных), встраивании скрытой служебной информации.

знать и уметь использовать:

- возможные действия злоумышленника, направленные на нарушение политики безопасности информации;
- наиболее уязвимые для атак противника элементы компьютерных систем;
- механизмы решения типовых задач защиты информации.
- применять штатные средства защиты и специализированные продукты для решения типовых задач;
- квалифицированно оценивать область применения конкретных механизмов защиты;
- грамотно использовать аппаратные средства защиты при решении практических задач.

владеть:

- методами организации защиты информации в компьютерных системах с помощь, программно-аппаратных средств;
- методами анализа механизмов реализации методов защиты конкретных объектов и процессов для решения профессиональных задач;

иметь опыт (навык):

- освоения и внедрения новых систем защиты, сопровождения систем защиты.

Фундаментальность подготовки студентов по дисциплине обеспечивается рассмотрением основополагающих вопросов обеспечения защиты компьютерной информации при решении задач сбора, обработки, хранения и использования информационных ресурсов представленных в электронном виде.

Прикладная направленность дисциплины базируется на решении задач, связанных с будущей профессиональной деятельностью студентов.

Формирование личностных результатов воспитательной работы обучающихся

ЛР 1. Осознающий себя гражданином и защитником великой страны.

ЛР2.Проявляющий активную гражданскую позицию, демонстрирующий

иверженность принципам честности, порядочности, открытости, экономической активности

частвующий в студенческом и территориальном самоуправлении, в том числе на условиях

бровольчества, продуктивно взаимодействующий и участвующий в деятельности

щественных организаций.

ЛР3.Соблюдающий нормы правопорядка, следующий идеалам гражданского общества, еспечения безопасности, права и свобод граждан России. Лояльный к установкам и оявлениям представителей субкультур, отличающий их от групп с деструктивным и виантным поведением. Демонстрирующий неприятие и предупреждающий социально асное поведение окружающих.

ЛР4. Проявляющий и демонстрирующий уважение к людям труда, осознающий нность собственного труда. Стремящийся к формированию в сетевой среде личностно и офессионального конструктивного «цифрового следа».

ЛР5.Демонстрирующий приверженность к родной культуре, исторической памяти на нове любви к Родине, родному народу, малой родине, принятию традиционных ценностей огонационального народа России.

ЛР6. Проявляющий уважение к людям старшего поколения и готовность к участию в циальной поддержке и волонтерских движениях.

ЛР7. Осознающий приоритетную ценность личности человека; уважающий собственную ружую уникальность в различных ситуациях, во всех формах и видах деятельности.

ЛР8. Проявляющий и демонстрирующий уважение к представителям различных юкультурных, социальных, конфессиональных и иных групп. Сопричастность к сохранению, еумножению и трансляции культурных традиций и ценностей многонационального ссийского государства.

ЛР9. Соблюдающий и пропагандирующий правила здорового и безопасного образа зни, спорта; предупреждающий либо преодолевающий зависимости от алкоголя, табака, ихоактивных веществ, азартных игр и т.д. Сохраняющий психологическую устойчивость в гуативно сложных или стремительно меняющихся ситуациях.

ЛР10. Заботящийся о защите окружающей среды, собственной и чужой безопасности, в м числе цифровой.

ЛР11. Проявляющий уважение к эстетическим ценностям, обладающий основами стетической культуры.

ЛР12. Принимающий семейные ценности, готовый к созданию семьи и воспитанию детей; демонстрирующий неприятие насилия в семье, ухода от родительской ответственности, отказа от отношений со своими детьми и их финансового содержания

2 Структура и содержание учебной дисциплины

2.1 Объем дисциплины и виды учебной работы

Дисциплина ПАЗИ изучается в седьмом и восьмом семестрах в объеме 418 часов, из них с преподавателем – 280 часа.

Вид учебной работы и формы контроля	Дневная форма обучения		
	всего часов	Семестр 5	Семестр 6
Занятия на лекциях,уроках	140	60	80
Практич.зан., семинары	110	60	50
Курсовая работа	30		30
Самостоятельная работа	138	60	78
Вид итогового контроля	Диф зачет		Диф зачет

2.2 Тематический план и содержание учебной дисциплины

Наименование разделов и тем	Содержание учебного материала, практические занятия, самостоятельная работа обучающихся	Объем часов	Уровень освоения.
Тема 1. Программно-аппаратные средства разграничения доступа к компьютерной информации.	Введение. Программно-аппаратные средства разграничения доступа к компьютерной информации.	30	Репродуктивный. Продуктивный.
	Практические занятия	30	
	Самостоятельная работа	30	
	Всего	90	
Тема 2. Программно-аппаратные средства криптографической защиты информации.	Программно-аппаратные средства криптографической защиты информации.	30	Репродуктивный. Продуктивный.
	Практические занятия	30	
	Самостоятельная работа	30	
	Всего	90	
Всего за 5 семестр		180	
Тема 3. Программно-аппаратные средства защиты программного обеспечения от копирования и изучения.	Программно-аппаратные средства защиты программного обеспечения от копирования и изучения.	40	Репродуктивный. Продуктивный.
	Практические занятия	24	

Наименование разделов и тем	Содержание учебного материала, практические занятия, самостоятельная работа обучающихся	Объем часов	Уровень освоения.
	Курсовая работа	12	
	Самостоятельная работа	34	
	Всего	110	
Тема 4. Программно-аппаратная защита компьютерной информации от разрушающих программных воздействий.	Программно-аппаратная защита компьютерной информации от разрушающих программных воздействий. Заключение.	40	Репродуктивный. Продуктивный.
	Практические занятия	26	
	Самостоятельная работа	44	
	Курсовая работа	18	
	Всего	128	
Всего за 6 семестр		238	
Итого по курсу		418	

2.3 Образовательные технологии

Образовательные технологии, используемые при реализации различных видов учебной работы и дающие наиболее эффективные результаты освоения дисциплины.

В соответствии с требованиями ФГОС СПО по специальности реализация компетентностного подхода должна предусматривать широкое использование в учебном процессе активных и интерактивных форм проведения занятий (компьютерных симуляций, деловых и ролевых игр, разбор конкретных ситуаций, психологические и иные тренинги и т.д.) в сочетании с внеаудиторной работой с целью формирования и развития требуемых компетенций обучающихся.

Виды образовательных технологий.

Образовательная технология – это совокупность научно и практически обоснованных методов и инструментов для достижения запланированных

результатов в области образования. Применение конкретных образовательных технологий в учебном процессе определяется спецификой учебной деятельности, ее информационно-ресурсной основы и видов учебной работы.

1. Традиционные образовательные технологии ориентируются на организацию образовательного процесса, предполагающую прямую трансляцию знаний от преподавателя к студенту (преимущественно на основе объяснительно-иллюстративных методов обучения). Учебная деятельность студента носит в таких условиях, как правило, репродуктивный характер.

Примеры форм учебных занятий с использованием традиционных технологий:

Лекция – последовательное изложение материала в дисциплинарной логике, осуществляемое преимущественно вербальными средствами (монолог преподавателя).

Семинар – беседа преподавателя и студентов, обсуждение заранее подготовленных сообщений, проектов по каждому вопросу плана занятия с единым для всех перечнем рекомендуемой обязательной и дополнительной литературы.

Практическое занятие – занятие, посвященное освоению конкретных умений и навыков по предложенному алгоритму.

Лабораторная работа – организация учебной работы с реальными материальными и информационными объектами, экспериментальная работа с аналоговыми моделями реальных объектов.

2. Технологии проблемного обучения – организация образовательного процесса, которая предполагает постановку проблемных вопросов, создание 20 учебных проблемных ситуаций для стимулирование активной познавательной деятельности студентов.

Примеры форм учебных занятий с использованием технологий проблемного обучения:

Проблемная лекция – изложение материала, предполагающее постановку проблемных и дискуссионных вопросов, освещение различных научных подходов,

авторские комментарии, связанные с различными моделями интерпретации изучаемого материала.

Практическое занятие в форме практикума – организация учебной работы, направленная на решение комплексной учебно-познавательной задачи, требующей от студента применения как научно-теоретических знаний, так и практических навыков.

Практическое занятие на основе кейс-метода («метод кейсов», «кейс-стади») – обучение в контексте моделируемой ситуации, воспроизводящей реальные условия научной, производственной, общественной деятельности. Обучающиеся должны проанализировать ситуацию, разобраться в сути проблем, предложить возможные решения и выбрать лучшее из них. Кейсы базируются на реальном фактическом материале или же приближены к реальной ситуации.

