Фонд

оценочных средств

по дисциплине «Информационные технологии в сфере безопасности»

Уровень высшего образования

МАГИСТРАТУРА

Направление подготовки

Техносферная безопасность

Квалификация

МАГИСТР

2025 г.

Фонд оценочных средств предназначен для контроля знаний обучающихся по дисциплине *«Информационные технологии в сфере безопасности»*

Фонд оценочных средств рассмотрен и утвержден на заседании кафедры

Экологии и защиты в чрезвычайных ситуациях

Протокол № 1 от 05.09.2025г.

Заведующий кафедрой «ЭиЗЧС» Мамбетов Э.М.

Исполнители

Преподаватель Мамбетов Э.М.

5. ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

5.1. Контрольные вопросы и задания

1. Вопросы для проверки уровня обученности ЗНАТЬ
1.Информационные системы в области обеспечения безопасности.
2. Информационные ресурсы и технологии в сфере безопасности.
3. Современные информационные системы, компьютерные и информационные технологии в сфере безопасности.
4. Виды и назначение компьютерных справочно-правовых систем и информационно-поисковых систем.
5. Структуированные запросы и поиск информации.
6. Методология, принципы организации сбора, хранения и обработки информации, состав информационного обеспечения в сфере безопасности.
7. Правовые вопросы использования коммерческих и некоммерческих компьютерных и информационных технологий в области обеспечения безопасности.
8. Основные нормативно-правовые документы в области экологической, производственной, промышленной безопасности, безопасности в чрезвычайных ситуациях, охраны окружающей среды, реализованные в программном обеспечении и информационных технологиях.
9. Перспективы развития компьютерных и информационных технологий в решении практических задач в области обеспечения безопасности.
10. Характеристика и особенности задач системного анализа. Внедрение результатов анализа.
11. Проблемно-ориентированное прикладное программное обеспечение в сфере безопасности.
12. Программные средства по промышленной безопасности.
13. Автоматизация деятельности служб производственного контроля в сфере безопасности.
14. Картографическое производство. Дистанционное зондирование. Инфраструктура пространственных данных.
15. Структура ГИС
16. Цифровые карты.
17. Принципы географического анализа экологической информации.
18. Геоинформационные системы и технологии в безопасности.
19. Организационные и технические вопросы работы ГИС.
20. Природно-технические комплексы и системы, их виды и назначение.
21. Основы информационной безопасности.
22. Экспертные системы и системы принятия решений. Назначение, основные компоненты и этапы разработки экспертных систем.
23. Автоматизированные обучающие системы и дистанционные технологии в безопасности.
24. Информационные технологии для сбора данных о состоянии окружающей среды.
25. Компьютерные сети и комплексы. Локальные, городские и глобальные сети. Безопасность передачи данных.
26. Электронное правительство и межведомственное взаимодействие.
27. Межведомственный и внутренний документооборот.
28. Автоматизированные системы оценки и контроля состояния безопасности. Преимущества, недостатки, условия и ограничения применения

2. Примерные задания для проверки уровня обученности УМЕТЬ и ВЛАДЕТЬ:

1. Подготовить компьютерную презентацию для устных и стендовых научных докладов. Создание мультимедийных презентаций в PowerPoint.
2. Спроектируйте и создайте базу данных, которая позволяла бы вести учет произошедшие чрезвычайные ситуации (сход лавин, пожары, оползни, землетрясения, ДТП, аварии различного характера и др.). Подумайте о лучшем способе организации данных. Включите в базу данных удобные инструменты (формы,отчеты) для работы с ней. Создайте запросы, которые позволяли бы получать данные и подобную статистическую информацию (в том числе и в виде диаграмм). Подумайте о средствах обеспечения целостности и корректности данных.
3. База данных пожаров по г. Бишкек за последние 50 лет, вывести причины, сделать диаграмму.
4. Создать диаграмму в Access (сводную диаграмму) в которой отображается количество землетрясений за последние 100 лет.
5. Создать диаграмму в Access (сводную диаграмму) в которой отображается количество сошедших оползней за последние 50 лет (по областям).
6. Создать базу данных в программе EXEL произвести расчеты и вывести диаграмму.
7. Создать базу данных в СУБД Access в Microsoft Windows.
8. На основе геоинформационных систем, на примере программы QGIS создать базу данных.
9. Создать Web-страницу. Гиперссылки, списки, формы Web- страниц.

Примерные вопросы к зачету с оценкой.
Билет №1.
1. Организационные и технические вопросы работы ГИС
2. Информационные ресурсы и технологии в сфере безопасности.
3. На основе геоинформационных систем, на примере программы QGIS создать базу данных.

5.2. Темы курсовых работ (проектов)

Учебным планом курсовая работа не предусмотрена

5.3. Фонд оценочных средств

Вопросы к коллоквиуму:
1. Информационные технологии в сфере безопасности.
2. Коммуникационные технологии.
3. Использование современных компьютерных технологий во всех сферах деятельности человечества.
4. Локальные компьютерные сети. Конфигурации локальных сетей и организация обмена информацией.
5. Глобальные компьютерные сети, принципы построения и организация ресурсов и служб, протоколы коммуникаций.
6. Протокол передачи данных TCP/IP.
7. Протокол обмена файлами FTP.
8. Протокол передачи гипертекста HTTP.
9. Всемирная паутина.
10. Технология WWW.
11. Браузеры.
12. Файловые архивы.
13. Электронная почта, электронные журналы и конференции.
14. Модель взаимодействия объектов электронной почты.
15. Программное обеспечение.
16. Универсальные поисковые системы Internet и библиографические ресурсы Internet.
17. Поиск научно-технической информации в Интернет.
18. Образовательные и научные порталы.
19. Защита информации в Internet.
20. Компьютерная безопасность и компьютерная преступность.
21. Правовая охрана программ и данных.
22. Защита информации.
23. Лицензионные, условно бесплатные и бесплатные программы.

Тематика докладов
1. Управление информационной безопасностью
2. Организация безопасности образовательной среды
3. Информационная безопасность в сети Интернет
4. Политика безопасности
5. Система комплексного обеспечения безопасности жизнедеятельности города
6. Организация информационной безопасности и безопасного использования сети Интернет в ВУЗах
7. Правовые возможности парирования угроз информационной безопасности
8. Понятие, теория и практика информационной безопасности
9. Формирование информационной культуры и безопасности среди магистрантов
10. Комплексный подход к вопросам обеспечения информационной безопасности и защиты персональных данных
11. Системы электронного документооборота (СЭД) в безопасности: основные понятия, назначение, стандарты и примеры внедрения.
12. Интеграция СЭД с другими приложениями.
13. Особенности выбора и внедрения СЭД для решения задач в сфере безопасности.
14. Основные правила оформления документов. Создание и редактирования стилей, включая стили для формул.
15. Типы графических изображений и соответствующие файловые форматы. Примеры программ. Параметры растровых изображений.
16. Использование программы Statistica для выполнения профессиональных задач.
17. Примеры аппаратных средств реализации информационных процессов в сфере безопасности.
18. Программные продукты и методы, используемые при создании картографической информации. Основные методы картирования и работы с картами в сети Интернет.
19. Системы управления базами данных (СУБД).
20. Назначение и применение баз данных и знаний в сети Интернет.
21. Использование сети Интернет, как источника информации по проблемам безопасности и охраны окружающей среды.
22. Информационное обеспечение экологической и промышленной безопасности с использованием возможностей портала государственных услуг электронного правительства и многофункционального центра предоставления государственных услуг.
23. Современные компьютерные и информационные технологии в области обеспечения безопасности. Основы работы с информационными ресурсами в сфере безопасности: виды, назначение и условия доступа.
24. Возможности информационно-справочных, поисковых и нормативно-правовых систем.
25. Основные программные продукты, предназначенные для обеспечения безопасности природно-технических систем и комплексов.
26. Использование в профессиональной деятельности программных продуктов.
27. Применение в профессиональной деятельности топографических карт и карт градостроительного районирования города. Использование пространственных данных и картографических материалов в сети Интернет.
28. Обработка экспериментальных данных и методов решения практических задач с использованием программных комплексов.

Темы самостоятельных работ в содержании дисциплины.

Презентация базы данных 1. Создание базы в программе Excel 2. Создание базы в программе Qgis 3. Использование данных из программы Access
5.4. Перечень видов оценочных средств
активность, посещаемость, конспект, выполнение самостоятельных работ; коллоквиум, реферат с защитой презентации, доклад, тесты (шкалы оценивания по всем видам оценочных средств приведены в Приложении 1)

6. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

6.1. Рекомендуемая литература

6.1.1. Основная литература

	Авторы, составители	Заглавие	Издательство, год
Л1.1		Информатика. Свободное и открытое программное обеспечение:Учебное пособие/Под ред. В.П. Живоглядова	Бишкек : Изд-во КРСУ ,
Л1.2	Таненбаум Э.С.	Современные операционные системы	СПб.:Питер 2015
Л1.3	Хлебников А.А.	Информационные технологии: Учебник для студентов ВУЗов	2014
Л1.4	Дьяконов В.П.	MATLAB. Полный самоучитель: Самоучитель	Litres 2017
Л1.5	Е.В. Акимова	Информационные системы и технологии в экономике и управлении. Техническое и программное обеспечение: учебное пособие	Саратов: Вузовское образование 2016
Л1.6	Кудинов Ю.И., Суслова С.А.	Современные информационные технологии: Учебное пособие	Липецкий государственный технический университет, ЭБС АСВ 2013
Л1.7	Ю.Ф. Тельнова.	Информационные системы и технологии: Научное	М.: ЮНИТИ 2016

