Государственное бюджетное образовательное учреждение высшего образования
Московской области

ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ

имени дважды Героя Советского Союза, летчика-космонавта А.А. Леонова

ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ МОСКОВСКОЙ ОБЛАСТИ "ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ ИМЕНИ ДВАЖДЫ ГЕРОЯ СОВЕТСКОГО СОЮЗА, ЛЕТЧИКА-КОСМОНАВТА А.А.ЛЕОНОВА"

Подписано цифровой подписью: ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ МОСКОВСКОЙ ОБЛАСТИ "ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ ИМЕНИ ДВАЖДЫ ГЕРОЯ СОВЕТСКОГО СОЮЗА, ЛЕТЧИКА-КОСМОНАВТА А.А.ЛЕОНОВА"

УТВЕРЖДАЮ
Ректор
А.Ю. Щиканов
«__» _____ 2021 г.

ПРОГРАММА МЕЖДИСЦИПЛИНАРНОГО ВСТУПИТЕЛЬНОГО ИСПЫТАНИЯ ПО НАПРАВЛЕНИЮ ПОДГОТОВКИ 10.04.01 ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

Королев
2021

Автор: Сухотерин А.И. Программа междисциплинарного вступительного испытания по направлению подготовки 10.04.01 Информационная безопасность. – Королев МО: «Технологический университет», 2021 г.

Программа рекомендована на заседании УМС:

Год утверждения (переутверждения)	2021	2022	2023	2024
Номер и дата протокола заседания УМС	Протокол № 1 от 19.10.2021	Протокол № 2 от 11.10.2022		

1. **Форма проведения вступительного испытания.**

Вступительные испытания проводятся очно и (или) с использованием дистанционных технологий (при условии идентификации поступающих при сдаче ими вступительных испытаний).

2. **Продолжительность вступительного испытания**: 120 мин.

3. **Критерии оценки, шкала оценивания**:

Минимальный проходной балл – 40.

Прием в магистратуру осуществляется на конкурсной основе по результатам вступительных испытаний (собеседование по профилю направления подготовки) и показателей индивидуальных достижений.

- 85-100 баллов соответствует оценке («отлично») выставляется, когда студент показал глубокое и всестороннее знание теории защиты информации, аргументировано и логически изложил материал, обоснованно связал изложение материала с практическими вопросами обеспечения защиты информации. На основные и дополнительные вопросы отвечал самостоятельно, без наводящих вопросов, глубоко знает обязательную и дополнительную литературу.

- 65-85 баллов соответствует оценке («хорошо») выставляется при твердых знаниях студентом теории защиты информации, аргументированном и логическом изложении материала, умении связать материал с практическими вопросами обеспечения защиты информации. При ответе на вопросы допустил отдельные неточности, которые самостоятельно исправил после замечания членов комиссии, знает обязательную и знаком с дополнительной литературой.

- 40-56 баллов соответствует оценке («удовлетворительно») ставится, когда студент в основном знает теорию защиты информации, материал излагал не совсем аргументировано и последовательно, изложенный материал связал с практическими вопросами обеспечения защиты информации после наводящих вопросов. При ответе на вопросы допустил серьезные неточности, которые исправил после замечания членов комиссии, знает обязательную литературу.

- оценка менее 40 баллов является неудовлетворительной и ставится, когда студент не усвоил основного содержания теории защиты информации, не ответил на вопросы билета или при ответе допустил серьезные неточности, которые не смог исправить после замечания членов комиссии, слабо знает обязательную литературу.

4. Поступающий должен:

знать:

– правовые основы обеспечения национальной безопасности Российской Федерации;

– основные разделы и направления философии, методы и приемы философского анализа проблем;

– общие принципы построения и использования современных языков программирования высокого уровня;
– эталонную модель взаимодействия открытых систем;
– основные задачи и понятия криптографии;
– частотные характеристики открытых текстов и способы их применения к анализу простейших шифров замены и перестановки;
– основные информационные технологии, используемые в автоматизированных системах;
– автоматизированную систему как объект информационного воздействия, критерии оценки ее защищенности и методы обеспечения ее информационной безопасности;
– методы, способы, средства, последовательность и содержание
– этапов разработки автоматизированных систем и подсистем безопасности автоматизированных систем;
– способы кодирования информации;
– современные технологии и методы программирования;
– методы анализа и синтеза электронных схем;
– язык программирования высокого уровня (объектно-
– ориентированное программирование);
– возможности, классификацию и область применения
– макрообработки;

в научно-исследовательской деятельности:

– принципы построения и функционирования, примеры реализаций современных операционных систем;
– принципы построения и функционирования, примеры реализаций современных локальных и глобальных компьютерных сетей;
– основные информационные технологии, используемые в автоматизированных системах;
– показатели качества программного обеспечения;
– язык программирования высокого уровня (объектно-ориентированное программирование);
– возможности, классификацию и область применения макрообработки;
– способы обработки исключительных ситуаций;
– принципы построения и функционирования, примеры реализаций современных операционных систем;
– основные угрозы безопасности информации и модели нарушителя в автоматизированных системах;
– основные меры по защите информации в автоматизированных системах (организационные, правовые, программно-аппаратные, криптографические, технические);
– основные криптографические методы, алгоритмы, протоколы, используемые для обеспечения информационной безопасности в автоматизированных и телекоммуникационных системах;

– требования к шифрам и основные характеристики шифров;

– требования к шифрам и основные характеристики шифров;

– архитектуру, принципы функционирования, элементную базу современных компьютеров, вычислительных и телекоммуникационных систем;

– источники и классификацию угроз информационной безопасности;

– основные средства и способы обеспечения информационной безопасности, принципы построения систем защиты информации;

– основные информационные технологии, используемые в

– автоматизированных системах;