3. Игровые технологии – организация образовательного процесса, основанная на реконструкции моделей поведения в рамках предложенных сценарных условий.

Примеры форм учебных занятий с использованием игровых технологий:

Деловая игра – моделирование различных ситуаций, связанных с выработкой и принятием совместных решений, обсуждением вопросов в режиме «мозгового штурма», реконструкцией функционального взаимодействия в коллективе и т.п.

Ролевая игра – имитация или реконструкция моделей ролевого поведения в предложенных сценарных условиях.

4. Технологии проектного обучения – организация образовательного процесса в соответствии с алгоритмом поэтапного решения проблемной задачи или выполнения учебного задания. Проект предполагает совместную учебно-познавательную деятельность группы студентов, направленную на выработку концепции, установление целей и задач, формулировку ожидаемых результатов, определение принципов и методик решения поставленных задач, планирование хода работы, поиск доступных и оптимальных ресурсов, поэтапную реализацию плана работы, презентацию результатов работы, их осмысление и рефлексию.

Основные типы проектов:

Исследовательский проект – структура приближена к формату научного исследования (доказательство актуальности темы, определение научной проблемы, предмета и объекта исследования, целей и задач, методов, источников, выдвижение гипотезы, обобщение результатов, выводы, обозначение новых проблем).

Творческий проект, как правило, не имеет детально проработанной структуры; учебно-познавательная деятельность студентов осуществляется в рамках рамочного задания, подчиняясь логике и интересам участников проекта, жанру конечного результата (газета, фильм, праздник и т.п.).

Информационный проект – учебно-познавательная деятельность с ярко выраженной эвристической направленностью (поиск, отбор и систематизация информации о каком-то объекте, ознакомление участников проекта с этой информацией, ее анализ и обобщение для презентации более широкой аудитории).

5. Интерактивные технологии – организация образовательного процесса, которая предполагает активное и нелинейное взаимодействие всех участников, достижение на этой основе личностно значимого для них образовательного результата. Наряду со специализированными технологиями такого рода принцип интерактивности прослеживается в большинстве современных образовательных технологий. Интерактивность подразумевает субъект-субъектные отношения в ходе образовательного процесса и, как следствие, формирование саморазвивающейся информационно-ресурсной среды.

Примеры форм учебных занятий с использованием специализированных интерактивных технологий:

лекция «обратной связи» – лекция–провокация (изложение материала с заранее запланированными ошибками),

лекция-беседа,

лекция-дискуссия,

семинар-дискуссия – коллективное обсуждение какого-либо спорного вопроса, проблемы, выявление мнений в группе.

6. Информационно-коммуникационные образовательные технологии – организация образовательного процесса, основанная на применении

специализированных программных сред и технических средств работы с информацией.

Примеры форм учебных занятий с использованием информационно-коммуникационных технологий:

Лекция-визуализация – изложение содержания сопровождается презентацией (демонстрацией учебных материалов, представленных в различных знаковых системах, в т.ч. иллюстративных, графических, аудио- и видеоматериалов).

Практическое занятие в форме презентации – представление результатов проектной или исследовательской деятельности с использованием специализированных программных сред.

Удельный вес занятий, проводимых в интерактивных формах, определяется главной целью программы, особенностью контингента обучающихся и содержанием конкретных дисциплин, и в целом в учебном процессе они должны составлять не менее определенного процента от всего объема аудиторных занятий.

Технологии, используемые при формировании образовательных компетенций приведены в таблице 1.

Таблица 1 - Технологии формирования ОК

Название ОК ПК	Технология формирования ОК (на учебных занятиях)
ОК 1. Понимать сущность и социальную значимость своей будущей профессии, обладать высокой мотивацией к выполнению профессиональной деятельности в области обеспечения информационной безопасности.	Технология «публичная презентация проекта» (представление содержания, выделение и иллюстрация сообщения)
ОК 2. Организовывать собственную деятельность, выбирать типовые методы и способы выполнения профессиональных задач, оценивать их эффективность и качество.	Технология развития критического мышления (групповое обсуждение проблемных вопросов, выполнение творческих заданий, учебная дискуссия)
ОК 3. Принимать решения в стандартных и нестандартных	Технология электронных образовательных ресурсов (умение ориентироваться в специальной

ситуациях и нести за них ответственность.	юридической литературе – работа с нормативно-правовыми актами)
ОК 4. Осуществлять поиск и использование информации, необходимой для эффективного выполнения профессиональных задач, профессионального и личностного развития.	Технология электронных образовательных ресурсов (работа с информационно-справочной правовая системой «ГАРАНТ» и информационно-справочная правовая система «КОНСУЛЬТАНТ-ПЛЮС».
ОК 5. Использовать информационно-коммуникационные технологии в профессиональной деятельности.	Технология «Деловая игра» (обучение коллективной мыслительной и практической работе, формирование умений и навыков социального взаимодействия и общения, навыков индивидуального и совместного принятия решений; воспитание ответственного отношения к делу, уважения к социальным ценностям и установкам коллектива и общества в целом).
ОК 6. Работать в коллективе и команде, эффективно общаться с коллегами, руководством, потребителями.	Технология «Творческое задание» (подборка примеров из практики; подборка материала по определенной проблеме; участие в ролевой игре)
ОК 7. Брать на себя ответственность за работу членов команды (подчиненных), результат выполнения заданий.	Технология «Анализ конкретных ситуаций» (выявление проблемы; поиск причин возникновения проблемы; анализ проблемы с использованием теоретических конструкций; анализ положительных и отрицательных последствий решения проблемы; обоснование лучшего варианта решения проблемы).
ОК 8. Самостоятельно определять задачи профессионального и личностного развития, заниматься самообразованием, осознанно планировать повышение квалификации.	Технология «Творческое задание» (подборка примеров из практики; подборка материала по определенной проблеме; участие в ролевой игре)
ОК 9. Ориентироваться в условиях частой смены технологий в профессиональной деятельности.	Технология «Деловая игра» (обучение коллективной мыслительной и практической работе, формирование умений и

	навыков социального взаимодействия и общения, навыков индивидуального и совместного принятия решений; воспитание ответственного отношения к делу, уважения к социальным ценностям и установкам коллектива и общества в целом).
ОК 10. Применять математический аппарат для решения профессиональных задач.	Технология «Творческое задание» (подборка примеров из практики; подборка материала по определенной проблеме; участие в ролевой игре)
ОК 11. Оценивать значимость документов, применяемых в профессиональной деятельности.	Технология «Анализ конкретных ситуаций» (выявление проблемы; поиск причин возникновения проблемы; анализ проблемы с использованием теоретических конструкций; анализ положительных и отрицательных последствий решения проблемы; обоснование лучшего варианта решения проблемы).
ОК 12. Ориентироваться в структуре федеральных органов исполнительной власти, обеспечивающих информационную безопасность.	Технология «Анализ конкретных ситуаций» (выявление проблемы; поиск причин возникновения проблемы; анализ проблемы с использованием теоретических конструкций; анализ положительных и отрицательных последствий решения проблемы; обоснование лучшего варианта решения проблемы).

3 Условия реализации программы дисциплины

3.1 Требования к минимальному материально-техническому обеспечению

Аппаратное обеспечение

1. Компьютерный класс с развернутой ЛВС на базе ПЭВМ типа IBM PC (процессор Intel Pentium (Celeron) не ниже 1500 МГц, ОЗУ не менее 512 Mb RAM, HDD не менее 30 Gb), подключенной к ИВС ОП (Internet) из расчета одна ПЭВМ на одного обучаемого;

2. Принтер (плоттер) для печати на бумаге формата А4.

Программное обеспечение

1. Операционные системы - Unix, МСВС 3.0, MS Windows 7/9/XP.

2. Офисные программы Microsoft Office, Libre Office.

3. Антивирусные программные средства Doctor Web for Windows и антивирус Касперского.

4. Программные средства криптографической защиты CriptonLite и PGP 7.0.

5. Digital Security Office (Кондор, Гриф)

Лекционное оборудование.