6.1.2. Дополнительная литература

	Авторы, составители	Заглавие	Издательство, год
Л2.1	Фролов А. В., Фролов Г. В.	Базы данных в Интернете: практическое руководство по созданию WEB- приложений с базами данных	М.: Русская Редакция 2000
Л2.2	Карпова Т.	Базы данных. Модели, разработка, реализация: учебник	СПб.: Питер 2002
Л2.3	Мастрюков Б.С.	Безопасность в чрезвычайных ситуациях в природно-техногенной сфере. Прогнозирование последствий: учебное пособие для студ. учреждений высш. проф.	М.: Издательский центр "Академия" 2011
Л2.4	Пьянзин М.П., Борисов А.Ф.	Чрезвычайные ситуации (источники, погноз, защита): учебное пособие	НГАСУ. Вента Н.Новгород 2004
Л2.5	Шадрина Н.И.	Лабораторный практикум по приложениям Microsoft Word и Excel 2010: учебное пособие	Хабаровск: Изд-во Тихоокеан. гос. ун-та 2014
Л2.6	Баженова И.Ю.	Основы проектирования приложений баз данных [Электронный ресурс] : учебное пособие	ИНТУИТ 2017

6.1.3. Методические разработки

	Авторы, составители	Заглавие	Издательство, год
Л3.1	Айдаралиев Б.Р., Ордобаев Б.С., Абдыкеева Ш.С.	Терминологический словарь по чрезвычайным ситуациям: словарь	Бишкек: Изд-во КРСУ 2013
Л3.2	Джаманкулова Г.М., Ордобаев Б.С.	Безопасность в чрезвычайных ситуациях: учебное пособие	Бишкек: Изд-во КРСУ 2017

6.2. Перечень ресурсов информационно-телекоммуникационной сети "Интернет"

Э1	www.elibrary.ru - Научная электронная библиотека eLIBRARY.RU	www.elibrary.ru - Научная электронная библиотека
Э2	http://scientbook.com - Свободная информационная площадка научного общения. Инструмент коммуникации, поиска людей и научных знаний.	http://scientbook.com - Свободная
Э3	http://www.iprbookshop.ru.- Электронно-библиотечная система IPRbooks	http://www.iprbookshop.ru.- Электронно-библиотечная

Э4	http://www.public.ru - Интернет-библиотека предлагает широкий спектр информационных услуг: от доступа к электронным архивам публикаций русскоязычных СМИ и готовых тематических обзоров прессы до индивидуального мониторинга и эксклюзивных аналитических исследований, выполненных по материалам печати.	http://www.public.ru - Интернет-библиотека
Э5	http://scientbook.com - Свободная информационная площадка научного общения. Инструмент коммуникации, поиска людей и научных знаний.	http://scientbook.com - Свободная

6.3. Перечень информационных и образовательных технологий	
6.3.1 Компетентностно-ориентированные образовательные технологии	
6.3.1.1	Для успешного овладения дисциплиной используются следующие инновационные и информационные технологии обучения:
6.3.1.2	• при проведении занятий используются презентации материала в программе Microsoft Office (PowerPoint), выход на профессиональные сайты, использование видеоматериалов различных интернет-ресурсов
6.3.1.3	• практические занятия по дисциплине проводятся с применением необходимого методического материала (методические указания, справочники, нормативы и т.п.)
6.3.1.4	• занятия по дисциплине проводятся в специализированной учебной аудитории – компьютерном классе
6.3.1.5	В процессе изучения дисциплины учебными целями являются первичное восприятие учебной информации о теоретических основах и принципах работы с документами (карты, планы, схемы, регламенты), ее усвоение, запоминание, а также структурирование полученных знаний и развитие интеллектуальных умений, ориентированных на способы деятельности. Посредством использования этих интеллектуальных умений достигаются узнавание ранее усвоенного материала в новых ситуациях, применение абстрактного знания в конкретных ситуациях.
6.3.1.6	Для достижения этих целей используются в основном традиционные информативно- развивающие технологии обучения с учетом различного сочетания пассивных форм (практическое занятие, консультация, самостоятельная работа) и репродуктивных методов обучения (повествовательное изложение учебной информации, объяснительно- иллюстративное изложение) и практических методов обучения (выполнение заданий на
6.3.1.7	Университет обеспечен необходимым комплектом лицензионного программного обеспечения:
6.3.1.8	• операционных системы Microsoft Windows;
6.3.1.9	• офисный пакет приложений Microsoft Office;
6.3.1.10	• программная система для обнаружения текстовых заимствований в учебных и научных работах «Антиплагиат.ВУЗ».
6.3.2 Перечень информационных справочных систем и программного обеспечения	
6.3.2.1	Электронная библиотека при Учебно-научном техническом центре «Развитие гражданской защиты» Кулатова 11.
6.3.2.2	http://www.iprbookshop.ru.- Электронно-библиотечная система IPRbooks
6.3.2.3	www.elibrary.ru - Научная электронная библиотека eLIBRARY.RU
6.3.2.4	http://www.public.ru - Интернет-библиотека предлагает широкий спектр информационных услуг: от доступа к электронным архивам публикаций русскоязычных СМИ и готовых тематических обзоров прессы до индивидуального мониторинга и эксклюзивных аналитических исследований, выполненных по материалам печати.
6.3.2.5	http://e.lanbook.com - Ресурс, включающий в себя как электронные версии книг издательства «Лань» и других ведущих издательств учебной литературы, так и электронные версии периодических изданий по естественным, техническим и гуманитарным наукам.
6.3.2.6	http://scientbook.com - Свободная и информационная площадка научного общения. Инструмент коммуникации, поиска людей и научных знаний.

7. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)	
7.1	Реализация учебного процесса осуществляется в специальных учебных аудиториях университета для проведения занятий, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации. Все аудитории укомплектованы специализированной мебелью и техническими средствами обучения, служащими для представления учебной информации большой аудитории. Самостоятельная работа обучающихся выполняется в специализированной аудитории, которая оборудована учебной мебелью, компьютерной техникой с возможностью подключения к сети «Интернет» и обеспечением доступа в электронную информационно- образовательную среду. Помещения для проведения, практических занятий и самостоятельных занятий укомплектованы необходимой специализированной учебной мебелью и техническими средствами для представления учебной информации магистрантам. Практические и самостоятельные работы проводятся в 10 корпусе ФАДиС, 305 ауд. где имеется 20 посадочных мест и 15 компьютеров.

8. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ (МОДУЛЯ)

1. Технологическая карта дисциплины: Информационные технологии в сфере безопасности представлена а ПРИЛОЖЕНИИ 1.

2. МОДУЛЬНЫЙ КОНТРОЛЬ ПО ДИСЦИПЛИНЕ ВКЛЮЧАЕТ:
1. Текущий контроль: усвоение учебного материала на аудиторных занятиях (лекциях, практических, лабораторных работах, в том числе учитывается посещение и активность) и выполнение обязательных заданий для самостоятельной работы и тестов.
2. Рубежный контроль: проверка полноты знаний и умений по материалу модуля в целом. Выполнение модульных заданий проводится в письменном виде и является обязательной компонентой модульного контроля.
3. Промежуточный контроль - завершенная задокументированная часть учебной дисциплины – совокупность тесно связанных между собой зачетных модулей.
ОСНОВНЫЕ ТРЕБОВАНИЯ К ПРОМЕЖУТОЧНОМУ КОНТРОЛЮ
При явке на зачёт студенты обязаны иметь при себе зачётные книжки, которые они предъявляют экзаменатору в начале зачета.
Преподавателю предоставляется право поставить зачёт без опроса по билету тем студентам, которые набрали более 60 баллов за текущий и рубежный контроли.
На промежуточном контроле студент должен верно ответить на теоретические вопросы билета.
Студенты могут использовать технические средства, справочно-нормативную литературу, наглядные пособия, учебные программы.
Оценка промежуточного контроля:
- min 20 баллов - Вопросы для проверки уровня обученности ЗНАТЬ (в случае, если при ответах на заданные вопросы студент правильно формулирует основные понятия)
- 20-25 баллов – Задания для проверки уровня обученности УМЕТЬ и ВЛАДЕТЬ(в случае, если студент правильно формулирует сущность заданной в билете проблемы и дает рекомендации по ее решению)
- 25-30 баллов - Задания для проверки уровня обученности УМЕТЬ и ВЛАДЕТЬ (в случае полного выполнения контрольного задания)
ОСНОВНЫЕ ТРЕБОВАНИЯ К ТЕКУЩЕМУ КОНТРОЛЮ.
Для понимания материала и качественного его усвоения рекомендуется такая последовательность действий:
1. После прослушивания лекции и окончания учебных занятий, при подготовке к занятиям следующего дня, нужно сначала просмотреть и обдумать текст лекции, прослушанной сегодня.
2. При подготовке к следующей лекции, нужно просмотреть текст предыдущего материала, подумать о том, какая может быть тема следующей лекции.
3. В течение недели выбрать время для работы с рекомендуемой литературой.
4. При подготовке к семинарским занятиям следующего дня, необходимо сначала прочитать основные понятия и подходы по теме домашнего задания. При выполнении задания нужно сначала понять, что в нем требуется, какой теоретический материал нужно использовать, наметить план решения.
5. Для подготовки к семинарским занятиям и выполнению самостоятельной работы необходимо сначала прочитать основные понятия и подходы по теме задания. Рекомендуется использовать методические указания по курсу, глоссарий, конспекты лекций. При выполнении задания нужно сначала понять, что требуется в нем, какой теоретический материал нужно использовать, наметить план выполнения, а затем приступить к заданию и сделать качественный вывод.
6. При подготовке к промежуточному и рубежному контролям нужно изучить теорию: определения всех понятий и подходы к оцениванию до состояния понимания материала и самостоятельно выполнить несколько типовых заданий.
7. Отработки пропущенных занятий.
Контроль над усвоением студентами материала учебной программы дисциплины осуществляется систематически преподавателем кафедры и отражается в журнале преподавателя и в баллах. Студент, получивший неудовлетворительную оценку по текущему материалу, обязан подготовить данный раздел и ответить по нему преподавателю на индивидуальном собеседовании. При фронтальном обучении неудовлетворительная оценка должна быть отработана в течение месяца со дня ее получения, при цикловом обучении - до конца цикла.
Пропущенная без уважительных причин лекция должна быть отработана методом устного опроса лектором или подготовки реферата по материалам пропущенной лекции в течение месяца со дня пропуска. Возможны и другие методы отработки пропущенных лекций (опрос на практических, тестовый контроль и т.д.).
Отработка семинарских занятий.
- Каждое занятие, пропущенное студентом без уважительной причины, отрабатывается в обязательном порядке. Отработки проводятся по расписанию кафедры, согласованному с деканатом.
- При фронтальном обучении пропущенные занятия должны быть отработаны в течение 10 дней со дня пропуска, при цикловом обучении - до конца цикла. Пропущенные студентом без уважительной причины семинарские занятия отрабатываются не более одного занятия в день. Пропущенные занятия по уважительной причине (по болезни, пропуски с разрешения деканата) отрабатываются по тематическому материалу без учета часов.
- Студент, не отработавший пропуск в установленные сроки, допускается к очередным занятиям только при наличии разрешения декана или его заместителя в письменной форме. Не разрешается устранение от очередного практического занятия студентов, слабо подготовленных к данным занятиям. - Для студентов, пропустивших семинарские занятия из-за длительной болезни, отработка должна проводиться после разрешения деканата по индивидуальному графику, согласованному с кафедрой.
- В исключительных случаях (участие в межвузовских конференциях, соревнованиях, олимпиадах, дежурство и др.) декан и его заместитель по согласованию с кафедрой могут освобождать студентов от отработок некоторых пропущенных занятий.