– основные угрозы безопасности информации и модели нарушителя в автоматизированных системах;

– основные комбинаторные и теоретико-графовые алгоритмы, а также способы их эффективной реализации и оценки сложности;

в проектно-конструкторской деятельности:

– средства обеспечения безопасности данных;

– основы организационного и правового обеспечения;

– информационной безопасности, основные положения законодательства Российской Федерации в области защиты информации;

– показатели качества программного обеспечения;

– методологии и методы проектирования программного обеспечения;

– методы тестирования и отладки ПО;

– принципы организации документирования разработки, процесса сопровождения программного обеспечения;

– основные структуры данных и способы их реализации на языке программирования;

– основные комбинаторные и теоретико-графовые алгоритмы, а также способы их эффективной реализации и оценки сложности принципы построения и функционирования, примеры реализаций современных систем управления базами данных;

– архитектуру систем баз данных;

– основные модели данных;

– физическую организацию баз данных;

– последовательность и содержание этапов проектирования баз данных;

– основные задачи и понятия криптографии;

– основные угрозы безопасности информации и модели нарушителя в автоматизированных системах принципы формирования политики информационной безопасности в автоматизированных системах;

в контрольно-аналитической деятельности:

– требования к шифрам и основные характеристики шифров;

– основные информационные технологии, используемые в автоматизированных системах;

– требования к шифрам и основные характеристики шифров;

– способы и средства защиты информации от утечки по техническим каналам и контроля эффективности защиты информации;

– возможности технических средств перехвата информации;

– технические каналы утечки информации;

в организационно-управленческой деятельности:

– основные понятия и методы в области управленческой деятельности;

– порядок выработки и реализации управленческих решений;

– содержание управленческой работы руководителя подразделения;

– проводить анализ архитектуры и структуры ЭВМ и систем,

– оценивать эффективность архитектурно-технических решений, реализованных при построении ЭВМ и систем;

– содержание и порядок деятельности персонала по эксплуатации защищенных автоматизированных систем и подсистем безопасности автоматизированных систем;

– состав системы управления и требования к ее элементам;

– основные криптографические методы, алгоритмы, протоколы,

– используемые для обеспечения безопасности в сетях ЭВМ;

– программно-аппаратные средства обеспечения

– информационной безопасности в типовых операционных системах, системах управления базами данных, компьютерных сетях;

в эксплуатационной деятельности:

– основы организационного и правового обеспечения информационной безопасности, основные положения законодательства Российской Федерации в области защиты информации;

– основные методы управления информационной безопасностью основные криптографические методы, алгоритмы, протоколы, используемые для обеспечения безопасности в сетях ЭВМ;

– основы организационного и правового обеспечения информационной безопасности, основные положения законодательства Российской Федерации в области защиты информации типовые шифры с открытыми ключами;

– технические характеристики, показатели качества ЭВМ и систем, методы их оценки и пути совершенствования;

– источники и классификацию угроз информационной безопасности;

– программно-аппаратные средства обеспечения информационной безопасности в типовых операционных системах, системах управления базами данных, компьютерных сетях;

– основные угрозы безопасности информации и модели нарушителя в автоматизированных системах;

– содержание и порядок деятельности персонала по эксплуатации защищенных автоматизированных систем и подсистем безопасности автоматизированных систем;

– основные меры по защите информации в автоматизированных системах (организационные, правовые, программно-аппаратные, криптографические, технические);

− основные криптографические методы, алгоритмы, протоколы, используемые для обеспечения информационной безопасности в автоматизированных и телекоммуникационных системах;

− современные технологии и методы программирования;

− типовые шифры с открытыми ключами;

− основные методы управления информационной безопасностью;

уметь:

− анализировать мировоззренческие, социально и личностно значимые философские проблемы, проводить исторический анализ событий, анализировать и оценивать социальную информацию, планировать и осуществлять свою деятельность с учетом результатов этого анализа;

− оценивать эффективность управленческих решений и анализировать экономические показатели деятельности подразделения;

− пользоваться сетевыми средствами для обмена данными, в том числе с использованием глобальной информационной сети Интернет;

− использовать в практической деятельности правовые знания;

− разрабатывать и исследовать аналитические и компьютерные модели автоматизированных систем и подсистем безопасности автоматизированных систем;

− применять знания о системах электрической связи для решения задач по созданию защищенных телекоммуникационных систем;

− анализировать тенденции развития систем и сетей электросвязи, внедрения новых служб и услуг связи;

− применять требования Единой системы конструкторской документации и Единой системы программной документации при разработке технической документации;

− применять действующую законодательную базу в области обеспечения информационной безопасности;

− классифицировать защищаемую информацию по видам тайны и степеням конфиденциальности;

− разрабатывать и исследовать аналитические и компьютерные модели автоматизированных систем и подсистем безопасности автоматизированных систем;

− администрировать подсистемы информационной безопасности автоматизированных систем;

− пользоваться нормативными документами по противодействию технической разведке;

− разрабатывать предложения по совершенствованию системы управления информационной безопасностью автоматизированных систем;

− реализовывать и контролировать выполнение требований по охране труда и технике безопасности в профессиональной деятельности;

− применять основные методы защиты производственного персонала и населения от возможных последствий аварий, катастроф, стихийных бедствий;

− применять типовые программные средства сервисного назначения (средства восстановления системы после сбоев, очистки и дефрагментации

диска);

− проводить выбор программно-аппаратных средств обеспечения информационной безопасности для использования их в составе автоматизированной системы с целью обеспечения требуемого уровня защищенности автоматизированной системы;

− применять на практике методы анализа электрических цепей;

− работать с современной элементной базой электронной аппаратуры;

− проектировать и администрировать компьютерные сети, реализовывать политику безопасности компьютерной сети;