1. LCD-проектор.
2. Экран

3.2 Информационное обеспечение обучения

Рекомендуемая литература
Основная

1. Башлы, П. Н. Информационная безопасность и защита информации [Электронный ресурс] : Учебник / П. Н. Башлы, А. В. Бабаш, Е. К. Баранова. - М.: РИОР, 2013. - 222 с. / Режим доступа: http://znanium.com/catalog.php?bookinfo=405000

2. Информационная безопасность компьютерных систем и сетей: Учебное пособие / В.Ф. Шаньгин. - М.: ИД ФОРУМ: ИНФРА-М, 2017. - 416 с. / Режим доступа: http://znanium.com/catalog.php?bookinfo=775200

3. Криптографические методы защиты информации. Том 3: Учебно-методическое пособие / А.В. Бабаш. - 2-е изд. - М.: ИЦ РИОР: НИЦ ИНФРА-М, 2014. - 216 с. / Режим доступа: http://znanium.com/catalog.php?bookinfo=432654

4. Программно-аппаратная защита информации: Учебное пособие / П.Б. Хорев. - 2-е изд., испр. и доп. - М.: Форум: НИЦ ИНФРА-М, 2015. - 352 с. / Режим доступа: http://znanium.com/catalog.php?bookinfo=489084

5. Комплексная защита информации в корпоративных системах: Учебное пособие / В.Ф. Шаньгин. - М.: ИД ФОРУМ: НИЦ ИНФРА-М, 2017. - 592 с. / Режим доступа: http://znanium.com/catalog.php?bookinfo=546679

Дополнительная

1. Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации. Руководящий документ Гостехкомиссии России. - М.: ГТК РФ, 2020.
2. Программно-аппаратная защита информации: учебное пособие / П.Б. Хорев. - М.: Форум, 2019. - 352 с.
3. Шаньгин, В. Ф. Защита компьютерной информации. Эффективные методы и средства [Электронный ресурс] / В. Ф. Шаньгин. - М.: ДМК Пресс, 2020. - 544 с.
4. Информационная безопасность: Учебное пособие для студентов учреждений среднего проф. обр. / Т.Л. Партыка, И.И. Попов. - 3-е изд., перераб. и доп. - М.: Форум, 2019. - 432 с.
5. Ахмад, Д. М. Защита от хакеров корпоративных сетей [Электронный ресурс] / Дэвид М. Ахмад, Идо Дубравский, Хал Флинн и др.; пер. с англ. А. А. Петренко. - 2-ое изд. - М.: Компания АйТи; ДМК-Пресс, 2019. - 864 с.
6. Барнс, К. Защита от хакеров беспроводных сетей [Электронный ресурс] / Кристиан Барнс, Тони Боутс, Дональд Лойд и др.; пер. с англ. А. В. Семенова. - М.: Компания АйТи; ДМК Пресс, 2021. - 480 с.
7. Алферов А.П., Зубов А.Ю. и др. Основы криптографии: Учеб. пособие, 2-е изд.,испр. и доп. М.: Гелиос АРВ, 2021.- 480 с: ил.
8. Б. Шнайер. Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си.- М.: Издательство Триумф, 2020.- 816 с: ил.
9. Баранова, Е. К. Основы информатики и защиты информации [Электронный ресурс] : Учеб. пособие / Е. К. Баранова. - М. : РИОР : ИНФРА-М, 2020. - 183 с.
10. Башлы, П. Н. Информационная безопасность и защита информации [Электронный ресурс] : Учебник / П. Н. Башлы, А. В. Бабаш, Е. К. Баранова. - М.: РИОР, 2021. - 222 с.
11. Введение в криптографию / Под ред. В.В. Ященко СПб.: Питер, 2021.-288 с: ил.
12. Вильям Столлингс Криптографическая защита сетей. – М.: Издательсткий дом “Вильямс”, 2020.
13. Гайкович В., Першин А. Безопасность электронных банковских систем. М., 2019.
14. Галатенко В.В. Основы информационной безопасности /Галатенко В.В. Под редакцией члена-корреспондента РАН В.Б. Бетелина /М.: ИНТУИТ.РУ «Интернет-университет» 2019, - 280 с.
15. Герасименко В.А. Защита информации в автоматизированных системах обработки данных. В 2-х кн. - М.: Энергоатомиздат, 2019.
16. ГОСТ 28147-89. Системы обработки информации. Защита криптографическая. Алгоритмы криптографического преобразования.
17. ГОСТ 34.10-94. Информационная технология. Криптографическая защита информации. Процедуры выработки и проверки электронной цифровой подписи на базе асимметричного криптографического алгоритма.

Интернет-ресурсы:

1. http://www.znanium.com
2. http://www.citforum.ru

3.3 Методические указания для обучающихся по освоению учебной дисциплины

В соответствии с задачами дисциплины определена структура и последовательность изучения разделов и тем. Изучение курса осуществляется в форме лекций и практических занятий.

На лекциях систематизируются знания студентов по вопросам изучения информационных ресурсов менеджмента, систем управления информационными ресурсами и обработки информации.

Тема 1. Введение. Программно-аппаратные средства разграничения доступа к компьютерной информации.

Введение. Цели и задачи дисциплины. Основные понятия и определения в области защиты компьютерной информации. Современная ситуация в области защиты компьютерной информации. Основы защиты компьютерной информации от несанкционированного доступа. Основные термины и определения в области защиты компьютерной информации от НСД. Основные принципы и направления защиты от НСД. Формальные модели управления доступом. Понятие идентификации и аутентификации субъекта. Алгоритмы аутентификации пользователей.

Секретная информация, используемая для контроля доступа: ключи и пароли. Злоумышленник и ключи. Классификация средств хранения ключей и идентифицирующей информации. Магнитные диски прямого доступа. Магнитные и интеллектуальные. Средство TouchMemory.

Тема 2. Программно-аппаратные средства криптографической защиты информации.

Роль и место криптографических методов и средств в обеспечении безопасности компьютерной информации. Основные понятия и процедуры технологии управления криптографическими ключами. Аппаратные и программно-аппаратные средства криптозащиты данных. Построение аппаратных компонент криптозащиты данных, специализированные СБИС как носители алгоритма шифрования. Защита алгоритма шифрования; принцип чувствительной области и принцип главного ключа. Необходимые и достаточные функции аппаратного средства криптозащиты. Секретная информация, используемая для контроля доступа: ключи и пароли.

Тема 3. Программно-аппаратные средства защиты программного обеспечения от копирования и изучения.

Несанкционированное копирование программ как тип НСД. Юридические аспекты несанкционированного копирования программ. Общее понятие зашиты от копирования. Разновидности задач защиты от копирования. Привязка ПО к аппаратному окружению и физическим носителям как единственное средство защиты от копирования ПО. Привязка программ к гибким магнитным дискам (ГМД). Привязка программ к жестким магнитным дискам (ЖМД). Особенности привязки к ЖМД. Виды меток на ЖМД. Привязка к прочим компонентам штатного оборудования ПЭВМ. Привязка к внешним (добавляемым) элементам ПЭВМ. Привязка к портовым ключам. Использование дополнительных плат расширения. Методы "водяных знаков" и методы "отпечатков пальцев".

Понятие изучения и обратного проектирования ПО. Цели и задачи изучения работы ПО. Способы изучения ПО: статическое и динамическое изучение. Роль программной и аппаратной среды. Временная надежность (невозможность обеспечения гарантированной надежности). Защита от отладки. Динамическое преобразование кода. Принцип ловушек и избыточного кода. Защита от дизассемблирования. Принцип внешней загрузки файлов. Динамическая модификация программы. Защита от трассировки по прерываниям.

Тема 4 Программно-аппаратная защита компьютерной информации от разрушающих программных воздействий. Заключение.

Защита от разрушающих программных воздействий. Вирусы как особый класс разрушающих программных воздействий. Необходимые и достаточные условия недопущения разрушающего воздействия. Понятие изолированной программной среды. Программные средства антивирусной защиты: основные характеристики, принципы построения и применения.

3.4 Методические указания к лабораторным занятиям

Лабораторных занятий не предусмотрено.

3.5 Методические указания к практическим занятиям

На практических занятиях материалы лекций конкретизируются, закрепляются знания, полученные студентами в процессе самостоятельной работы, получаются практические навыки в решении стандартных и нестандартных прикладных задач.

3.5.1 Тематика практических занятий по дисциплине

Тема 1. Введение. Программно-аппаратные средства разграничения доступа к компьютерной информации.

Сравнительный анализ понятийных аппаратов различных источников в области защиты информации». Знакомство с программным комплексом «Secret Net 5.0». Изучение свойств и возможностей программного комплекса «Secret Net 5.0». Исследование возможностей системы безопасности Windows XP по разграничению полномочий пользователей. «Формирование политики безопасности парольной системы аутентификации»

Тема 2. Программно-аппаратные средства криптографической защиты информации.

Исследование особенностей криптографической защиты информации при применении классических шифров замены. Применение алгоритма криптографической защиты ГОСТ28147-89. Шифрующая файловая система EFS в Windows XP. Программный комплекс Криптон. Знакомство с программным комплексом Криптон. Программный комплекс Крипто-АРМ. Знакомство с программным комплексом Крипто-АРМ

Тема 3. Программно-аппаратные средства защиты программного обеспечения от копирования и изучения.