3. Методические указания для самостоятельной работы обучающихся

Самостоятельная работа способствует закреплению навыков работы с учебной и научной литературой, осмыслению и закреплению теоретического материала по умению аргументировано применять информационные технологии для прикладного применения в науке и производственной деятельности, направленного на обеспечение безопасности.
Самостоятельная работа выполняется во внеаудиторное (аудиторное) время по заданию и при методическом руководстве преподавателя, но без его непосредственного участия (при частичном непосредственном участии преподавателя, оставляющем ведущую роль в контроле за работой магистрантов).
Формы самостоятельной работы магистрантов разнообразны. Они включают в себя:
− знакомство, изучение и систематизацию официальных государственных документов: законов, постановлений, указов, нормативно-инструкционных и справочных материалов с использованием информационно-поисковых систем глобальной сети «Интернет» в Приложении 7 представлен Глоссарий.
− изучение учебной, научной и методической литературы, материалов периодических изданий с привлечением электронных средств официальной, статистической, периодической и научной информации;
− создание презентаций и докладов.
В процессе изучения дисциплины «Информационные технологии в сфере безопасности» магистрами направления 20.04.01 «Техносферная безопасность» основными видами самостоятельной работы являются:
-подготовка к аудиторным занятиям (практическим занятиям) и выполнение соответствующих заданий;
-самостоятельная работа над отдельными темами учебной дисциплины в соответствии с учебно-тематическим планом;
-подготовка доклада и презентации;
-подготовка реферата к зачету с оценкой.

3. Подготовка к практическим работам.
Выполнение индивидуальной практической работы является частью самостоятельной работы обучающегося и предусматривает индивидуальную работу магистрантов с учебной, технической и справочной литературой по соответствующим разделам курса.
Руководитель из числа преподавателей кафедры осуществляет текущее руководство, которое включает: систематические консультации с целью оказания организационной и научно-методической помощи студенту; контроль над выполнением работы в установленные сроки; проверку содержания и оформления завершенной работы.
Практическая работа выполняется обучающимся самостоятельно и должна быть представлена к проверке преподавателю до начала экзаменационной сессии. Выполняемая работа должна быть защищена магистрантом. Студенты, не выполнившие практические работы, к сдаче (зачета) экзамена не допускаются. Работа должна быть аккуратно оформлена в печатном или письменном виде, удобна для проверки и хранения. Защита работы может носить как индивидуальный, так и публичный характер.

4. Методические рекомендации по проведению коллоквиума
Коллоквиум (в переводе с латинского “беседа, разговор”) – форма учебного занятия, понимаемая как беседа преподавателя с учащимися с целью активизации знаний. Коллоквиум проводится в середине семестра или после изучения раздела в форме опроса с билетами.
Коллоквиум — форма проверки и оценивания знаний учащихся в системе образования. Представляет собой мини-экзамен, проводимый в середине семестра и имеющий целью уменьшить список тем, выносимых на зачет или экзамен. Оценка, полученная на коллоквиуме, может влиять на оценку на зачет или экзамен. Формы коллоквиума Коллоквиум может проводится в устной и письменной форме. Устная форма. Ответы оцениваются одновременно в традиционной шкале ("неудовлетворительно" — "отлично"). Билеты содержат как теоретические вопросы, так и задачи практического характера. На коллоквиум выносится часть материала экзамена. Оценка за коллоквиум учитывается при выставлении финальной оценки за экзамен.
Коллоквиум не переписывается, но магистранты, набравшие менее пяти баллов, сдают письменный зачет или экзамен по отдельным вариантам, содержащим, в том числе и вопросы коллоквиума. Задачи коллоквиума.
Коллоквиум ставит следующие задачи:
- проверка и контроль полученных знаний по изучаемой теме;
- расширение проблематики в рамках дополнительных вопросов по данной теме;
- углубление знаний при помощи использования дополнительных
материалов при подготовке к занятию;
- магистранты должны продемонстрировать умения работы с различными видами исторических источников;
- формирование умений коллективного обсуждения (поддерживать диалог в микрогруппах, находить компромиссное решение, аргументировать свою точку зрения, умение слушать оппонента, готовность принять позицию другого учащегося;)
Этапы проведения коллоквиума
1. Подготовительный этап:
- Формулирование темы и проблемных вопросов для обсуждения (преподаватель должен заранее продумать проблемные вопросы, в соответствии с уровнем учащихся в группе и создать карточки, вопросы в которых будут дифференцироваться по уровню сложности);
- Предоставление списка дополнительной литературы;
- Постановка целей и задач занятия;
- Разработка структуры занятия;
- Консультация по ходу проведения занятия;
2. Начало занятия:
- Подготовка аудитории: поскольку каждая микрогруппа состоит из 5-7 магистрантов, то парты нужно соединить по две, образовав квадрат, и расставить такие квадраты по всему помещению.
- Комплектация микрогрупп.

- Раздача вопросов по заданной теме для совместного обсуждения в микрогруппах.
3. Подготовка учащихся по поставленным вопросам.
4. Этап ответов на поставленные вопросы:
- В порядке установленном преподавателем, представители от микрогрупп зачитывают выработанные, в ходе коллективного обсуждения, ответы;
- магистранты из других микрогрупп задают вопросы отвечающему, комментируют и дополняют предложенный ответ;
- Преподаватель регулирует обсуждения, задавая наводящие вопросы, корректируя неправильные ответы (важно, чтобы преподаватель не вмешивался напрямую в ход обсуждения, не навязывал собственную точку зрения);
- После обсуждения каждого вопроса необходимо подвести общие выводы и логично перейти к обсуждению следующего вопроса (важно вопросы распределить таким образом, чтобы ответы микрогрупп чередовались);
- После обсуждения всех предложенных вопросов преподаватель подводит общие выводы;
5. Итог:
- Преподаватель должен соотнести цели и задачи данного занятия и итоговые результаты, которых удалось добиться;
- Заключительный этап суммирует все достигнутое с тем, чтобы дать новый импульс для дальнейшего изучения и решения обсуждавшихся вопросов (в рамках одного занятия невозможно решить все поставленные проблемы, одна из задач подобного вида занятий,
спровоцировать интерес к обсуждаемым проблемам);
- Преподаватель должен охарактеризовать работу каждой микрогруппы, выделить наиболее грамотные и корректные ответы учащихся.
темы коллоквиума в приложении 5.

5. ДОКЛАД составляется по заданной тематике, предполагает подбор необходимого материала и его анализ, определение его актуальности и достаточности, формирование плана доклада или структуры выступления, таким образом, чтобы тема была полностью раскрыта. Изложение материала должно быть связным, последовательным, доказательным. Способ изложения материала для выступления должен носить конспективный или тезисный характер
Подготовка доклада к занятию.
Основные этапы подготовки доклада:
• выбор темы;
• консультация преподавателя;
• подготовка плана доклада;
• работа с источниками и литературой, сбор материала;
• написание текста доклада;
• оформление рукописи и предоставление ее преподавателю до начала доклада, что определяет готовность студента к выступлению;
• выступление с докладом, ответы на вопросы.
Тематика доклада предлагается преподавателем в ФОС.