− применять действующую законодательную базу в области обеспечения информационной безопасности;

− разрабатывать проекты нормативных материалов, регламентирующих работу по защите информации;

− проводить выбор программно-аппаратных средств обеспечения информационной безопасности для использования их в составе автоматизированной системы с целью обеспечения требуемого уровня защищенности автоматизированной системы;

− разрабатывать технические задания на создание подсистем информационной безопасности автоматизированных систем, проектировать такие подсистемы с учетом действующих нормативных и методических документов;

− определять комплекс мер (правила, процедуры, практические приемы, руководящие принципы, методы, средства) для обеспечения информационной безопасности автоматизированных систем, составлять аналитические обзоры по вопросам обеспечения информационной безопасности автоматизированных систем;

− разрабатывать и исследовать аналитические и компьютерные модели автоматизированных систем и подсистем безопасности автоматизированных систем;

− исследовать эффективность создаваемых средств автоматизации, проводить технико-экономическое обоснование проектных решений;

− разрабатывать и исследовать аналитические и компьютерные модели автоматизированных систем и подсистем безопасности автоматизированных систем;

− анализировать и оценивать угрозы информационной безопасности объекта;

− анализировать и оценивать угрозы информационной безопасности объекта;

− анализировать программные, архитектурно-технические и

схемотехнические решения компонентов автоматизированных систем с целью выявления потенциальных уязвимостей информационной безопасности автоматизированных систем;

− классифицировать и оценивать угрозы информационной безопасности для объекта информатизации;

− проектировать структуру и архитектуру программного обеспечения с использованием современных методологий и средств автоматизации

проектирования программного обеспечения;

− разрабатывать проекты нормативных материалов, регламентирующих работу по защите информации;

− разрабатывать технические задания на создание подсистем информационной безопасности автоматизированных систем, проектировать такие подсистемы с учетом действующих нормативных и методических документов;

− определять информационную инфраструктуру и информационные ресурсы организации, подлежащие защите;

− определять комплекс мер (правила, процедуры, практические приемы, руководящие принципы, методы, средства) для обеспечения информационной безопасности автоматизированных систем, составлять аналитические обзоры по вопросам обеспечения информационной безопасности автоматизированных систем

− формировать требования и разрабатывать внешние спецификации для разрабатываемого программного обеспечения;

− планировать разработку сложного программного обеспечения;

− проводить комплексное тестирование и отладку программных систем;

− проектировать и кодировать алгоритмы с соблюдением требований к качественному стилю программирования;

− реализовывать основные структуры данных и базовые алгоритмы средствами языков программирования;

− проводить выбор эффективных способов реализации структур данных и конкретных алгоритмов при решении профессиональных задач;

− работать с интегрированной средой разработки программного обеспечения;

− оценивать информационные риски в автоматизированных системах;

− разрабатывать и администрировать базы данных;

− выделять сущности и связи предметной области;

− отображать предметную область на конкретную модель данных;

− нормализовывать отношения при проектировании реляционной базы данных;

− применять требования Единой системы конструкторской документации и Единой системы программной документации при разработке технической документации;

− применять на практике методы анализа электрических цепей;

− использовать стандартные методы и средства проектирования цифровых узлов и устройств, в том числе для средств защиты информации;

− проектировать структуру и архитектуру программного обеспечения с использованием современных методологий и средств автоматизации проектирования программного обеспечения;

− проводить выбор эффективных способов реализации структур данных и конкретных алгоритмов при решении профессиональных задач;

− разрабатывать модели угроз и нарушителей информационной безопасности автоматизированных систем;

− разрабатывать частные политики информационной безопасности

информационной безопасности автоматизированных систем;

− применять требования Единой системы конструкторской документации и Единой системы программной документации при разработке технической документации;

− оценивать информационные риски в автоматизированных системах;

− применять требования Единой системы конструкторской документации и Единой системы программной документации при разработке технической документации;

− эффективно использовать криптографические методы и средства защиты информации в автоматизированных системах;

− разрабатывать технические задания на создание подсистем информационной безопасности автоматизированных систем, проектировать такие подсистемы с учетом действующих нормативных и методических документов;

− исследовать эффективность создаваемых средств автоматизации, проводить технико-экономическое обоснование проектных решений;

− разрабатывать частные политики информационной безопасности информационной безопасности автоматизированных систем;

владеть:

− навыками поиска нормативной правовой информации, необходимой для профессиональной деятельности;

− навыками публичной речи, аргументации, ведения дискуссии и полемики, практического анализа логики различного рода рассуждений; навыками критического восприятия информации; навыками письменного аргументированного изложения собственной точки зрения;

− представлениями о событиях российской и всемирной истории, основанными на принципе историзма;

− навыками анализа исторических источников;

− приемами ведения дискуссии и полемики;

− навыками поиска нормативной правовой информации, необходимой для профессиональной деятельности;

− методиками оценки показателей качества и эффективности ЭВМ и вычислительных систем;

− навыками анализа и синтеза структурных и функциональных схем защищенных автоматизированных информационных систем;

− навыками анализа основных характеристик и возможностей телекоммуникационных систем по передаче информации;

− навыками использования современной измерительной аппаратуры при экспериментальном исследовании электронной аппаратуры;

− навыками работы с программными средствами схемотехнического моделирования;

− навыками работы с нормативными правовыми актами;

− навыками работы с технической документацией на компоненты автоматизированных систем на русском и иностранном языках;

− навыками использования программно-аппаратных средств обеспечения

информационной безопасности автоматизированных систем;

− методами формирования требований по защите информации;

− методиками оценки показателей качества и эффективности ЭВМ и вычислительных систем;

− профессиональной терминологией в области информационной безопасности;

− навыками анализа основных узлов и устройств современных автоматизированных систем;