Защита CD или DVD дисков от копирования с помощью программного средства WildCDProtector. Ознакомиться с методом защиты путём создания оболочки диска. Описать основные свойства, преимущества и недостатки программ и разработок компании Protection Technology, обеспечивающих защиту дисков

Тема 4 Программно-аппаратная защита компьютерной информации от разрушающих программных воздействий. Заключение.

Проверка потенциальных мест записи вредоносного программного обеспечения в системном реестре операционной системы Windows 2000 (XP). Формирование политики защиты от макровирусов при использовании приложения Microsoft Word (из пакета Office XP). Антивирусное средство DrWeb. Изучение функциональных возможностей антивирусного средства DrWeb. Применение средства для обнаружения программ-шпионов SUPERAntiSpyware.

3.5.2 Методические указания по выполнению практических работ по дисциплине

Практические работы имеют целью углубить и закрепить полученные теоретические знания, обучить студентов методам экспериментальных и научных исследований, привить навыки анализа и обобщения полученных результатов,

навыки работы с инструментальными средствами управления информационной безопасностью.

К выполнению практических работ допускаются студенты, уяснившие тему, цель, содержание работы, правила техники безопасности и эксплуатации ПЭВМ и знающие теоретический материал по теме практической работы.

При подготовке к очередной практической работе необходимо:

1. Изучить правила техники безопасности и правила технической эксплуатации ПЭВМ и программы в соответствии с задание на практическое занятие.

2. Подготовить бланк отчета по практической работе, куда занести тему, цель работы, ее содержание, состав и назначение применяемых для измерений приборов, а также таблицы наблюдений измеряемых величин.

3. Подготовиться к индивидуальному собеседованию по вопросам, указанным в описании практической работы.

По выполнении практической работы студенты представляют отчет и защищают его.

Примечания:

1. Отчет должен быть представлен и защищен в срок, не позднее семи дней со дня выполнения данной практической работы учебной группой.

2.Студенты, не выполнившие практические работы, обязаны самостоятельно их выполнить, предварительно согласовав дату и время выполнения с инженером лаборатории, но не позднее, чем в десятидневный срок.

3. Индивидуально оформленные бланки отчетов по практической работе представляются старшим учебной бригады, состоящей из 3 – 4 студентов за всю бригаду инженеру лаборатории или преподавателю для последующей проверки полноты и правильности выполнения объема практической работы. В отчете у старшего учебной бригады должен быть листок с рабочими материалами (черновик) практической работы, обязательно подписанный инженером лаборатории.

СОДЕРЖАНИЕ И ОФОРМЛЕНИЕ ОТЧЕТА

Отчет должен содержать:

- тему, цель, задание по практической работе;
- содержание работы;
- отчет, сформированный соответствующей программой;
- выводы по проделанной работе;
- ответы на контрольные вопросы.

Отчет оформляется черным или синим цветом на листах формата А4 с вычерчиванием необходимых схем в соответствии с требованиями ЕСКД. Допускается выполнение отчета по лабораторной работе в электронном виде с представлением результатов в папке «Выполненные задания» под своей фамилией.

3.5.3 Правила техники безопасности при работе на ПЭВМ

Каждый студент обязан знать и неукоснительно выполнять основные требования правил техники безопасности и расписаться за их изучение.

К самостоятельной работе в классе ПЭВМ допускаются лица, прошедшие инструктаж по технике безопасности.

Общие требования:

1. К работе на ПЭВМ, не связанной с их обслуживанием, допускаются лица, имеющие первую квалификационную группу, обученные безопасным методам работы с ПЭВМ, а также прошедшие проверку знаний и периодический инструктаж.

2. ПЭВМ должны удовлетворять следующим основным требованиям:

а) быстро включаться и отключаться от электросети (но не самопроизвольно);

б) быть безопасными в работе и иметь недоступные для случайного прикосновения токоведущие части;

в) подключаться к розетке оборудованной дополнительной заземляющей жилой или иметь заземленный корпус.

Перед началом работы на ПЭВМ необходимо проверить:

1. Состояние сетевого кабеля, целостность изоляции, отсутствие излома жил, надежность крепления сетевой вилки.

2. Исправность заземления, защитных отключающих устройств.

При обнаружении каких-либо неисправностей работа на ПЭВМ должна быть немедленно прекращена и об этом доложено преподавателю или инженеру или технику лаборатории.

Во время работы на ПЭВМ запрещается:

1. Начинать работу на ПЭВМ без прохождения инструктажа по мерам безопасности при работе с ПЭВМ.

2. Включать ПЭВМ без разрешения преподавателя.

3. Самостоятельно (без согласия преподавателя) изменять что-либо в схеме или удалять какие-либо файлы в директории с установленной программой.

4. Без разрешения начальника лаборатории, инженера или техника переносить с места на место системные блоки, мониторы, другие комплектующие ПЭВМ и периферийные устройства.

5. Снимать защитный кожух системного блока и монитора и производить самим какой-либо ремонт (как ПЭВМ, так и другого оборудования, разного рода кабелей и т.п.).

6. Держать сетевой кабель, касаться открытых токонесущих элементов, касаться одновременно корпуса ПЭВМ (металлических частей периферийных устройств) и заземляющего провода.

7. Подключать к работающей ПЭВМ и отключать от нее периферийные устройства, проверять надежность подключенных кабелей.

8. Касаться сетевых терминаторов и коннекторов обнаженными частями тела, подключать и вынимать их из разъемов сетевых карт.

9. Разбирать силовые розетки, помещать в них посторонние предметы.

3.5.4 Тематика рефератов, докладов эссе

Номер темы	ТЕМЫ ДЛЯ РЕФЕРИРОВАНИЯ
1.	Электронная цифровая подпись (ЭЦП). Общие положения по формированию и применению ЭЦП.
2.	Математические основы и базовые процедуры формирования электронной цифровой подписи в соответствии с ГОСТ Р 34.10. 2001
3.	Современные программно-аппаратные средства защиты от несанкционированного доступа к программной среде (например, Система защиты информации «Secret Net»)
4.	Современные средства контроля и управления физическим доступом к компьютерной информации (например, программа контроля соблюдения правил работы на персональном компьютере «X-Files»)
5.	Современные средства защиты программ от несанкционированного копирования.
6.	Средства гарантированного уничтожения информации (например, Система гарантированного уничтожения информации СГУ-1).
7.	Средства анализа защищенности, реализуемые в современных компьютерных системах управления и обработки информации.
8.	Средства защиты информации при работе в сетях, реализующие технологию экранирования (межсетевые экраны)
9.	Средства защиты информации, построенные на основе технологии «туннелирования».
10.	Средства криптографической защиты информации при работе в сетях общего пользования (например, криптографический маршрутизатор «Crypton IP»).
11.	Средства криптографической защиты информации в компьютерах и локальных сетях (например, программно-аппаратный комплекс «ШИПКА»).
12.	Защищенные системы электронной почты и документооборота (например, Программно- аппаратный комплекс «Щит-почта Интернет»)
13.	Отечественные аппаратно-программные средства криптографической защиты компьютерной информации (например, криптографические средства семейства КРИПТОН)
14.	Современные алгоритмы реализации функции хеширования. Практические аспекты применения.
15.	Современные алгоритмы реализации электронной цифровой подписи. Практические аспекты применения.

Номер темы	ТЕМЫ ДЛЯ РЕФЕРИРОВАНИЯ
16.	Средства защиты информации от перехвата за счет побочных электромагнитных излучений и наводок (например, ПЭВМ в защищенном исполнении «Flagman-Z»).
17.	Средства радиомониторинга и контроля эффективности защиты информации от утечки по техническим каналам (например, Универсальный мобильный комплекс радиоконтроля «Патруль»)
18.	Характеристика современных средств идентификации и аутентификации пользователей (например, Комплекс программно-аппаратных средств контроля доступа к ПЭВМ "Рубеж").
19.	Основы построения систем аутентификации с использованием интеллектуальных карт (smart card)
20.	Современные средства защиты информации от компьютерных вирусов.
21.	Современные средства защиты компьютерной информации от программных закладок.
22.	Средства реализации инфраструктуры открытых ключей (например, DEKART Certification Authority® - комплекс административных, технических и программных решений, позволяющих построить инфраструктуру защиты информации на основе открытых ключей)
23.	Комплексные системы защиты информации (например, Программный комплекс ViPNet).
24.	Системы централизованного управления корпоративной политикой безопасности (например, система SAFEsuite Decisions)

3.6 Методические указания к курсовому проектированию и другим видам самостоятельной работы

Методические указания к самостоятельной работе студентов по дисциплине программно-аппаратные средства защиты информации и сети разработаны на основе Федерального государственного образовательного стандарта среднего профессионального образования, по специальности 10.02.01 «Организация и технология защиты информации», утвержденного приказом Министерства образования и науки Российской Федерации от 28 июля 2014 г. No 805. Указания включают материал, необходимый для выполнения самостоятельной работы, требования к оформлению отчета по самостоятельное работе. Методические указания рассмотрены и одобрены Предметно-цикловой комиссией технического профиля.