6. ПУБЛИЧНАЯ ЗАЩИТА ПРЕЗЕНТАЦИИ

Этапы подготовки презентации
Составление плана презентации (постановка задачи; цели данной работы)
Продумывание каждого слайда (на первых порах это можно делать вручную на бумаге), при этом важно ответить на вопросы:
- как идея этого слайда раскрывает основную идею всей презентации?
- что будет на слайде?
- что будет говориться?
- как будет сделан переход к следующему слайду?
Изготовление презентации с помощью MS PowerPoint:
- Имеет смысл быть аккуратным. Неряшливо сделанные слайды (разнобой в шрифтах и отступах, опечатки, типографические ошибки в формулах) вызывают подозрение, что и к содержательным вопросам студент – докладчик подошёл спустя рукава.
- Титульная страница необходима, чтобы представить аудитории Вас и тему Вашего доклада.
- Количество слайдов не более 30.
- Оптимальное число строк на слайде — от 6 до 11.
- Распространённая ошибка — читать слайд дословно. Лучше всего, если на слайде будет написана подробная информация (определения, формулы), а словами будет рассказываться их содержательный смысл. Информация на слайде может быть более формальной и строго изложенной, чем в речи.
- Оптимальная скорость переключения — один слайд за 1–2 минуты.
- Приветствуется в презентации использовать больше рисунков, картинок, формул, графиков, таблиц. Можно использовать эффекты анимации.
- При объяснении таблиц необходимо говорить, чему соответствуют строки, а чему — столбцы.
- Вводите только те обозначения и понятия, без которых понимание основных идей доклада невозможно.
- В коротком выступлении нельзя повторять одну и туже мысль, пусть даже другими словами — время дорого.
- Любая фраза должна говориться зачем-то. Тогда выступление будет цельным и оставит хорошее впечатление.
- Последний слайд с выводами в коротких презентациях проговаривать не надо.
- Если на слайде много формул, рекомендуется набирать его полностью в MS Word (иначе формулы приходится размещать и выравнивать на слайде вручную). Для этого удобно сделать заготовку — пустой слайд с одним большим Word-объектом «Вставка / Объект / Документ Microsoft Word», подобрать один раз его размеры и размножить на нужное число слайдов.

Основной шрифт в тексте и формулах рекомендуется изменить на Arial или ему подобный; шрифт Times плохо смотрится издалека. Обязательно установите в MathType основной размер шрифта равным основному размеру шрифта в тексте. Никогда не выравнивайте размер формулы вручную, вытягивая ее за уголок. загрязнения воздуха в некоторые часы может превышать предельно допустимые концентрации в 10 и более раз (Лихачева, Смирнова, 2006) ...

7. Тесты. По данной дисциплине имеются 3 теста. В одном тестовом задании 20 закрытых вопросов. К заданиям даются готовые ответы на выбор, один правильный и остальные неправильные.
Обучающемуся необходимо помнить: в каждом задании с выбором одного правильного ответа правильный ответ должен быть.За каждый правильный ответ – 1 балл. Общая оценка определяется как сумма набранных баллов. Тесты в приложении 2,3,4.

Все темы текущего, рубежного контроля выдаются на первом практическом занятии, уточняются даты сдачи заданий. Шкалы оценивания представлены в Приложении 6.

8. Проведение интерактивных занятий:

Мозговой штурм
Мозговой штурм («мозговая атака») – это практическое занятие, в ходе которого поиск решения проблемы осуществляется через стимулирование творческой активности, когда участникам обсуждения предлагают высказывать как можно большее количество вариантов решения, из которых в дальнейшем выбирается наиболее удачное для использования на практике.
Основной целью мозгового штурма является стимулирование у студентов творческой активности, динамичности мыслительных процессов, абстрагирования от привычных взглядов и сосредоточения на какой-либо конкретной практической цели.
Метод мозгового штурма характеризуется отсутствием критики поисковых усилий, сбором всех гипотез, рожденных в поиске, их анализом на перспективу использования для снятия затруднений в практике.
Структура подготовки и проведения мозгового штурма.
1. Постановка цели и задач.
2. Подготовка к проведению мозгового штурма.
Преподаватель:
• подбирает материал;
• разрабатывает сценарий;
• определяет методы, приемы и средства стимулирования творческой и мыслительной активности студентов;
• подбирает наглядный материал и техническое сопровождение.
Студент:
• самостоятельно прорабатывает материал по теме занятия.
При разработке сценария мозгового штурма преподаватель должен помнить о том, что сценарий включает в себя следующие компоненты:
• формулирование проблемы, которую необходимо решить;
• формирование рабочих групп по 3 – 4 человека и экспертной группы, способной отобрать наилучшие идеи и разработать показатели и критерии оценки;
• тренировочная интеллектуальная разминка для приведения обучаемых в рабочее психологическое состояние за счет активизации их знаний, обмена мнениями и выработки общей позиции по проблеме;
• собственно мозговой штурм, решение поставленной проблемы;
• оценка и отбор наилучших идей экспертной группой;
• обобщение результатов мозгового штурма, подведение итогов работы учебных групп, оценка наилучших идей, их обоснование и публичная защита.
3. Проведение мозгового штурма.
Мозговой штурм начинается с проведения тренировочной интеллектуальной разминки, основной задачей которой является определение уровня подготовленности слушателей к дальнейшей работе. Она позволяет студентам максимально освободиться от воздействия сковывающих факторов, психологических барьеров и дискомфорта.
Тренировочная интеллектуальная разминка осуществляется в форме экспресс – опроса. Преподаватель обращается к студентам с вопросом, на который те должны дать краткий ответ. При затруднении одного отвечающего преподаватель спрашивает другого. Таким образом, в течение 10 – 15 мин. в учебной аудитории проверяется понимание исходных понятий, категорий, принципов, основных теоретических положений и производится подготовка к дальнейшей активной познавательной деятельности.
Генерирование идей, то есть сам «мозговой штурм», начинается с подачи преподавателем сигнала о начале работы в учебных группах. Экспертная группа фиксирует и анализирует выдвинутые идеи.
При проведении мозгового штурма необходимо соблюдать следующие правила:
1. Любая возникшая идея, неважно насколько она осуществима, должна быть выслушана.
2. Любой может высказать одну или несколько идей одновременно, чтобы не заблокировать свою фантазию.
3. Остальные члены группы должны воздерживаться от критики в адрес выступающего с идеей.
4. После того как идеи высказали все члены группы, происходит их последовательное обсуждение и выработка общего решения.
5. Несогласный с общим решением имеет право выступить с особым мнением на этапе защиты темы. После подачи сигнала о завершении работы в группах, начинается публичная защита выдвинутых идей с их обоснованием. По результатам защит экспертная комиссия проводит оценку представленных идей. В завершении занятия подводятся итоги всей работы и обобщаются результаты мозгового штурма.

ПРИЛОЖЕНИЕ 1

ТЕХНОЛОГИЧЕСКАЯ КАРТА ДИСЦИПЛИНЫ " ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ В СФЕРЕ БЕЗОПАСНОСТИ "

Курс 1, семестр 1, Количество ЗЕ –4, Отчетность – зачет с оценкой

Название модулей дисциплины согласно РПД	Контроль	Форма контроля	зачетный минимум	зачетный максимум	график контроля
Модуль 1					
Информационные технологии в сфере безопасности. Коммуникационные технологии	Текущий	Активность, посещаемость, выполнение самостоятельных заданий, фронтальный опрос по тестам	4	5	5 неделя
	Рубежный	Коллоквиум	6	10	
Модуль 2					
Современные технологии и средства создания информационных ресурсов. Современные компьютерные технологии в образовании и безопасности.	Текущий	Активность, посещаемость, выполнение самостоятельных заданий, фронтальный опрос по тестам	4	5	10 неделя
	Рубежный	Доклад	6	10	
Модуль 3					
Базы данных	Текущий	Активность, посещаемость, выполнение самостоятельных заданий, фронтальный опрос по тестам	4	8	15 неделя
	Рубежный	Презентация базы данных	6	12	
Модуль 4					
Базы данных	Текущий	Активность, посещаемость, выполнение самостоятельных заданий,	4	8	18 неделя
	Рубежный	Презентация базы данных	6	12	
ВСЕГО за семестр			40	70	19 неделя
Промежуточный контроль (Зачет с оценкой)			20	30	
Семестровый рейтинг по дисциплине			60	100	

Примечание:

1. За каждое пропущенное и не отработанное лекционное и практическое занятие снимается 1 балл.

2. За активное участие на семинарском и практическом занятии добавляется 1 балл.

ПРИЛОЖЕНИЕ 2

ДЕМОНСТРАЦИОННЫЕ ВАРИАНТЫ ВОПРОСОВ (фронтальный опрос на семинарских занятиях)

ТЕСТ № 1. ДЛЯ ТЕКУЩЕГО КОНТРОЛЯ

1. Информация – это:

а) данные;

б) сведения;

в) процесс.

2. Графический вид информации:

а) это воспринимаемая органами зрения информация;

б) содержит тривиальные сведения и оперирует набором понятий, понятным большей части социума;

в) в виде изображений, предметов, графиков и т.д.

3. Информация – используемая в разделе прикладной математики, радиотехнике, информатики, относящийся к измерению количества информации, ее свойств и устанавливающий предельные соотношения для систем передачи данных и является:

а) теорией информации;

б) информатикой;

в) математикой.

4. Аспект семиотики, которая использует связь с адресатом, т.е. проблемы интерпретации знаков теми, кто их использует, их полезности и ценности для интерпретатора, называется:

а) синтаксис (синтактика);

б) семантика;

в) прагматика.

5. Свойство информации соответствовать нуждам потребителя в нужный момент времени:

а) достоверность;

б) своевременность;

в) эргономичность.

6. Свойство информации однозначно соответствовать отображенному объекту или явлению:

а) адекватность;

б) защищенность;

в) релевантность.