− навыками анализа и синтеза структурных и функциональных схем защищенных автоматизированных информационных систем;

− навыками разработки, документирования компьютерных сетей с учетом требований по обеспечению безопасности;

− навыками разработки технической документации в соответствии с требованиями Единой системы конструкторской документации и Единой системы программной документации;

− навыками участия в экспертизе состояния защищенности информации на объекте защиты;

− навыками участия в экспертизе состояния защищенности информации на объекте защиты;

− навыками проектирования программного обеспечения с использованием средств автоматизации;

− навыками разработки, документирования, тестирования и отладки программного обеспечения в соответствии с современными технологиями и методами программирования;

− навыками разработки программной документации;

− навыками программирования с использованием эффективных реализаций структур данных и алгоритмов;

− навыками разработки технической документации в

соответствии с требованиями Единой системы конструкторской документации и Единой системы программной документации;

− навыками работы с программными средствами схемотехнического моделирования;

− навыками разработки программной документации;

− навыками программирования с использованием эффективных реализаций структур данных и алгоритмов;

− навыками разработки технической документации в соответствии с требованиями Единой системы конструкторской документации и Единой системы программной документации;

− навыками участия в экспертизе состояния защищенности информации на объекте защиты;

− криптографической терминологией;

− методами формирования требований по защите информации;

− методами и технологиями проектирования, моделирования, исследования автоматизированных систем и подсистем безопасности автоматизированных систем;

− методами и средствами технической защиты информации навыками

участия в экспертизе состояния защищенности информации на объекте защиты;

− навыками использования программно-аппаратных средств обеспечения информационной безопасности автоматизированных систем;

− методами расчета и инструментального контроля показателей технической защиты информации;

− навыками анализа информационной инфраструктуры автоматизированной системы и ее безопасности;

− методами мониторинга и аудита, выявления угроз информационной безопасности автоматизированных систем;

− методами оценки информационных рисков;

− методами мониторинга и аудита, выявления угроз информационной безопасности автоматизированных систем;

− навыками обоснования, выбора, реализации и контроля результатов управленческого решения;

− навыками организации и обеспечения режима секретности;

− навыками работы с технической документацией на ЭВМ и вычислительные системы;

− навыками обоснования, выбора, реализации и контроля результатов управленческого решения;

− навыками работы с нормативными правовыми актами;

− навыками, эксплуатации и администрирования (в части, касающейся разграничения доступа, аутентификации и аудита) баз данных, локальных компьютерных сетей, программных систем с учетом требований по обеспечению информационной безопасности;

− навыками использования программно-аппаратных средств обеспечения безопасности сетей ЭВМ

− навыками, эксплуатации и администрирования (в части, касающейся разграничения доступа, аутентификации и аудита) баз данных, локальных компьютерных сетей, программных систем с учетом требований по обеспечению информационной безопасности

− навыками эксплуатации и администрирования баз данных с учетом требований по обеспечению информационной безопасности;

− навыками организации и обеспечения режима секретности;

− навыками работы с технической документацией на компоненты автоматизированных систем на русском и иностранном языках;

− навыками поддержания работоспособности, обнаружения и устранения неисправностей в работе электронных аппаратных средств автоматизированных систем;

− навыками использования программно-аппаратных средств обеспечения информационной безопасности автоматизированных систем навыками использования программно-аппаратных средств обеспечения безопасности сетей ЭВМ;

− методами формирования требований по защите информации;

− навыками, эксплуатации и администрирования (в части, касающейся разграничения доступа, аутентификации и аудита) баз данных, локальных компьютерных сетей, программных систем с учетом требований по

обеспечению информационной безопасности;

− навыками использования программно-аппаратных средств обеспечения безопасности сетей ЭВМ;

− методами управления информационной безопасностью автоматизированных систем;

− навыками выбора и обоснования критериев эффективности функционирования защищенных автоматизированных информационных систем

− навыками, эксплуатации и администрирования (в части, касающейся разграничения доступа, аутентификации и аудита) баз данных, локальных компьютерных сетей, программных систем с учетом требований по обеспечению информационной безопасности;

− навыками использования программно-аппаратных средств обеспечения безопасности сетей ЭВМ;

− навыками работы с технической документацией на ЭВМ и вычислительные системы;

− профессиональной терминологией в области информационной безопасности;

− навыками, эксплуатации и администрирования (в части, касающейся разграничения доступа, аутентификации и аудита) баз данных, локальных компьютерных сетей, программных систем с учетом требований по обеспечению информационной безопасности;

− навыками использования программно-аппаратных средств обеспечения безопасности сетей ЭВМ;

− навыками чтения принципиальных схем, построения временных диаграмм и восстановления алгоритма работы узла, устройства и системы по комплекту документации;

− навыками оценки быстродействия и оптимизации работы электронных схем на базе современной элементной базы;

− навыками разработки программной документациинавыками использования типовых криптографических алгоритмов;

− навыками использования ЭВМ в анализе простейших шифров.

4. Основные темы и их содержание:

№	Тема	Содержание
1	Организационно - правовая защита информации	Введение в профессию. Правовое обеспечение информационной безопасности. Организационное обеспечение информационной безопасности. Экономические аспекты информационной безопасности.
2	Инженерно-техническая защита	Информационные процессы (системы) и их . безопасность. Инженерно-техническая защита информации. Защита и обработка конфиденциальных документов. Информационная безопасность предприятии.

3	Защита информационных технологий	Основы информационной безопасности. Криптографические методы защита информации. Программно-аппаратные средства защита информации
4	Профильные дисциплины	История защиты информации в России. Система защиты информации в зарубежных странах. Основы управления информационной безопасностью. Информационно-аналитическая деятельность по обеспечению комплексной безопасности. Информационная безопасность автоматизированных систем.