Курсовое проектирование обеспечено методическими указаниями по выполнению курсовой работы по дисциплине программно-аппаратные средства защиты информации и разработаны на основе Федерального государственного образовательного стандарта среднего профессионального образования, по специальности 10.02.01 «Организация и технология защиты информации»,

утвержденного приказом Министерства образования и науки Российской Федерации от 28 июля 2014 г. No 804.

3.7 Программное обеспечение современных информационно-коммуникационных технологий

Преподавание и подготовка студентов предполагает использование стандартного программного обеспечения для персонального компьютера:

No п/п	Название технических и компьютерных средств обучения
1.	Операционная система Microsoft Windows 7
2.	Офисный пакет Microsoft Office Professional
3.	Пакет редактор диаграмм, блок-схем, планов и схем этажей, участков и т.п. MicrosoftVisio 2010.
4.	Пакет автоматизации календарного планирования Microsoft Project.
5.	Consultant Plus
6.	VirtualBox
7.	Digital Security Office
8.	браузеps для поиска информации по дисциплине в глобальной сети ИНТЕРНЕТ: MOZILLA FIREFOX, GOOGLE CHROME, OPERA, INTERNET EXPLORER

3.8 Условия реализации программы для обучающихся инвалидов и лиц с ограниченными возможностями здоровья

Для студентов из числа лиц с ограниченными возможностями здоровья обучение проводится Академией с учетом особенностей их психофизического развития, их индивидуальных возможностей и состояния здоровья .

При проведении обучения по дисциплине обеспечивается соблюдение следующих общих требований:

− проведение обучения для лиц с ограниченными возможностями здоровья в одной аудитории совместно со студентами, не имеющими ограниченных возможностей здоровья, если это не создает трудностей для них в процессе обучения;

− присутствие в аудитории ассистента, оказывающего обучающимся необходимую техническую помощь с учетом их индивидуальных особенностей

(занять рабочее место, передвигаться, прочитать и оформить задание, общаться с преподавателем);

− пользование необходимыми обучающимся техническими средствами при выполнении практических и других работ в соответствии с учебным планом с учетом их индивидуальных особенностей;

В зависимости от индивидуальных особенностей обучающихся с ограниченными возможностями здоровья образовательная среда Академии обеспечивает выполнение следующих требований при обучении и проведении промежуточной и итоговой аттестации:

а) для слепых:

− задания и иные материалы для аттестации зачитываются ассистентом;

− письменные задания надиктовываются обучающимся ассистенту;

б) для слабовидящих:

− задания и иные учебно-методические материалы оформляются увеличенным шрифтом;

− обеспечивается индивидуальное равномерное освещение не менее 300

− люкс;

− при необходимости обучающимся предоставляется увеличивающее устройство, допускается использование увеличивающих устройств, имеющихся у обучающихся;

в) для глухих и слабослышащих, с тяжелыми нарушениями речи:

− обеспечивается наличие звукоусиливающей аппаратуры коллективного пользования, при необходимости обучающимся предоставляется звукоусиливающая аппаратура индивидуального пользования;

− по их желанию аттестационные испытания проводятся в письменной форме;

г) для лиц с нарушениями опорно-двигательного аппарата (тяжелыми нарушениями двигательных функций верхних конечностей или отсутствием верхних конечностей):

− письменные задания надиктовываются ассистенту;

− по их желанию все аттестационные испытания проводятся в устной форме.

4 Контроль и оценка результатов освоения дисциплины

4.1 Примерные вопросы к зачету

1. Основные понятия и определения[1] в области защиты компьютерной информации.
2. Современная ситуация в области защиты компьютерной информации.
3. Требования к системам защиты информации.
4. Понятие угрозы безопасности компьютерной информации. Интервал потенциальной опасности.
5. Классификация угроз безопасности компьютерной информации.
6. Источники, риски и формы атак на информацию.
7. Принципы защиты компьютерной информации
8. Идентификация субъекта, понятие протокола идентификации, идентифицирующая информация;
9. Основные подходы к защите данных от НСД (контроль доступа и разграничение доступа, иерархический доступ к файлу).
10. Формальные модели управления доступом.
11. Классификация средств защиты компьютерной информации от НСД
12. Аутентификация пользователей. Основные алгоритмы (протоколы) аутентификации.
13. Администрирование сетей в аспекте безопасности информации
14. Защита сетевого файлового ресурса, фиксация доступа к файлам.
15. Доступ к данным со стороны процесса, способы фиксации факта доступа.
16. Надежность систем ограничения доступа;
17. Защита файлов от изменения;
18. Электронная цифровая подпись (ЭЦП);
19. Методы и средства ограничения доступа к компонентам ЭВМ;
20. Программно-аппаратные средства шифрования;
21. Построение аппаратных компонент криптозащиты данных;
22. Защита алгоритма шифрования.
23. Принцип чувствительной области и принцип главного ключа,
24. Пароли и ключи, организация хранения ключей;
25. Необходимые и достаточные функции аппаратного средства криптозащиты;
26. Защита программ от несанкционированного копирования;
27. Защита программ от изучения;
28. Защита программ от отладки, защита от дизассемблирования,
29. Защита программ от трассировки по прерываниям;
30. Защита от разрушающих программных воздействий (РПВ);
31. Компьютерные вирусы как особый класс РПВ;
32. Необходимые и достаточные условия недопущения разрушающего воздействия;

[1] выделенные элементы являются дидактическими единицами

33. Понятие изолированной программной среды.
34. Общая характеристика и классификация вредоносных программ.
35. Компьютерные вирусы. Классификация компьютерных вирусов.
36. Основы технологии анализа защищенности компьютерных систем управления и обработки информации.
37. Многоуровневая защита корпоративных сетей.

по материалам практических занятий:

1. Показать на примере повышение стойкости парольной системы идентификации на основе применения метода разделения знаний (пароля).
2. Продемонстрировать принцип аутентификации с нулевым разглашением на основе схемы Гиллоу-Куискуотера
3. Настроить параметры аутентификации Windows XP
4. Сформировать учетную запись с ограниченными правами и установить для нее пароль (операционная система Windows XP).
5. Произвести настройку брандмауэра Windows XP (добавить программу в список исключений по указанию преподавателя).
6. Установить режим работы с документами MS Word при котором запрещается бесконтрольная обработка всех макросов.
7. Установить парольную защиту на документ MS Word, предотвращающую несанкционированное изменение содержания документа.
8. Произвести зашифрование (расшифрование) сообщения (криптограммы) [метод и сообщение по указанию преподавателя]
9. Рассчитать требуемую мощность пространства паролей, обеспечивающую требуемый уровень надежности парольной защиты (данные по заданию преподавателя).
10. Проверить потенциальные места записей вредоносного программного обеспечения в системном реестре операционной системы Windows 2000 (XP) [Найдите ключ Userinit (REG_SZ) и проверьте его содержимое]
11. Активизировать механизма регистрации и аудита с помощью оснастки «Локальные политики безопасности» системы безопасности ОС Windows 2000 (XP).
12. Создать VPN-подключение средствами ОС Windows XP к узлу с адресом 122.122.122.122.

4.2 Тест по дисциплине

Рекомендации по проведению педагогических измерений при тестировании по дисциплине

Для проведения тестирования необходимо иметь следующий комплект материалов

1 .Инструкцию и бланк отчета о проведении тестирования;

2.Тест-билеты в количестве, равном списочному составу группы (плюс 1-2 билета);

3.Бланки для ответов в соответствии с количеством тестируемых (плюс 3-4 бланка);

4. Листы для черновиков

1.Начальный этап

В начале тестирования необходимо:

- Объяснить цель тестирования, указать количество заданий и время выполнения теста;
- Напомнить студентам, что использование каких-либо справочных материалов не допускается;
- Раздать бланки для ответов, листы для черновиков;
- Объяснить правила заполнения бланка для ответов и показать на доске пример такого заполнения. Напомнить, что основное требование при заполнении бланка - разборчивость сведений, поэтому делать записи лучше печатными буквами;
- Проверить правильность заполнения бланка для ответов каждым студентом;
- Напомнить студентам правила записи ответов в бланке (штриховка, запись номера или другие способы).