7. Дезинформация – это:

а) информация, в предоставлении которой на практике органы власти часто отказывают гражданину на том основании, что запрошенные сведения непосредственным образом не затрагивают его права;

б) информация о законе «об обеспечении доступа к информации о деятельности государственных органов и органов местного самоуправления»;

в) один из способов манипулирования информацией, как то: введение кого-либо в заблуждение путем предоставления неполной информации или полной, но уже не нужной информации, или полной, но не в нужной области, искажения контекста, искажения части информации.

8. Информационный процесс – это:

а) процесс получения, создания, сбора, обработки, накопления, хранения, поиска, распространения и использования информации;

б) процесс, против которого накоплена дезинформация, принятие нужного решения, нужных данных;

в) процесс информационного права и свободы.

9. Информационный процесс, исполняющий совокупность спланированных действий над имеющейся информацией с целью получения новой:

а) представление информации;

б) обработка информации;

в) сбор информации.

10. Поиск информации – это:

а) нахождение первоначальной информации с целью ее дальнейшего применения (методы: наблюдение, измерение, опросы, анкетирование, тестирование и т.д.);

б) приведение информации в форму, наиболее удобную для ее использования (методы: сортировка, систематизация, подача в табличной или графической форме);

в) выявление нужной информации в информационных системах (каталоги, справочники, поисковые системы и т.д.).

11. Обоснованное принятие решений в разных видах человеческой деятельности:

а) использование информации;

б) передача информации;

в) хранение информации.

12. Введение определенных мер с целью предотвращения потери, повреждения или злоумышленного использования информации:

а) представление информации;

б) защита информации;

в) блокирование информации.

13. Материальный объект, который применяется для ее хранения и передачи информации в пространстве и времени, называются ее:

а) объектом;

б) свойством;

в) носителем.

14. Вид по сроку хранения, носителя, который используется для хранения информации:

а) долго существующие;

б) коротко существующие;

в) звуковая волна.

15. Постоянное увеличение скорости и объемов публикаций (объема информации) в масштабах планеты, лавинообразное настроение массы разнообразной информации в современном обществе:

а) информационный барьер;

б) информационная культура;

в) информационный взрыв.

16. Противоречие между информационными запросами общества и техническими возможностями их обеспечения это:

а) информационный взрыв;

б) информационный барьер;

в) информационная культура.

17. Процесс обеспечения конфиденциальности, целостности и доступности информации:

а) защита информации;

б) информационная безопасность;

в) процесс конфиденциальности.

18. Важнейший критерий при принятии решений о защите информации – уровень секретности – это административная или законодательная мера, соответствующая мере ответственности лица за утечку или потерю секретной конкурентной информации, регламентируемой специальным документом с учетом государственно-военной стратегической, коммерческих, служебных или частных интересов:

а) ценность информации;

б) информационная безопасность;

в) защита информационной конфиденциальности.

19. Избежание несанкционированной модификации информации:

а) конфиденциальность;

б) целостность;

в) доступность.

20. Подотчетность модели безопасности – это:

а) свойство, гарантирующее, что субъект или ресурс идентичны заявленным;

б) свойство соответствия предусмотренному поведению или результату;

в) свойство, обеспечивающее однозначное прослеживание действий любого логического объекта.

ПРИЛОЖЕНИЕ 3

ДЕМОНСТРАЦИОННЫЕ ВАРИАНТЫ ВОПРОСОВ
(фронтальный опрос на семинарских занятиях)

ТЕСТ № 2. ДЛЯ ТЕКУЩЕГО КОНТРОЛЯ

1) Автоматизация офиса:

a) предназначена для решения хорошо структурированных задач, по которым имеются необходимые входные данные и известны алгоритмы и другие стандартные процедуры их обработки;

b) предназначена для удовлетворения информационных потребностей всех сотрудников организации, имеющих дело с принятием решений;

c) первоначально была призвана избавить работников от рутинной секретарской работы.

2) При компьютеризации общества основное внимание уделяется:

a) обеспечению полного использования достоверного, исчерпывающего и своевременного знания во всех видах человеческой деятельности;

b) развитию и внедрению технической базы компьютеров, обеспечивающих оперативное получение результатов переработки информации и ее накопление.

3) Результатом процесса информатизации является создание:

a) информационного общества;

b) индустриального общества.

4) Информационная услуга – это:

a) совокупность данных, сформированная производителем для распространения в вещественной или невещественной форме;

b) результат непроизводственной деятельности предприятия или лица, направленный на удовлетворение потребности человека или организации в использовании различных продуктов;

c) получение и предоставление в распоряжение пользователя информационных продуктов;

d) совокупность связанных данных, правила организации которых основаны на общих принципах описания, хранения и манипулирования данными.

5) Информационно-поисковые системы позволяют:

a) осуществлять поиск, вывод и сортировку данных;

b) осуществлять поиск и сортировку данных;

c) редактировать данные и осуществлять их поиск;

d) редактировать и сортировать данные.

6) Информационная культура человека на современном этапе в основном определяется:

a) совокупностью его умений программировать на языках высокого уровня;

b) его знаниями основных понятий информатики;

c) совокупностью его навыков использования прикладного программного обеспечения для создания необходимых документов;

d) уровнем понимания закономерностей информационных процессов в природе и обществе, качеством знаний основ компьютерной грамотности, совокупностью технических навыков взаимодействия с компьютером, способностью эффективно и своевременно использовать средства информационных и коммуникационных технологий при решении задач практической деятельности;

e) его знаниями основных видов программного обеспечения и пользовательских характеристик компьютера.

7) Деловая графика представляет собой:

a) график совещания;

b) графические иллюстрации;

c) совокупность графиков функций;

d) совокупность программных средств, позволяющих представить в графическом виде закономерности изменения числовых данных.

8) В чем отличие информационно-поисковой системы (ИПС) от системы управления базами данных (СУБД)?

a) в запрете на редактирование данных;

b) в отсутствии инструментов сортировки и поиска;

c) в количестве доступной информации.

9) WORD – это…

a) графический процессор;

b) текстовый процессор;

c) средство подготовки презентаций;

d) табличный процессор;

e) редактор текста.

10) ACCESS реализует … структуру данных.

a) реляционную;

b) иерархическую;

c) многослойную;

d) линейную;

e) гипертекстовую.

11) Front Page – это средство ...

a) системного управления базой данных;

b) создания WEB-страниц;

c) подготовки презентаций;

d) сетевой передачи данных;

e) передачи данных.

12) Электронные таблицы позволяют обрабатывать …

a) цифровую информацию;

b) текстовую информацию;

c) аудио информацию;

d) схемы данных;

e) видео информацию.

13) Технология OLE обеспечивает объединение документов, созданных …

a) любым приложением, удовлетворяющим стандарту CUA;

b) при помощи информационных технологий, входящих в интегрированный пакет;

c) электронным офисом;

d) любыми информационными технологиями;

e) PHOTO и Word.

14) Схему обработки данных можно изобразить посредством…

a) коммерческой графики;

b) иллюстративной графики;

c) научной графики;

d) когнитивной графики;

e) Front Page.

15) Векторная графика обеспечивает построение…

a) геометрических фигур;

b) рисунков;

c) карт;

d) различных формул;

e) схем.

16) Деловая графика включена в состав…

a) Word;
b) Excel;
c) Access;
d) Outlook;
e) Publisher.

17) Структура гипертекста …

a) задается заранее;
b) задается заранее и является иерархической;
c) задается заранее и является сетевой;
d) задается заранее и является реляционной;
e) заранее не задается.

18) Гипертекст – это…

a) технология представления текста;
b) структурированный текст;
c) технология поиска данных;
d) технология обработки данных;
e) технология поиска по смысловым связям.

19) Сетевая операционная система реализует …

a) управление ресурсами сети;
b) протоколы и интерфейсы;
c) управление серверами;
d) управление приложениями;
e) управление базами данных.

20) Клиент – это …

a) абонентская ЭВМ, выполняющая запрос к серверу;
b) приложение, выдающее запрос к базе данных;
c) запрос пользователя к удаленной базе данных;
d) запрос приложения;
e) локальная система управления базой данных.

21) Единицей обмена физического уровня сети является …

a) байт;
b) бит;
c) сообщение;
d) пакет;
e) задание.

22) Протокол IP сети используется на …

a) физическом уровне;
b) канальном уровне;
c) сетевом уровне;
d) транспортном уровне;
e) сеансовом уровне;
f) уровне представления данных;
g) прикладном уровне.

23) ***(выбрать несколько вариантов ответа)*** **Интернет возник благодаря соединению таких технологий, как …**

a) мультимедиа;
b) гипертекста;
c) информационные хранилища;
d) сетевые технологии;
e) телеконференции;

f) геоинформационные технологии.

24) *(выбрать несколько вариантов ответа)* Ресурсы интернета – это …

a) электронная почта;

b) телеконференции;

c) компьютеры, еще не подключенные к глобальной сети;

d) каталоги рассылки в среде;

e) FTP-системы.

25) *(выбрать несколько вариантов ответа)* URL-адрес содержит информацию о…

a) типе приложения;

b) местонахождении файла;

c) типе файла;

d) языке программирования;

e) параметрах программ.

26) Результатом поиска в интернет является …

a) искомая информация;

b) список тем;

c) текст;

d) сайт с текстом;

e) список сайтов.

27) Почтовый сервер обеспечивает … сообщений.

a) хранение почтовых;

b) передачу;

c) фильтрацию;

d) обработку;

e) редактирование.

28) В режиме off-line пользователь …

a) общается непосредственно с адресатом;

b) передает сообщение одному адресату;

c) посылает сообщение в почтовый сервер;

d) передает сообщение нескольким адресатом;

e) передает сообщение в диалоговом режиме.