СПИСОК ВОПРОСОВ, ВКЛЮЧАЕМЫХ В ЭКЗАМЕНАЦИОННЫЕ БИЛЕТЫ

РАЗДЕЛ 1. ОРГАНИЗАЦИОННО - ПРАВОВАЯ ЗАЩИТА ИНФОРМАЦИИ

1.1. Введение в профессию

1. Характеристика бакалавра по информационной безопасности.
2. Объекты и виды профессиональной деятельности, состав решаемых задач. Требования к профессиональной подготовленности в области информационной безопасности: что должен профессионально знать и уметь использовать.

1.2. Правовое обеспечение информационной безопасности

3. Назначение и структура правового обеспечения защиты информации. Методы правовой защиты информации.
4. Правовые основы защиты государственной, коммерческой, служебной, профессиональной и личной тайны, персональных данных.
5. Правовая основа допуска и доступа персонала к защищаемым сведениям.
6. Система правовой ответственности за утечку информации и утрату носителей информации.
7. Правовые основы деятельности подразделений защиты информации.
8. Отрасли права, обеспечивающие законность в области защиты информации. Основные законодательные акты, правовые нормы и положения.
9. Назначение и задачи подзаконных правовых актов, регулирующих процессы защиты информации в отраслях, на предприятиях различных форм собственности.
10. Правовое регулирование взаимоотношений администрации и персонала в области защиты информации. Виды и условия применения правовых норм уголовной, гражданско-правовой, административной и

дисциплинарной ответственности за разглашение защищаемой информации и невыполнение правил ее защиты.

11. Понятие интеллектуальной собственности, ее виды и основные объекты образования. Интеллектуальный продукт как объект интеллектуальной собственности и предмет защиты.

1.3 Организационное обеспечение информационной безопасности

12. Принципы, силы, средства и условия организационной защиты информации.

13. Порядок засекречивания и рассекречивания сведений, документов и продукции.

14. Допуск и доступ к конфиденциальной информации и документам.

15. Организация внутриобъектового и пропускного режимов на предприятиях.

16. Организация подготовки и проведения совещаний и заседаний по конфиденциальным вопросам.

17. Организация охраны предприятий. Защита информации при публикаторской и рекламной деятельности.

18. Организация аналитической работы по предупреждению утечки конфиденциальной информации.

19. Направления и методы работы с персоналом, обладающим конфиденциальной информацией.

1.4. Экономические аспекты информационной безопасности

20. Экономическая безопасность. Информация как важнейший ресурс экономики. Информация как товар, цена информации. Основные подходы к определению затрат на защиту информации.

21. Система ресурсообеспечения защиты информации и эффективность ее использования. Управление ресурсами в процессе защиты информации.

22. Виды ущерба, наносимые информации. Степень наносимого ущерба информации. Методы и способы страхования информации.

23. Формирование бюджета службы защиты информации. Оценка эффективности защиты и страхования информации.

РАЗДЕЛ 2. ИНЖЕНЕРНО-ТЕХНИЧЕСКАЯ ЗАЩИТА

2.1. Информационные процессы (системы) и их безопасность

24. Основные типы электронных средств генерации и преобразования сигналов. Преобразователи спектра сигналов. Акусто-электрические и электроакустические конверторы энергии сигналов. Элементы оптоэлектроники и инфракрасной техники.

25. Методы и средства записи, хранения и воспроизведения информации на магнитных носителях. Голографические носители и их перспективы.

26. Электромагнитные системы передачи и приема информации, их классификация.

27. Излучение и прием радиоволн, основные виды антенно-фидерных устройств, радиопередатчиков и радиоприемников.

28. Системы передачи и приема видеоинформации, звуковой (речевой) и цифровой информации. Организация связи с помощью ЭВМ, телекоммуникационные сети.

29. Способы и средства специальных видов связи (радиорелейные линии, спутниковая связь, лазерные каналы и др.)

2.2. Инженерно-техническая защита информации

30. Виды информации, защищаемой техническими средствами. Демаскирующие признаки объектов защиты. Источники и носители информации, защищаемой техническими средствами.

31. Виды угроз безопасности информации, защищаемой техническими средствами. Принципы добывания и обработки информации техническими средствами.

32. Классификация и структура технических каналов утечки информации. Основные способы и принципы работы средств наблюдения объектов, подслушивания и перехвата сигналов.

33. Системный подход к инженерно-технической защите информации. Основные этапы проектирования системы защиты информации техническими средствами.

34. Принципы моделирования объектов защиты и технических каналов утечки информации.

35. Организационные и технические меры инженерно-технической защиты информации в государственных и коммерческих структурах.

36. Основные составляющие систем ТСО: датчики, приборы визуального наблюдения, системы сбора и обработки информации, средства связи, питания и тревожно-вызывной сигнализации.

2.3. Защита и обработка конфиденциальных документов

37. Структура защищаемых документопотоков, состав технологических этапов и операций.

38. Подготовка и издание конфиденциальных документов. Учет конфиденциальных документов. Порядок рассмотрения и исполнения конфиденциальных документов. Размножение конфиденциальных документов. Контроль исполнения конфиденциальных документов.

39. Составление и оформление номенклатуры дел. Формирование и хранение дел, содержащих конфиденциальные документы. Уничтожение конфиденциальных документов. Проверка наличия конфиденциальных документов.

40. Порядок комплектования ведомственного архива конфиденциальной документации и классификация хранилищ документов. Учет деловых (управленческих) и научно-технических документов в архиве.

41. Машиноориентация содержания и форм конфиденциальных документов. Принцип включения различных типов автоматизированных систем в традиционный документооборот. Безбумажный документооборот.

42. Локальная и комплексная автоматизация процессов обработки конфиденциальных документов в документной службе. Домашинная и послемашинная технология выполнения операций по блокам: блока подготовки и издания документов, справочно-информационного блока, блока оперативного хранения и использования документов.