2.Основной этап

На этом этапе необходимо:

- Раздать билеты с заданиями, соблюдая принцип отличия вариантов у ближайших соседей;
- Зафиксировать время начала работы над тестом и указать момент ее окончания (эти отметки времени записать на доске);
- Проконтролировать проставление студентами в листе ответов номера полученного варианта тест-билета;
- Обеспечить самостоятельность работы студентов.

В процессе выполнения теста могут возникнуть ситуации, не предусмотренные процедурой тестирования. Все эти отклонения обязательно должны быть отражены в отчете.

Приведем некоторые из возможных ситуаций:

Некорректные вопросы. Вопросы тестируемых.

Если у кого-либо из студентов возникнут уточняющие вопросы или замечания по заданиям теста, то следует записать фамилию студента и кратко описать вопросы (замечания), указав номер варианта и задания. (Напоминаем, что ответы на вопросы не должны служить подсказкой для решения!)

Неверная запись ответов.

Иногда студент неправильно отмечает ответы в бланке для ответов или делает отметки в тест-билете. В этом случае студенту следует предложить заполнить новый бланк ответов, либо внести исправления в старый бланк. Любые исправления в листе ответов должны .быть заверены подписью .членов комиссии при необходимости дано краткое пояснение.

Инструкция по оценке заданий тест-билетов АПИМ

Ключи ответов

№	Вариант 1	Вариант 2
1	2	1
2	3	1
3	2	2
4	4	2
5	1	3
6	3	2
7	4	4
8	3	2
9	4	1
10	2	3
11	3	4
12	1	2
13	4	2
14	3	3
15	3	4
16	3	4
17	2	3
18	4	1
19	3	1
20	1	2
21	3	3
22	4	2
23	2	1
24	3	2
25	4	3
26	2	2
27	2	1
28	1	3
29	3	3
30	1	1
31	2	3
32	3	3
33	2	2
34	3	2
35	1	1

3. Завершение тестирования

По истечении времени тестирования следует собрать все материалы, провести их сортировку и заполнить отчет о проведении тестирования.

При сборе материалов необходимо еще раз ПРОВЕРИТЬ СООТВЕТСТВИЕ НОМЕРА ВАРИАНТА В БЛАНКЕ ОТВЕТОВ И ТЕСТ-БИЛЕТЕ

Для сбора материалов не следует привлекать студентов!

Сортировка материалов предполагает разделение на отдельные пачки тест-билетов, листов ответов и черновиков.

«Программно-аппаратные средства защиты информации»
Количество заданий в тест – билете: 35
Форма (формы) заданий тест – билетов: закрытая
Время выполнения тест – билета: 50 минут
Количество вариантов тест – билетов: 2
Реквизиты разработчика: к.т.н., доцент Чернуха Юрий Владимирович
Год разработки: 2013

ТЕСТ
по дисциплине «Программно-аппаратные средства защиты информации»

Вариант № 1

Указания:

Задания имеют разное количество вариантов ответа, из которых правильными могут быть как один, так и несколько вариантов. В листе ответа проставляются номера правильных ответов.

1. Сколько уровней возможностей нарушителей предоставляемых им штатными средствами КС предусмотрено классификацией в соответствии с РД ГТК (ФСТЭК)?

1. Один.
2. Два.
3. Три.
4. Четыре.
5. Пять.
6. Семь.

2. Схемы разграничения доступа в которых защитные механизмы встраиваются в каждый объект и осуществляют контроль в соответствии со отеками доступа данного объекта называются:

1. «Списковые» схемы (дискреционный доступ).
2. «Мандатные» схемы (мандатный доступ).
3. «Полномочные» схемы (полномочный доступ).

3. Документ «Служба директорий: обзор концепций, моделей и сервисов» относится к:

1. Оценочным стандартам
2. Техническим спецификациям
3. Руководящим документам ФСТЭК

4. В каком году был принят Стандарт Министерства обороны США «Критерии оценки доверенных компьютерных систем» (Trusted Computer System Evaliation Criteria, TCSEC)?

1. 1975
2. 1980
3. 1985

4. 1990

5. Каким стандартом было введено понятие: «Сетевая доверенная вычислительная база»?
1. Department of Defense Trusted Computer System Evaliation Criteria, TCSEC
2. Trusted Network Interpretation
3. ISO/IEC 15408-99
4. ГОСТ/ИСО МЭК 15408:2002

6. Какой стандарт называют «Оранжевой книгой»?
1. Стандарт Министерства обороны США «Критерии оценки доверенных компьютерных систем» (Department of Defense Trusted Computer System Evaliation Criteria, TCSEC)
2. Гармонизированные критерии Европейских стран" [европейские критерии]
3. Международный стандарт ISO/IEC 15408-99 «Критерии оценки безопасности информационных технологий» (Evaluation criteria for IT security)

1. Какой стандарт сокращенно называют «Общими критериями» (ОК)?
1. Стандарт Министерства обороны США «Критерии оценки доверенных компьютерных систем»
2. Международный стандарт ISO/IEC 15408-99
3. Британский стандарт BS 7799 «Управление информационной безопасностью. Практические правила»

4. Какое из перечисленных понятий было введено в Стандарте Министерства обороны США «Критерии оценки доверенных компьютерных систем» (Trusted Computer System Evaliation Criteria, TCSEC)?
1. Сервисы безопасности
2. Политика безопасности
3. Оценочные уровни доверия - ОУД

4. Международный стандарта ISO/IEC 15408-99 раскрывает (описывает):
1. Систематический подход к вопросам доступности, формирование архитектурных принципов ее обеспечения.
2. Различие между системами и продуктами информационных технологий, но для унификации требований вводится единое понятие - объект оценки
3. Критерии оценки безопасности информационных технологий

5. Как называется документ, в котором в целях добровольного многократного использования устанавливаются характеристики продукции, правила осуществления и характеристики процессов производства, эксплуатации, хранения, перевозки, реализации и утилизации, выполнения работ или оказания услуг?
1. Технические условия
2. Спецификация
3. Регламент
4. Стандарт

6. Цель создания политики информационной безопасности?
1. Для организационно-технической поддержки политики формирования и использования информационных ресурсов при осуществлении доступа к информации
2. Для защиты от внешних деструктивных воздействий
3. Для защиты от недобросовестных работников (пользователей)

7. Совокупность принципов, правил и рекомендаций, определяющих порядок организации защиты информации, обрабатываемой в конкретной компьютерной системе, зафиксированная документально называется:
1. Технической политикой безопасности компьютерной системы
2. Политикой информационной безопасности компьютерной системы
3. Стандарт безопасности компьютерной системы

8. Формулировка целей, которые преследует организация в области безопасности информации, определение общих направлений в достижении этих целей является составной частью:
1. Политики безопасности верхнего (правового и административного) уровня
2. Политики безопасности среднего (процедурного) уровня
3. Политики безопасности нижнего (программно-аппаратного) уровня
4. Нет правильного ответа

9. Контроль участников взаимодействия является ключевым моментом при составлении политики информационной безопасности:
1. Политики безопасности верхнего (правового и административного) уровня
2. Политики безопасности среднего (процедурного) уровня
3. Политики безопасности нижнего (программно-аппаратного) уровня
4. Нет правильного ответа

10. Список подчиненных политик безопасности является основой:
1. Acceptable use policies - AUP
2. Корневой политики безопасности
3. Политики формирования и использования информационных ресурсов

11. Совокупность требований и правил по информационной безопасности для объекта информационной безопасности, выработанных в соответствии с требованиями руководящих и нормативных документов в целях противодействия заданному множеству угроз информационной безопасности, с учетом ценности защищаемой информационной сферы и стоимости системы обеспечения информационной безопасности называется:
1. Стандарт безопасности
2. Политика информационной безопасности
3. Политика безопасности верхнего уровня
4. Корневая политика безопасности

12. В каком документе (разделе) политики безопасности отражается ответ на вопрос: «Существуют ли ограничения на установку ПО»?
1. Сертификате безопасности
2. Acceptable use policies - AUPS
3. Incident response plan - IRP
4. Password policy

13. Какой документ включает в себя следующие подразделы: политику формирования и использования информационных ресурсов, политику информационной безопасности и техническую политику?
1. Стандарт безопасности
2. Техническая спецификация
3. Информационная политика
4. Политика информационной безопасности
5. Политика использования информационных ресурсов