29) *(выбрать несколько вариантов ответа)* К мультимедийным функциям относятся …

a) цифровая фильтрация;

b) методы защиты информации;

c) сжатие-развертка изображения;

d) поддержка «живого» видео;

e) поддержка 3D графики.

30) *(выбрать несколько вариантов ответа)* Видеоконференция предназначена для…

a) обмена мультимедийными данными;

b) общения и совместной обработки данных;

c) проведения телеконференций;

d) организации групповой работы;

e) автоматизации деловых процессов.

31) Искусственный интеллект служит для …

a) накопления знаний;

b) воспроизведения некоторых функций мозга;

c) моделирования сложных проблем;

d) копирования деятельности человека;

e) создания роботов.

32) Достоверность данных – это …

a) отсутствие в данных ошибок;

b) надежность их сохранения;

c) их полнота;

d) их целостность;

e) их истинность.

33) Безопасность компьютерных систем – это …

a) защита от кражи, вирусов, неправильной работы пользователей, несанкционированного доступа;

b) правильная работа компьютерных систем;

c) обеспечение бессбойной работы компьютера;

d) технология обработки данных;

e) правильная организация работы пользователя.

34) Безопасность данных обеспечивается в результате …

a) контроля достоверности данных;

b) контроля искажения программ и данных;

c) контроля от несанкционированного доступа к программам и данным;

d) технологических средств обеспечения безопасности и организационных средств обеспечения безопасности.

35) Система электронного документооборота обеспечивает …

a) массовый ввод бумажных документов;

b) управление электронными документами;

c) управление знаниями;

d) управление новациями;

e) автоматизацию деловых процессов.

36) Моделирование деятельности сотрудника в электронном документообороте – это …

a) имитация деятельности;

b) формализованное описание его деятельности;

c) реализация бизнес-процессов;

d) реализация деятельности сотрудника;

e) организация групповой работы.

37) Для изменения электронного документа в системе управления документами задается …

a) пароль и право доступа;

b) имя базы данных;

c) имя информационного хранилища;

d) идентификатор электронного документа.

8) Операция «чистка изображения» в системе массового ввода документов – это удаление …

a) пятен и шероховатостей, линий сгиба, других дефектов;

b) элементов форм;

c) пересечения букв с элементами форм;

d) фона.

39) Системы оптического распознавания работают с…

a) рукописным текстом;

b) полиграфическим текстом;

c) штрих-кодами;

d) специальными метками;

e) гипертекстом.

40) Управление знаниями необходимо для…

a) создания интеллектуального капитала предприятия;
b) поддержки принятия решений;
c) преобразования скрытых знаний в явные;
d) создания иерархических хранилищ;
e) создания электронного документооборота.

ПРИЛОЖЕНИЕ 4

ДЕМОНСТРАЦИОННЫЕ ВАРИАНТЫ ВОПРОСОВ
(фронтальный опрос на семинарских занятиях)

ТЕСТ № 3. ДЛЯ ТЕКУЩЕГО КОНТРОЛЯ

1. Под информационной безопасностью понимается…

а) защищенность информации и поддерживающей инфраструктуры от случайных или преднамеренных воздействий естественного или случайного характера, которые могут нанести неприемлемый ущерб субъектам информационных отношений в том числе владельцам и пользователям информации, и поддерживающей инфраструктуре;

б) программный продукт и базы данных должны быть защищены по нескольким направлениям от воздействия;

в) нет правильного ответа.

2. Защита информации – это…

а) комплекс мероприятий, направленных на обеспечение информационной безопасности;

б) процесс разработки структуры базы данных в соответствии с требованиями пользователей;

в) небольшая программа для выполнения определенной задачи.

3. От чего зависит информационная безопасность?

а) от компьютеров;

б) от поддерживающей инфраструктуры;

в) от информации.

4. Основные составляющие информационной безопасности:

а) целостность;

б) достоверность;

в) конфиденциальность.

5. Доступность – это…

а) возможность за приемлемое время получить требуемую информационную услугу;

б) логическая независимость;

в) нет правильного ответа.

6. Целостность – это...

а) целостность информации;

б) непротиворечивость информации;

в) защищенность от разрушения.

7. Конфиденциальность – это...

а) защита от несанкционированного доступа к информации;

б) программ и программных комплексов, обеспечивающих технологию разработки, отладки и внедрения создаваемых программных продуктов;

в) описание процедур.

8. Для чего создаются информационные системы?

а) получения определенных информационных услуг;

б) обработки информации;

в) все ответы правильные.

9. Целостность можно подразделить:

а) статическую;

б) динамичную;

в) структурную.

10. Где применяются средства контроля динамической целостности?

а) анализе потока финансовых сообщений;

б) обработке данных;

в) при выявлении кражи, дублирования отдельных сообщений.

11. Какие трудности возникают в информационных системах при конфиденциальности?

а) сведения о технических каналах утечки информации являются закрытыми;

б) на пути пользовательской криптографии стоят многочисленные технические проблемы;

в) все ответы правильные.

12. Угроза – это…

а) потенциальная возможность определенным образом нарушить информационную безопасность;

б) система программных языковых организационных и технических средств, предназначенных для накопления и коллективного использования данных;

в) процесс определения отвечает на текущее состояние разработки требованиям данного этапа.

13. Атака – это…

а) попытка реализации угрозы;

б) потенциальная возможность определенным образом нарушить информационную безопасность;

в) программы, предназначенные для поиска необходимых программ.

14. Источник угрозы – это...

а) потенциальный злоумышленник;

б) злоумышленник;

в) нет правильного ответа.

15. Окно опасности – это…

а) промежуток времени от момента, когда появится возможность слабого места и до момента, когда пробел ликвидируется;

б) комплекс взаимосвязанных программ для решения задач определенного класса конкретной предметной области;

в) формализованный язык для описания задач алгоритма решения задачи пользователя на компьютере.

16. Кто является основным ответственным за определение уровня классификации информации?

а) руководитель среднего звена;

б) высшее руководство;

в) владелец;

г) пользователь.

17. Какая категория является наиболее рискованной для компании с точки зрения вероятного мошенничества и нарушения безопасности?

а) сотрудники;

б) хакеры;

в) атакующие;

г) контрагенты (лица, работающие по договору).

18. **Если различным группам пользователей с различным уровнем доступа требуется доступ к одной и той же информации, какое из указанных ниже действий следует предпринять руководству?**

а) снизить уровень безопасности этой информации для обеспечения ее доступности и удобства использования;

б) требовать подписания специального разрешения каждый раз, когда человеку требуется доступ к этой информации;

в) улучшить контроль за безопасностью этой информации;

г) снизить уровень классификации этой информации.

19. Что самое главное должно продумать руководство при классификации данных?

а) типы сотрудников, контрагентов и клиентов, которые будут иметь доступ к данным;

б) необходимый уровень доступности, целостности и конфиденциальности;

в) оценить уровень риска и отменить контрмеры;

г) управление доступом, которое должно защищать данные.

20. Кто в конечном счете несет ответственность за гарантии того, что данные классифицированы и защищены?

а) владельцы данных;

б) пользователи;

в) администраторы;

г) руководство.

21. Что такое процедура?

а) правила использования программного и аппаратного обеспечения в компании;

б) пошаговая инструкция по выполнению задачи;

в) руководство по действиям в ситуациях, связанных с безопасностью, но не описанных в стандартах;

г) обязательные действия.

22. Какой фактор наиболее важен для того, чтобы быть уверенным в успешном обеспечении безопасности в компании?

а) поддержка высшего руководства;

б) эффективные защитные меры и методы их внедрения;

в) актуальные и адекватные политики и процедуры безопасности;

г) проведение тренингов по безопасности для всех сотрудников.

23. Когда целесообразно не предпринимать никаких действий в отношении выявленных рисков?

а) никогда. Для обеспечения хорошей безопасности нужно учитывать и снижать все риски;

б) когда риски не могут быть приняты во внимание по политическим соображениям;

в) когда необходимые защитные меры слишком сложны;

г) когда стоимость контрмер превышает ценность актива и потенциальные потери.

24. Что такое политики безопасности?

а) пошаговые инструкции по выполнению задач безопасности;

б) общие руководящие требования по достижению определенного уровня безопасности;

в) широкие, высокоуровневые заявления руководства;

г) детализированные документы по обработке инцидентов безопасности.

25. Какая из приведенных техник является самой важной при выборе конкретных защитных мер?

а) анализ рисков;

б) анализ затрат / выгоды;

в) результаты ALE;

г) выявление уязвимостей и угроз, являющихся причиной риска.

26. База данных – это…

а) специальным образом организованная и хранящаяся на внешнем носителе совокупность взаимосвязанных данных о некотором объекте;

б) произвольный набор информации;

в) совокупность программ для хранения и обработки больших массивов информации;

г) интерфейс, поддерживающий наполнение и манипулирование данными;

д) компьютерная программа, позволяющая в некоторой предметной области делать выводы, сопоставимые с выводами человека-эксперта.

27. В записи файла реляционной базы данных (БД) может

содержаться: а) исключительно однородная информация (данные только одного типа); б) только текстовая информация;

в) неоднородная информация (данные разных типов);

г) только логические величин;

д) исключительно числовая информация.