2.4. Информационная безопасность предприятия (объекта)

43. Сущность и задачи комплексной системы защиты информации (КСЗИ). Принципы организации и этапы разработки КСЗИ.

44. Определение и нормативное закрепление состава защищаемой информации. Определение объектов защиты.

45. Анализ и оценка угроз безопасности информации: выявление и оценка источников, способов и результатов дестабилизирующего воздействия на информацию.

46. Определение потенциальных каналов и методов несанкционированного доступа к информации. Определение возможностей несанкционированного доступа к защищаемой информации.

47. Определение компонентов КСЗИ. Определение условий функционирования КСЗИ. Разработка модели КСЗИ.

48. Технологическое и организационное построение КСЗИ. Кадровое обеспечение функционирования КСЗИ. Материально-техническое и нормативно-методическое обеспечение функционирования КСЗИ.

49. Состав методов и моделей оценки эффективности КСЗИ.

РАЗДЕЛ 3. ЗАЩИТА ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ

3.1 Основы информационной безопасности

50. Сущность и понятие информационной безопасности, характеристика ее составляющих. Место информационной безопасности в системе национальной безопасности.

51. Современная концепция информационной безопасности. Понятие и сущность защиты информации, ее место в системе информационной безопасности. Цели и концептуальные основы защиты информации.

52. Критерии, условия и принципы отнесения информации к защищаемой. Носители защищаемой информации. Классификация конфиденциальной информации по видам тайны и степеням конфиденциальности.

53. Понятие и структура угроз защищаемой информации. Источники, виды и методы дестабилизирующего воздействия на защищаемую информацию. причины, обстоятельства и условия, вызывающие дестабилизирующее воздействие на защищаемую информацию.

54. Виды уязвимости информации и формы ее проявления. Каналы и методы несанкционированного доступа к конфиденциальной информации.

55. Направления, виды и особенности деятельности спецслужб по несанкционированному доступу к конфиденциальной информации.

56. Методологические подходы к защите информации и принципы ее организации. Объекты защиты. Виды защиты. Классификация методов и средств защиты информации.

3.2. Криптографическая защита информации

57. Классические шифры, шифры гаммирования и колонной замены. Простейшие шифры и их свойства. композиции шифров.

58. Основные требования к шифрам. Вопросы практической стойкости. Имитостойкость и помехоустойчивость шифров.

59. Принципы построения криптографических алгоритмов. различие между программными и аппаратными реализациями. криптографические параметры узлов и блоков шифраторов. синтез шифров.

60. Криптографические хеш-функции. Общая схема подписывания и проверки подписи с использованием хэш-функции. Основные свойства хэш-функций. Схема вычисления хэш-функции.

3.3. Программно-аппаратная защита информации

61. Основные подходы к защите данных от НСД. Шифрование, контроль доступа и разграничение доступа, иерархический доступ к файлу, защита сетевого файлового ресурса, фиксация доступа к файлам.

62. Защита программ от несанкционированного копирования. Пароли и ключи, организация хранения ключей. Защита программ от излучения.

63. Защита от разрушающих программных воздействий (РПВ). Компьютерные вирусы как особый класс РПВ.

РАЗДЕЛ 4. ПРОФИЛЬНЫЕ ДИСЦИПЛИНЫ

4.1 История защиты информации в России

64. Предпосылки формирования системы защиты информации в России в XV-XVII вв.

65. Организация защиты информации в Российской империи в XVIII в.

66. Совершенствование организации защиты информации в первой половине XIX в.

67. Формирование системы защиты информации во второй половине XIX в.

68. Особенности системы защиты информации в начале XX в. (1900-1908 г.г.).

69. Организация защиты информации в период промышленного подъема (1909-1913 г.г.).

70. Организация защиты информации в период первой мировой войны.

71. Достоинства и недостатки системы защиты информации в Российской империи.

72. Укрепление системы защиты государственных секретов накануне и в период Великой Отечественной войны

73. Основные особенности организации защиты информации в советский период.

74. Полномочия органов власти, специальных федеральных органов и предприятий в области защиты информации в современной России.

75. Современное состояние системы защиты информации и перспективы ее совершенствования.

4.2 Система защиты информации в зарубежных странах

76. Стандарты и спецификации информационной безопасности в ведущих зарубежных стран.

77. Общая методология оценки безопасности информационных технологий (ОМОБИТ): история и перспективы развития, процесс оценки.

78. Критерии оценки надежных компьютерных систем: основные понятия, добровольное управление доступом, безопасность повторного использования объектов, метки безопасности, принудительное управление доступом.

79. Организация защиты информации в США: особенности государственного устройства, политики и законодательства в области защиты информации; организация системы специальных служб по национальной безопасности; классификация и защита государственной тайны и промышленных секретов (торговой тайны).

80. Организация защиты информации в Германии: особенности государственного устройства, политики и законодательства в области защиты информации; организация системы специальных служб по национальной безопасности; классификация и защита государственной тайны и промышленных секретов (торговой тайны).

81. Организация защиты информации в Великобритании: особенности государственного устройства, политики и законодательства в области защиты информации; организация системы специальных служб по национальной безопасности; классификация и защита государственной тайны и промышленных секретов (торговой тайны).

82. Организация защиты информации во Франции: особенности государственного устройства, политики и законодательства в области защиты информации; организация системы специальных служб по национальной безопасности; классификация и защита государственной тайны и промышленных секретов (торговой тайны).

83. Организация защиты информации в Японии: особенности государственного устройства, политики и законодательства в области защиты информации; организация системы специальных служб по национальной безопасности; классификация и защита государственной тайны и промышленных секретов (торговой тайны).