14. В политике безопасности какого уровня описывается отношение к передовым, но еще недостаточно проверенным технологиям защиты информации?
1. Правового и административного
2. Процедурного
3. Аппаратно-программного

15. Что определяет системная информационная политика?
1. Принципы, порядок и правила интеграции информационных ресурсов
2. Принципы, порядок и правила построения систем защиты информации
3. Принципы, порядок и правила разграничения доступа к информационным ресурсам

16. Как называется внешняя или внутренняя по отношению к атакуемой компьютерной системе программа, обладающая определенными деструктивными функциями по отношению к этой системе?
1. Компьютерный вирус
2. Программная закладка
3. Аппаратная закладка

17. Как называется несаморазмножающаяся программа, обеспечивающая злоумышленнику возможности несанкционированного доступа к защищаемой информации?
1. Компьютерный вирус
2. Ловушка
3. Люк
4. Логическая бомба

18. Какая из перечисленных функций не относится к программных закладкам?
1. Уничтожение информации
2. Самостоятельное распространение в компьютерных системах
3. Перехват и передача информации
4. Целенаправленная модификация кода программы

19. По какому признаку классифицируются «драйверные закладки»?
1. По методу внедрения
2. По принципу действия
3. По деструктивным последствиям

20. Какое из перечисленных воздействий не относится к моделям воздействия программных закладок?
1. Уборка мусора
2. Искажение
3. Наблюдение
4. Копирование
5. Перехват

21. К какому виду РПС относится «Клавиатурный шпион»
1. К программным закладкам
2. К вирусам
3. К бактериям

22. Какие из перечисленных свойств присущи компьютерным вирусам?
1. Способность к включению своего кода в тела других файлов и системных областей памяти компьютера

2. Способность к последующему самостоятельному выполнению и самовоспроизведению
3. Способность к самостоятельному распространению в КС
4. Все перечисленные свойства
5. Только 1 и 3 свойство
6. Только 2 и 3 свойство

23. Сотрудник Лехайского университета (США) Фред Коэн:
1. Впервые создал антивирус
2. Сделал сообщение о возможности существования компьютерных вирусов
3. Является создателем вируса-червя

24. В чем принципиальное отличие компьютерного вируса от программной закладки?
1. Сложностью написания
2. Возможностью деструктивного воздействия
3. Способностью к саморазмножению и модификации
4. Всеми вышеперечисленными свойствами

25. Как называются закладки, интерфейс которых, совпадает с интерфейсом некоторых служебных программ, требующих ввод конфиденциальной информации
1. Прикладные закладки
2. Исполняемые закладки
3. Закладки-имитаторы
4. Закладки-невидимки

26. По какому признаку вирус классифицируется как резидентный вирус?
1. По режиму функционирования
2. По объекту внедрения
3. По особенностям реализуемого алгоритма
4. По деструктивным возможностям

27. По какому признаку вирус классифицируется как «stealth-вирус»?
1. По объекту внедрения
2. По особенностям реализуемого алгоритма
3. По деструктивным возможностям

28. По какому признаку вирус классифицируется как «загрузочный (бутовый) вирус»?
1. По объекту внедрения
2. По особенностям реализуемого алгоритма
3. По режиму функционирования

29. Вирусы, содержащие в себе алгоритмы шифрования и обеспечивающие различие разных копий вируса называются:
1. Вирусы-спутники
2. Stealth-вирусы
3. MtE-вирусы
4. Репликаторы

30. К какому типу компьютерных вирусов относятся полиморфные вирусы?
1. К MtE-вирусам
2. К Stealth-вирусам
3. К вирусам-спутникам

31. По какому признаку компьютерный вирус классифицируется как репликатор?
1. По особенностям реализуемого алгоритма
2. По объекту внедрения
3. По наличию дополнительных возможностей

32. Вирусы, создающие для заражаемых файлов одноименные файлы с кодом вируса и переименовывающие исходные файлы называются:
1. Вирусы - спутники
2. Вирусы - невидимки
3. Вирусы - мутанты

33. Как называется компьютерный вирус, который использует слабую защищенность некоторых ОС и заменяет некоторые их компоненты (драйверы дисков, прерывания)?
1. Файловым
2. Загрузочным
3. Stealth-вирус
4. Репликатор

34. Как называются группы из нескольких вирусов?
1. Поливирусами
2. Семейством вирусов
3. Вирусным классом
4. Нет верных ответов

35. Какие вирусы характеризуются способностью самостоятельно передавать свой код на удаленный сервер или рабочую станцию?
1. Файловые вирусы
2. Бутовые (загрузочные) вирусы
3. Нет правильных ответов
4. Файловых и загрузочных вирусы

ВАРИАНТ № 2

Указания:

Задания имеют один правильный вариант ответа. В листе ответа проставляются номера правильных ответов.

1. Сколько классов АВС определено РД ГТК «Средства антивирусной защиты. Показатели защищенности и требования по защите от вирусов»
1. три
2. пять
3. семь
4. девять
5. нет правильных ответов

2. Деятельность, направленную на предотвращение получения защищаемой информации заинтересованным субъектом с нарушением установленных правовыми документами или собственником (владельцем информации) прав или правил доступа к защищаемой информации называется:
1. Обеспечение целостности информации
2. Обеспечение доступности информации
3. Защита информации от НСД
4. Защита информации

2. Как называется тип документа, в котором в целях добровольного многократного использования устанавливаются порядок осуществления процессов производства, эксплуатации, хранения, перевозки, реализации и утилизации, выполнения работ или оказания услуг?
1. Регламент
2. Стандарт
3. Спецификация
4. Сертификат

7. Как называется Спецификация X.509
1. «Служба директорий: каркасы сертификатов открытых ключей и атрибутов».
2. «Служба директорий: обзор концепций, моделей и сервисов».
3. «Архитектура безопасности для взаимодействия открытых систем».

8. Что обозначает аббревиатура ФСТЭК?
1. Федеральная система технологического и эксплуатационного контроля.
2. Федеральная служба технического и экспортного контроля.
3. Федеральная служба технического и экспертного контроля.
4. Федеральная служба таможенного и экспертного контроля.
5. Нет правильного ответа.

9. Как называется процесс присвоение объектам и субъектам доступа идентификатора и (или) сравнение предъявляемого идентификатора с перечнем присвоенных идентификаторов?
1. Аутентификация.
2. Национализация.
3. Идентификация.
4. Паролизация.

10. Для каких целей при администрировании, парольной системы, устанавливается ограничение числа попыток ввода пароля?
1. Усложняет задачу злоумышленника при попытке подобрать пароль по словарю
2. Препятствует интерактивному подбору паролей злоумышленником
3. Усложняет задачу злоумышленника при попытке подобрать пароль методом «тотального опробования».
4. Защищает от неправомерных действий системного администратора, имеющего доступ к паролю в момент создания учетной записи.
5. Для всех целей перечисленных в пунктах 1-4.

11. Какой из перечисленных методов не применяется для аутентификации пользователей?
1. Системы, основанные на знании некоторой секретной информации.
2. Системы, основанные на владении некоторым специальным предметом или устройством.
3. Системы, основанные на биометрических характеристиках.
4. Нет правильного ответа. Все применяются.

12. Может ли на одном компьютере создаваться несколько учетных записей с правами администратора?
1. Нет, только должна быть только одна учетная запись данного типа.
2. Может быть не менее одной учетной записи данного типа.
3. Допускается не более двух учетных записей данного типа.
4. Нет правильных ответов.

13. Свойство информации, заключающееся в ее актуальности и непротиворечивости, ее защищенности от разрушения и несанкционированного изменения называется:
1. Доступностью.
2. Целостностью.
3. Конфиденциальностью.

14. Какой из перечисленных сервисов не является сервисом безопасности?
1. Экранирование.
2. Туннелирование.
3. Архивирование.
4. Шифрование.
5. Контроль целостности.
6. Контроль защищенности.