28. Предположим, что некоторая база данных содержит поля *ФАМИЛИЯ, ГОД РОЖДЕНИЯ, ДОХОД*. **При поиске по условию** *ГОД РОЖДЕНИЯ > 1958 AND ДОХОД < 3500* **будут найдены фамилии лиц:**

а) имеющих доход не менее 3500, и старше тех, кто родился в 1958 году;

б) имеющих доход менее 3500, или тех, кто родился е 1958 году и позже;

в) имеющих доход менее 3500, и родившихся в 1958 году и позже;

г) имеющих доход менее 3500, и родившихся в 1959 году и позже;

д) имеющих доход менее 3500, и тех, кто родился в 1958 году.

29. Какой из вариантов не является функцией СУБД?

а) реализация языков определения и манипулирования данными;

б) обеспечение пользователя языковыми средствами манипулирования данными;

в) поддержка моделей пользователя;

г) защита и целостность данных;

д) координация проектирования, реализации и ведения БД.

30. Система управления базами данных представляет собой программный продукт, входящий в состав:

а) прикладного программного обеспечения;

б) операционной системы;

в) уникального программного обеспечения;

г) системного программного обеспечения;

д) систем программирования.

31. Какая наименьшая единица хранения данных в БД?

а) хранимое поле;

б) хранимый файл;

в) ничего из вышеперечисленного;

г) хранимая запись;

д) хранимый байт.

32. Что обязательно должно входить в СУБД?

а) процессор языка запросов;

б) командный интерфейс;

в) визуальная оболочка;

г) система помощи.

33. Перечислите преимущества централизованного подхода к хранению и управлению данными:

а) возможность общего доступа к данным;

б) поддержка целостности данных;

в) соглашение избыточности;

г) сокращение противоречивости.

34. Предположим, что некоторая база данных описывается следующим перечнем записей:

а) Иванов, 1956, 2400;

б) Сидоров, 1957, 5300;

в) Петров, 1956, 3600;

г) Козлов, 1952, 1200.

35. Какие из записей этой БД поменяются местами при сортировке по возрастанию, произведенной по первому полю:

а) 3 и 4;

б) 2 и 3;

в) 2 и 4;
г) 1 и 4;
д) 1 и 3.

36. Структура файла реляционной базы данных (БД) меняется:

а) при изменении любой записи;
б) при уничтожении всех записей;
в) при удалении любого поля;
г) при добавлении одной или нескольких записей;
д) при удалении диапазона записей.

37. Как называется набор хранимых записей одного типа?

а) хранимый файл;
б) представление базы данных;
в) ничего из вышеперечисленного;
г) логическая таблица базы данных;
д) физическая таблица базы данных.

38. Таблица СУБД содержит:

а) информацию о совокупности однотипных объектов;
б) информацию о совокупности всех объектов, относящихся к некоторой предметной области;
в) информацию о конкретном объекте.

39. Строки таблицы СУБД содержат:

а) информацию о совокупности однотипных объектов;
б) информацию о совокупности всех объектов, относящихся к некоторой предметной области;
в) информацию о конкретном объекте.

40. Столбцы таблицы СУБД содержат:

а) информацию о совокупности однотипных объектов;
б) информацию о совокупности всех объектов, относящихся к некоторой предметной области;
в) совокупность значений одного из атрибутов для всех однотипных объектов.

41. Структура таблицы СУБД определяется:

а) размерностью таблицы;
б) списком наименований столбцов таблицы;
в) списком наименований столбцов и номеров строк таблицы.

42. Поле данных в СУБД – это…

а) значение атрибута для конкретного объекта;
б) элемент структуры таблицы;
в) список значений атрибута для всех однотипных объектов.

43. Ключевое поле таблицы в СУБД – это…

а) строку таблицы, содержащей уникальную информацию;
б) совокупность полей таблицы, которые однозначно определяют каждую строку;
в) столбец таблицы, содержащей уникальную информацию.

44. Таблица в СУБД может иметь:

а) только одно ключевое поле;
б) только два ключевых поля;
в) любое количество ключевых полей.

45. В текстовом поле СУБД MS Access можно хранить:

а) только буквенную (символьную) информацию;
б) маску ввода;
в) картинки.

46. Мастер подстановок в СУБД MS Access используется:

а) для создания новых полей;

б) для придания значений полей из других таблиц, или введение фиксированного списка данных;

в) для расчета функций.

47. В режиме конструктора таблицы СУБД Access можно:

а) добавить новое поле;

б) набрать текстовый документ;

в) выполнить вычисления.

48. Изменить формат числового поля в СУБД Access можно:

а) набрав соответствующую комбинацию клавиш;

б) в конструкторе таблицы;

в) изменив название поля в самой таблице.

49. Имя поля таблицы в СУБД Access может хранить:

а) до 64-х символов;

б) только знаки 0 и 1;

в) нет ограничений на количество символов.

50. Для каких целей удобно использовать запросы в MS Access? Выберите наиболее правильное и полное толкование:

а) с их помощью можно просматривать, анализировать и изменять данные из нескольких таблиц и других запросов. Они также используются как источник для форм и отчетов;

б) с их помощью можно просматривать, анализировать и изменять данные из нескольких таблиц, запросов, отчетов, форм. Они используются в качестве источника данных для таблиц и отчетов;

в) с их помощью можно просматривать, анализировать и изменять данные из нескольких таблиц, отчетов, форм.

ПРИЛОЖЕНИЕ 5

ВОПРОСЫ К КОЛЛОКВИУМУ ДЛЯ САМОСТОЯТЕЛЬНОЙ ПРОРАБОТКИ К СЕМИНАРУ ИНТЕРАКТИВНОГО ТИПА

1. Что такое информация?
2. По каким классификациям можем рассмотреть информацию?
3. В каких еще сферах используется понятие информация?
4. Чем отличается информация от данных?
5. Объясните информатику и теорию информации?
6. Какими государственными информациями своей страны может владеть гражданин?
7. Можно ли рассматривать информацию как товар? В каких случаях?
8. Какое положение не позволяет в полной мере обеспечить права граждан на доступ к информации о деятельности о деятельности органов власти? И значит ли это не позволять достигнуть главной цели закона об обеспечении подотчетности органов власти обществу?
9. К какому свойству информации относиться способность информации соответствовать нуждам или запросам потребителя?
10. Как можно объяснить защищенность информации?
11. Какое свойство достоверности информации имеет свое имя?
12. Какие виды информации можете перечислить?
13. Что значит информационная открытость?
14. Чем отличается понятие государственной информации в России и Кыргызстане?
15. Что такое дезинформация?
16. Что такое информационный процесс?
17. Актуальность представления информации?
18. Как правильно хранить информацию?
19. Кого или что можно назвать носителями информации?
20. Что дает понятие информационный взрыв?
21. Какие информационные электронные носители вам знакомы?
22. Как можно объяснить информационный барьер? Какие виды барьера существуют?
23. В каких значениях можно рассмотреть информационную безопасность?
24. Что значит информационная безопасность государства?
25. Как можно объяснить ценность информации?
26. Объем информации и ее ценность, как это объяснить?
27. Что значит «Политика информационной безопасности»?
28. Какую классификацию средств защиты информации можно увидеть в литературе?
29. Как вы можете описать аспекты возникновения и развития информационной безопасности?
30. Дайте определение понятиям: «Информация», «Информационная безопасность», «Защита информации», «Информационная угроза».
31. Дайте характеристику основным составляющим информационной безопасности.
32. Перечислите основные объекты защиты.
33. Дайте характеристику понятиям «Государственная тайна», «Конфиденциальная информация» и «Персональные данные».

34. Дайте характеристику средствам защиты информации.
35. В чем заключается проблема информационной безопасности?
36. Дайте определение понятию «Информационная безопасность».
37. Что понимается под «Компьютерной безопасностью»?
38. Перечислите составляющие информационной безопасности.
39. Приведите определение доступности информации.
40. Приведите определение целостности информации.
41. Приведите определение конфиденциальности информации.
42. Каким образом взаимосвязаны между собой составляющие информационной безопасности? Приведите собственные примеры.
43. Перечислите задачи информационной безопасности общества.
44. Перечислите уровни формирования режима информационной безопасности.
45. Дайте краткую характеристику законодательно-правового уровня.
46. Какие подуровни включает программно-технический уровень?
47. Что включает административный уровень?
48. В чем особенность морально-этического подуровня?
49. Какие виды требований включает стандарт ISO/IEC 15408?
50. Чем отличаются функциональные требования от требований доверия?
51. В чем заключается иерархический принцип «класс – семейство – компонент – элемент»?
52. Какова цель требований по отказоустойчивости информационных систем?
53. Сколько классов функциональных требований?
54. Дайте характеристику составляющих «Информационной безопасности» применительно к вычислительным сетям.
55. Перечислите основные механизмы безопасности.
56. Какие механизмы безопасности используются для обес-печения конфиденциальности трафика?
57. Какие механизмы безопасности используются для обес-печения «Неотказуемости» системы?
58. Что понимается под администрированием средств безопасности?
59. Какие виды избыточности могут использоваться в вычислительных сетях?
60. Цели и задачи административного уровня обеспечения информационной безопасности?
61. Содержание административного уровня?
62. Дайте определение политики безопасности.
63. Направления разработки политики безопасности?
64. Перечислите составные элементы автоматизированных систем.
65. Субъекты информационных отношений и их роли при обеспечении информационной безопасности.
66. Перечислите классы угроз информационной безопасности.
67. Назовите причины и источники случайных воздействий на информационные системы.
68. Дайте характеристику преднамеренным угрозам.
69. Перечислите каналы несанкционированного доступа.
70. В чем особенность «Утверждающей» защиты в информационных системах?