84. Международное сотрудничество в области защиты информации: научно-техническое сотрудничество с зарубежными партнерами; защита информации в процессе проведения международных конференций, симпозиумов, обмена специалистами; опыт защиты информации в процессе банковской деятельности.

85. Корпоративная система безопасности информации НАТО: национальный уполномоченный орган по безопасности информации; руководство по организационно техническим мероприятиям и минимальной

стандартизации в области защиты секретной информации; административное соглашение по безопасности между НАТО и странами-участниками североатлантического совета по сотрудничеству (САСС).

4.3 Основы управления информационной безопасностью

86. Задачи службы информационной безопасности. Направления деятельности службы информационной безопасности. Взаимодействие службы информационной безопасности со службой информационных технологий.

87. Основные критерии необходимости создания службы информационной безопасности. Состав службы информационной безопасности.

88. Определение необходимого уровня подготовки специалистов службы информационной безопасности. Подбор кадров. Контроль процесса подбора кадров.

89. Основные подразделения службы защиты информации. Функции руководителя службы защиты информации. Документационное обеспечение защиты информации.

90. Принципы управления службой защиты информации. Методы управления службой защиты информации. Технология управления службой защиты информации.

91. Предпосылки и цели обеспечения информационной безопасности предприятия. Основные принципы обеспечения информационной безопасности предприятия. Политика информационной безопасности предприятия.

92. Уязвимость информационных систем. Классификация сетевых атак.

93. Анализ степени осведомленности работников о секретах фирмы. Контроль за соблюдением персоналом правил защиты информации. Формы контроля. Понятие служебного расследования. Планирование и проведение служебного расследования по вопросам утраты информации.

4.4 Информационно-аналитическая деятельность по обеспечению комплексной безопасности

94. Информация как товар. Цена информации. Технологическая и деловая информация фирмы. Информация о внешней и внутренней среде фирмы.

95. Органы добывания коммерческой информации. Информационно-аналитическая служба фирмы. Источники добывания коммерческой информации. Принципы и программа добывания коммерческой информации. Технология добывания информации.

96. Основные принципы проведения телефонных переговоров и методы обеспечения их защиты от несанкционированного доступа. Совещания и переговоры в предпринимательской деятельности, организация и порядок их проведения. Требования к помещениям для проведения конфиденциальных переговоров и порядок проведения их аттестации.

97. Интеллектуальная собственность фирмы и ее оценка. Методы защиты интеллектуальной собственности. Показатели состояния защиты интеллектуальной собственности.

98. Персонал фирмы и его роль в утечке информации. Особенности подходов к профотбору. Рекомендуемые подходы к отбору персонала.

Технология отбора персонала. Обеспечение защиты информации при увольнении персонала.

99. Понятие предпринимательского риска. Экономические пределы риска. Правовые аспекты риска. Риск при принятии решения. Оценка риска. Страхование рисков.

100. Виды чрезвычайных ситуаций. Планирование действий персонала по защите информации в условиях чрезвычайных ситуаций.

101. Понятие безопасности предприятия. Объект безопасности предприятия. Цель обеспечения безопасности предприятия. Принципы построения системы безопасности предприятия. Подсистемы системы безопасности предприятия.

102. Порядок создания и ликвидации службы безопасности. Проектирование оргструктуры службы безопасности.

103. Устав службы безопасности. Структура устава. Порядок разработки, согласования и утверждения устава.

104. Система управления службой безопасности. Объект и субъект управления, прямая и обратная связь. Функции управления: прогнозирование, планирование, организация, регулирование, мотивация, контроль.

105. Механизм управления службой безопасности. Методы управления службой безопасности. Принципы управления службой безопасности. Процесс управления.

4.5. Информационная безопасность автоматизированных систем

106. Особенности защиты информации в автоматизированных информационных системах. Структура систем защиты информации от несанкционированного доступа в автоматизированных информационных системах.

107. Назначение и структура система разграничения доступа автоматизированных информационных систем. Этапы построения систем разграничения доступа автоматизированных информационных систем.

108. Современные международные и отечественные стандарты и нормативные документы в области защиты информации. Роль отраслевых стандартов и нормативных документов при построении систем защиты информации.

109. Понятие и назначение формальных модулей управления доступом.

110. Политика безопасности, дискреционная и мандатная политики безопасности.

111. Дискреционные модели управления доступом. Свойства, особенности, недостатки.

112. Мандатные модели управления доступом. Свойства, особенности, недостатки.

113. Модели тематического разграничения доступа. Свойства, особенности, недостатки.

114. Ролевые модели управления доступом. Свойства, особенности, недостатки.

115. Функционально-ролевая модель разграничения доступа. Структура, свойства, особенности, недостатки.

116. Методика проектирования систем разграничения доступа автоматизированных информационных систем.

117. Методики построения структуры информационных ресурсов предприятия.

118. Использование методов искусственного интеллекта для обеспечения информационной безопасности автоматизированных систем.

119.Применение экспертных систем в прикладных задачах информационной безопасности

120.Безопасность системы. Взлом паролей. Меры безопасности парольной аутентификации.