15. По какому критерию классифицируется удаленная атака, приводящая к искажению информации?
1. По цели воздействия
2. По характеру воздействия
3. По расположению субъекта атаки относительно атакуемого объекта

16. Какой классификационный признак позволяет судить о так называемой «степени удаленности» атаки?
1. По уровню эталонной модели ISO/OSI, на котором осуществляется воздействие
2. По расположению субъекта атаки относительно атакуемого объекта
3. По условию начала осуществления воздействия

17. Какая из перечисленных удаленных атак является пассивной?
1. DNS spoofing
2. SYN flooding
3. Sniffing
4. Перехват пакетов на маршрутизаторе

18. Что означает аббревиатура NIDS:
1. Международная Организация по Стандартизации
2. Системы обнаружения (выявления) атак
3. Лавинное затопление ICMP-пакетами

19. Преимуществом метода данного типа является возможность обнаружения новых атак без необходимости постоянного изменения параметров функционирования модуля. О каком методе идет речь?
1. Сигнатурном (signature)
2. Шаблонном (pattern)
3. На основе обнаружения злоупотреблений
4. Нет правильных ответов

20. Принцип работы этого метода заключается в обнаружении несоответствия между текущим режимом функционирования КС и моделью штатного режима работы, заложенной в параметрах метода. О каком методе обнаружения атак идет речь?
1. На основе обнаружения аномального поведения (поведенческие методы)
2. На основе обнаружения злоупотреблений
3. Сигнатурный (signature)

4. Нет правильных ответов

21. Как называются СОА обнаруживающие атаки, направленные на всю сеть или сегмент?
1. host-based
2. network-based
3. Системы обнаружения атак на уровне хоста
4. Нет правильных ответов

22. Недостатком таких систем является то, что они сильно загружают процессор и требуют больших объемов дискового пространства для хранения журналов регистрации. О каких типах СОА идет речь?
1. network-based
2. host-based
3. Системы обнаружения атак уровня сети
4. Нет правильных ответов
23. Что означает аббревиатура DoS?
1. атаки типа «отказ в обслуживании»
2. атаки типа «затопление»
3. атаки типа «подмена адреса»
4. нет правильных ответов

24. Если атакующая программа, запущенная на сетевом компьютере, ждет посылки от потенциальной цели атаки определенного типа запроса, который будет условием начала осуществления атаки, то такая атака классифицируется как:
1. Атака по запросу от атакуемого объекта
2. Атака по наступлению определенного события на атакуемом объекте
3. Безусловная атака

25. Межсетевой экран предназначен:
1. Для защиты программ от несанкционированного копирования
2. Для обеспечения безопасного доступа к внешней сети и ограничения доступа внешних пользователей к внутренней сети.
3. Для защиты экрана монитора от несанкционированного снятия информации с помощью технических средств разведки.
4. Нет правильных ответов.

26. Какой из перечисленных компонентов не входит в состав технологии Межсетевого экранирования (МЭ):
1. Сетевая политика безопасности.
2. Централизованное управление.
3. Политика применения антивирусных средств при работе в сети.
4. Подсистема сбора статистики и предупреждения об атаке.
5. Все перечисленные компоненты входят в технологию МЭ.

27. Политика доступа к сетевым сервисам является подчиненной политикой:
1. Политики сетевой безопасности
2. Усиленной аутентификации
3. Политики реализации межсетевых экранов
4. Нет правильных ответов

28. Чем определяются правила доступа к ресурсам внутренней сети, при реализации политики межсетевого экранирования?

1. Политикой реализации межсетевых экранов
2. Политикой доступа к сетевым сервисам
3. Нет правильных ответов

29. Чем определяется список сервисов Internet, к которым пользователи должны иметь ограниченный доступ?
1. Политикой доступа к сетевым сервисам
2. Политикой реализации межсетевых экранов
3. Нет правильных ответов

30. Возможность некоторых МЭ по блокированию (уничтожению) пакетов, попадающих на МЭ, по заданному критерию на основе данных, содержащихся в заголовках пакетов и текущих параметров окружающей среды называется:
1. Фильтрация с применением Посредника (транспортного) уровня соединения (circuit-level proxy)
2. Простая фильтрация пакетов (с помощью фильтрующего маршрутизатора)
3. Фильтрация с применением Посредника прикладного уровня (application proxy)
4. Нет правильных ответов

31. Какие из перечисленных пунктов определяют достоинства простой фильтрации пакетов?
1. Локальная сеть может быть сделана невидимой из глобальной сети
2. Способность гибкого регулирования (ограничения) пропускной способности
3. Использование политики «запрещено все, что не разрешено»
4. Нет правильных ответов

32. Какие из перечисленных пунктов определяют достоинства шлюза прикладного уровня (application proxy)?
1. «Прозрачность» связи
2. Гибкость в определении правил фильтрации
3. Небольшая задержка при прохождении пакетов
4. Нет правильных ответов

33. Какие из перечисленных пунктов определяют недостатки фильтрующего маршрутизатора (простой фильтрации пакетов)
1. Не учитывается состояние соединения транспортного и прикладного уровней
2. При нарушении работоспособности МЭ все компьютеры за ним становятся полностью незащищенными либо недоступными
3. Не учитывается содержимое IP-пакетов
4. Все пункты определяют недостатки простой фильтрации пакетов
5. Нет правильных ответов

34. Функция МЭ, скрывающая внутренние адреса объектов (субъектов) от внешних субъектов называется:
1. Экранирование
2. Трансляция адреса
3. Правило фильтрации
4. Нет правильных ответов

35. Как называется наука о создании и анализе систем безопасной связи?
1. Криптология
2. Криптография
3. Криптоанализ

36. Как называется дисциплина (раздел науки), охватывающая принципы, средства и методы преобразования данных для сокрытия их информационного содержимого?
1. Криптоанализ
2. Криптография
3. Криптология

37. Как называется конкретное секретное состояние некоторых параметров алгоритма криптографического преобразования данных, обеспечивающее выбор одного преобразования из совокупности всевозможных?
1. Шифр
2. Ключ
3. Криптоалгоритм

38. Как называется совокупность обратимых преобразований множества возможных открытых данных (текстов) на множество возможных зашифрованных данных (криптограмм), осуществляемых по определенным правилам?
1. Шифр
2. Ключ
3. Криптоалгоритм

5 Дополнения и изменения в рабочей программе

№ изменения, дата внесения изменения; № страницы с изменением;	
БЫЛО	СТАЛО
Основание: Подпись лица внесшего изменения	

6. Оценка освоения достижений личностных результатов воспитательной работы

Оценка достижения обучающимися личностных результатов (далее – ЛР) проводиться в рамках контрольных и оценочных процедур, предусмотренных данной Программой.

Способы контроля результатов и критерии результативности реализации воспитательной работы обучающихся академического колледжа.

Вид контроля	Результат контроля
Входной контроль	диагностика способностей и интересов обучающихся (тестирование, анкетирование, социометрия, опрос).
Текущий контроль	педагогическое наблюдение в процессе проведения мероприятий, педагогический анализ творческих работ, мероприятий обучающихся, формирование и анализ портфолио обучающегося; исполнение текущей отчетности
Итоговый контроль	анализ деятельности

Комплекс критериев оценки личностных результатов обучающихся:

– демонстрация интереса к будущей профессии;

– оценка собственного продвижения, личностного развития;

– положительная динамика в организации собственной учебной деятельности по результатам самооценки, самоанализа и коррекции ее результатов;

– ответственность за результат учебной деятельности и подготовки к профессиональной деятельности;

– проявление высокопрофессиональной трудовой активности;

– участие в исследовательской и проектной работе;

– участие в конкурсах профессионального мастерства, олимпиадах по профессии, викторинах, в предметных неделях;

– соблюдение этических норм общения при взаимодействии с обучающимися, преподавателями, руководителями практик;

– конструктивное взаимодействие в учебном коллективе;

– демонстрация навыков межличностного делового общения, социального имиджа;

– готовность к общению и взаимодействию с людьми самого разного статуса, этнической, религиозной принадлежности и в многообразных обстоятельствах;

– сформированность гражданской позиции; участие в волонтерском движении;

– проявление мировоззренческих установок на готовность молодых людей к работе на благо Отечества;

– проявление правовой активности и навыков правомерного поведения, уважения к Закону;

– отсутствие фактов проявления идеологии терроризма и экстремизма среди обучающихся;

– отсутствие социальных конфликтов среди обучающихся, основанных на межличностной, межрелигиозной почве;

– участие в реализации просветительских программ, поисковых, военно-исторических, краеведческих отрядах и молодежных объединениях;

– добровольческие инициативы по поддержки инвалидов и престарелых граждан;

– проявление экологической культуры, бережного отношения к родной земле, природным богатствам России и мира;

– демонстрация умений и навыков разумного природопользования, нетерпимого отношения к действиям, приносящим вред экологии;

– демонстрация навыков здорового образа жизни и высокий уровень культуры здоровья обучающихся;

– проявление культуры потребления информации, умений и навыков пользования компьютерной техникой, навыков отбора и критического анализа информации, умения ориентироваться в информационном пространстве;

– участие в конкурсах профессионального мастерства и в командных проектах;

проявление экономической и финансовой культуры, экономической грамотности а также собственной адекватной позиции по отношению к социально-экономической действительности.