5. Список литературы для подготовки к вступительным испытаниям

1. Основы информационной безопасности : учебное пособие для студентов вузов / Е.В. Вострецова.— Екатеринбург : Изд-во Урал. ун-та, 2019. — 204 с. http://elar.urfu.ru/bitstream/10995/73899/3/978-5-7996-2677-8_2019.pdf
2. Ю.А.Родичев. Нормативная база и стандарты в области информационной безопасности: учебное пособие. – Издательство: Питер, 2017.- 256 с.
3. С.А.Нестеров. Основы информационной безопасности: учебное пособие. - 2-е издание. – Издательство: Озон. 2016. – 324 с.
4. В.В. Бондарев. Введение в информационную безопасность автоматизированных систем: учебное пособие. – Издательство: МГТУ им. Баумана, 2016.- 252 с.
5. Гатчин Ю.А., Сухостат В.В., Куракин А.С., Донецкая Ю.В. Теория информационной безопасности и методология защиты информации – 2-е изд., испр. и доп. – СПб: Университет ИТМО, 2018. – 100 с.
6. А.В. Бабаш, Е.К. Баранова, Д.А. Ларин. Информационная безопасность. История защиты информации в России. Изд-во: КДУ, 2015. – 736 с. ISBN 978-5-98227-928-6.
7. Е. К. Баранова, А. В. Бабаш. Информационная безопасность и защита информации. Учебное пособие. 3-е издание, переработанное и дополненное. Издательство: РИОР, Инфра-М, 2017. – 324 с. ISBN 978-5-369-01450-9, 978-5-16-011164-3.
8. В. В. Бондарев. Введение в информационную безопасность автоматизированных систем. Учебное пособие. Издательство: МГТУ им. Н. Э. Баумана, 2016. – 252 с. ISBN 978-5-7038-4414-4.
9. С. А. Нестеров. Основы информационной безопасности. Учебное пособие. 2-е издание, стереотипное.Издательство: Лань, 2016. – 324 с. ISBN 978-5-8114-2290-6
10. Ясенев В.Н., Дорожкин А.В., Матвеев В.А., Сочков А.Л., Ясенев О.В. Под общей редакцией проф. Ясенева В.Н. Информационная

безопасность: Учебное пособие.– Нижний Новгород: Нижегородский госуниверситет им. Н.И. Лобачевского, 2018. – 182 с.
11. Н. Н. Минакова. Основы управления информационной безопасностью: учебное пособие; Министерство образования и науки РФ, Алтайский государственный университет (АГУ). - Барнаул : Изд-во Алтайского гос. ун-та, 2017. - 45 с. ISBN 978-5-7904-2181-5.
12. Курило А.П., Милославская Н.Г., Сенаторов М.Ю., Толстой А.И. Основы управления информационной безопасностью. Учебное пособие для вузов. 2-е изд., испр 2016. - 244 с. ISBN 978-5-9912-0361-2.
13. Баранов С.А., Голодков Ю.Э., Демаков В.И., Кургалеева Е.Е. Основы информационной безопасности. Учебное пособие. - Иркутск, ФГОУ ВПО ВСИ МВД России, 2015, - 98 с.
14. Милославская Н.Г., Сенаторов М.Ю., Толстой А.И. Управление инцидентами информационной безопасности и непрерывностью бизнеса. Учебное пособие для вузов. 2-е издание, исправленное. 2016. - 170 с. ISBN 978-5-9912-0363-0.
15. Авдошин С. Дискретная математика. Модулярная алгебра, криптография, кодирование. - Москва: СИНТЕГ, 2016. – 260 с.
16. Жданов, О. Н. Методика выбора ключевой информации для алгоритма блочного шифрования / О.Н. Жданов. - М.: ИНФРА-М, 2015. - 607 с.
17. Гурин, А. В. Технологии встраивания цифровых водяных знаков в аудиосигнал / А.В. Гурин, А.А. Жарких, В.Ю. Пластунов. - М.: Горячая линия - Телеком, 2015. - 116 с.
18. Даниленко, А. Ю. Безопасность систем электронного документооборота. Технология защиты электронных документов / А.Ю. Даниленко. - М.: Ленанд, 2015. - 232 с.
19. Бабенко, Л. К. Современные интеллектуальные пластиковые карты / Л.К. Бабенко, Д.А. Беспалов, О.Б. Макаревич. - М.: Гелиос АРВ, 2015. - 416 с.
20. Литвинская, О. С. Основы теории передачи информации. Учебное пособие / О.С. Литвинская, Н.И. Чернышев. - М.: КноРус, 2015. - 168 с.
21. Управление рисками организации : Учебное пособие / Антонов Геннадий Дмитриевич, Валерий Максимович, Ольга Петровна. - Москва : ООО "Научно-издательский центр ИНФРА-М", 2015. - 153 с. - Для студентов высших учебных заведений. - ISBN 978-5-16-010203-0. URL: http://znanium.com/go.php?id=475625
22. Бузов Г.А., Калинин С.В., Кондратьев А.В. Защита от утечки информации по техническим каналам: Учебное пособие. - М.: Горячая линия – Телеком, 2015.
23. Гришина Наталия Васильевна. Информационная безопасность предприятия : Учебное пособие; доп. - Москва; - М.: Издательство «ФОРУМ» : ООО «Научно-издательский центр ИНФРА-М», 2016. - 240 с. - ISBN 978-5-00091-007-8. URL: http://znanium.com/go.php?id=544554
24. Кияев В.И., О.Н. Граничин Безопасность информационных систем. – М.: Национальный Открытый Университет «ИНТУИТ», 2016. - 192 с. URL: http://biblioclub.ru/index.php?page=book&id=429032

25. В.В. Ерохин, Д.А. Погонышева, И.Г. Степаненко. Безопасность информационных систем: уч. пос. -М.: ФЛИНТА: НАУКА, 2015 -184 с. SBN 978-5-9765-1904-6.
26. Безопасность информационных систем / В., О. Граничин ; В. Кияев; О. Граничин. - Москва : Национальный Открытый Университет «ИНТУИТ», 2016. - 192 с. URL: http://biblioclub.ru/index.php?page=book&id=429032
27. Е.А. Дубинин, Ф.Б. Тебуева, В.В. Копытов. Оценка относительного ущерба безопасности информационной системы. Монография. – М: РИОР, ИНФРА-М, 2015 – 192 + 11с SBN 978-5- 369-01371-7.