ПРИЛОЖЕНИЕ 6

ШКАЛА ОЦЕНИВАНИЯ САМОСТОЯТЕЛЬНЫХ ЗАДАНИЙ (текущий контроль)

1. СРАВНИТЕЛЬНАЯ ТАБЛИЦА

№	Наименование показателя	Отметка (в %)
ФОРМА		**0-60**
1	Количество сравнительных показателей	0-35
2	Актуальность выбранной темы	0-5
3	Сформированность идей и их ясное изложение и структурирование	0-10
4	Наличие выводов и замечаний по соответствующему показателю	0-10
ОТВЕТЫ НА ВОПРОСЫ		**0- 40**
Всего баллов		**Сумма баллов**

2. УСТНЫЙ ОПРОС по самостоятельным заданиям, тестам, вопросам. (текущий контроль)

№	Наименование показателя	Отметка (в %)
1	Оригинальность и убедительность	0-15
2	Понимание проблематики и адекватность трактовки	0-25
3	Обоснованное привлечение количественных показателей и нормативно-правовых актов (уместность и достоверность сведений)	0-40
4	Ключевые слова (их важность для заявленной темы, грамотное употребление, количество)	0-10
5	Логичность и последовательность устного высказывания	0-10
Всего баллов		**Сумма баллов**

ШКАЛА ОЦЕНИВАНИЯ ТЕСТА (текущий контроль)

1. В одном тестовом задании 20 закрытых вопросов.
2. К заданиям даются готовые ответы на выбор, один правильный и остальные неправильные.
3. Обучающемуся необходимо помнить: в каждом задании с выбором одного правильного ответа правильный ответ должен быть.
4. За каждый правильный ответ – 1 балл.
5. Общая оценка определяется как сумма набранных баллов.
6. Отметка (в %).

ШКАЛА ОЦЕНИВАНИЯ КОЛЛОКВИУМА (рубежный контроль)

«85-100%»

- глубокое и прочное усвоение материала темы или раздела;
- полные, последовательные, грамотные и логически излагаемые ответы;
- демонстрация обучающимся знаний в объеме пройденной программы и дополнительно рекомендованной литературы;
- воспроизведение учебного материала с требуемой степенью точности.

«75-84%»

- наличие несущественных ошибок, уверенно исправляемых обучающимся после дополнительных и наводящих вопросов;
- демонстрация обучающимся знаний в объеме пройденной программы;
- четкое изложение учебного материала.

«60-74%»

- наличие несущественных ошибок в ответе, не исправляемых обучающимся;
- демонстрация обучающимся не достаточно полных знаний по пройденной программе;
- не структурированное, не стройное изложение учебного материала при ответе.

« менее 60%»

- не знание материала темы или раздела;
- при ответе возникают серьезные ошибки.

ШКАЛА ОЦЕНИВАНИЯ ПРЕЗЕНТАЦИИ (рубежный контроль)

№	Наименование показателя	Отметка (в %)
ПРЕЗЕНТАЦИЯ		70
1	Титульный лист с заголовком	0-10
2	Дизайн слайдов и использование дополнительных эффектов (смена слайдов, звук, графики)	0-10
3	Текст презентации написан коротко, хорошо и сформированные идеи ясно изложены и структурированы	0-30
4	Слайды представлены в логической последовательности	0-10
5	Слайды распечатаны в формате заметок	0-10
ДОКЛАД		30
1	Правильность и точность речи во время защиты	0-10
2	Широта кругозора (ответы на вопросы)	0-10
3	Выполнение регламента	0-10
Всего баллов		**Сумма баллов**

ШКАЛА ОЦЕНИВАНИЯ ДОКЛАДА (рубежный контроль)

№	Наименование показателя	Отметка (в %)
ФОРМА		20
1	Деление текста на введение, основную часть и заключение	0-10
2	Логичный и понятный переход от одной части к другой, а также внутри частей	0-10
СОДЕРЖАНИЕ		60
1	Соответствие теме	0-10
2	Наличие основной темы (тезиса) в вводной части и обращенность вводной части к читателю	0-10
3	Развитие темы (тезиса) в основной части (раскрытие основных положений через систему аргументов, подкрепленных фактами, примерами и т.д.)	0-20
4	Наличие выводов, соответствующих теме и содержанию основной части	0-20
ДОКЛАД		20
1	Правильность и точность речи во время защиты	0-5
2	Широта кругозора (ответы на вопросы)	0-5
3	Выполнение регламента	0-5
Всего баллов		**Сумма баллов**

ШКАЛА ОЦЕНИВАНИЯ УСТНОГО ОПРОСА (промежуточный контроль – «ЗНАТЬ»)

При оценке устных ответов на проверку уровня обученности ЗНАТЬ учитываются следующие критерии:

1. Знание основных процессов изучаемой предметной области, глубина и полнота раскрытия вопроса.
2. Владение терминологическим аппаратом и использование его при ответе.
3. Умение объяснить сущность явлений, событий, процессов, делать выводы и обобщения, давать аргументированные ответы.
4. Владение монологической речью, логичность и последовательность ответа, умение отвечать на поставленные вопросы, выражать свое мнение по обсуждаемой проблеме.

Отметкой **(16-20 баллов)** оценивается ответ, который показывает прочные знания основ современных компьютерных и информационных технологий, применяемые в области обеспечения безопасности; потенциальные возможности и направления развития информационных систем и сетей; принципы организации, основные технические средства компьютерных систем и функциональные возможности информационных сетей; логичность и последовательность ответа.

Отметкой **(10-15 баллов)** оценивается ответ, обнаруживающий прочные знания основ современных компьютерных и информационных технологий, применяемые в области обеспечения безопасности; потенциальные возможности и направления развития информационных систем и сетей; принципы организации, основные технические средства компьютерных систем и функциональные возможности информационных сетей; логичность и последовательность ответа. Однако допускается одна - две неточности в ответе.

Отметкой **(5-10 баллов)** оценивается ответ, свидетельствующий в основном о знании основ современных компьютерных и информационных технологий, применяемые в области обеспечения безопасности; потенциальные возможности и направления развития информационных систем и сетей; принципы организации, основные технические средства компьютерных систем и функциональные возможности информационных сетей. Допускается несколько ошибок в содержании ответа.

Отметкой **(1-4 баллов)** оценивается ответ, обнаруживающий незнание современных компьютерных и информационных технологий, отличающийся неглубоким раскрытием темы; незнанием основных вопросов теории, несформированными навыками анализа явлений, процессов; неумением давать аргументированные ответы, слабым владением монологической речью, отсутствием логичности и последовательности. Допускаются серьезные ошибки в содержании ответа.

ШКАЛА ОЦЕНИВАНИЯ ПРАКТИЧЕСКИХ ЗАДАНИЙ
(промежуточный контроль – «УМЕТЬ и ВЛАДЕТЬ»)

При оценке ответов на проверку уровня обученности УМЕТЬ и ВЛАДЕТЬ учитываются следующие критерии:

Отметкой **(8-10 баллов)** оценивается ответ, при котором магистрант эффективно выбирает оптимальные компьютерные и информационные технологии; анализирует, оптимизирует и применяет современные информационные технологии при решении научных задач; прогнозирует воздействие новой техники и технологий; навыками реализации компьютерных и информационных технологий при решении практических задач в области безопасности, моделирования, упрощения, сравнения, использования известных решений в новом приложении при внедрении новой техники и технологий, включая наилучшие доступные технологии, навыками применения современных программ. Демонстрирует полное понимание проблемы. Все требования, предъявляемые к заданию выполнены.

Отметкой **(4-7 баллов)** оценивается ответ, при котором магистрант не достаточно эффективно выбирает оптимальные компьютерные и информационные технологии. Хорошо анализирует, оптимизирует и применяет современные информационные технологии при решении научных задач; прогнозирует воздействие новой техники и технологий; навыками реализации компьютерных и информационных технологий при решении практических задач в области безопасности, моделирования, упрощения, сравнения, использования известных решений в новом приложении при внедрении новой техники и технологий, включая наилучшие доступные технологии, навыками применения современных программ. Демонстрирует значительное понимание проблемы. Большинство требований, предъявляемых к заданию выполнены.

Отметкой **(1-3 балла)** оценивается ответ, при котором магистрант не эффективно выбирает оптимальные компьютерные и информационные технологии; слабо анализирует и не применяет современные информационные технологии при решении научных задач. Не достаточно хорошо владеет навыками реализации компьютерных и информационных технологий при решении практических задач в области безопасности, моделирования, упрощения, сравнения, использования известных решений в новом приложении при внедрении новой техники и технологий, слабо выражает навыки применения современных программ. Демонстрирует частичное или небольшое понимание проблемы. Многие требования, предъявляемые к заданию, не выполнены.

Отметкой **(0 баллов)** оценивается ответ, при котором магистрант демонстрирует непонимание проблемы или нет ответа и даже не было попытки решить задачу.

ПРИЛОЖЕНИЕ 7

ГЛОССАРИЙ

Application Service Provision (Аренда приложений) – аренда программных продуктов и инфраструктуры на базе периодических платежей с доступом к приложениям через Интернет или виртуальную частную сеть.

ASP – Application Service Provider (Провайдер услуг по аренде приложений) – организация, предоставляющая услуги аренды приложений.

IDS – Intrusion Detection System (Система обнаружения вторжения) – система, предназначенная для определения враждебной активности в сети.

IT – Information Technologies (ИТ, информационные технологии).

IT-инфраструктура – информационно-технологическая инфраструктура. Все информационные технологии, используемые в рамках одной организации: компьютеры, сети, программное обеспечение и т.п.

Web-интеграция – построение корпоративных информационных систем на базе web-технологий.

Web-клиент – как программа – браузер. Web-клиент как устройство – устройство, основным приложением которого (с точки зрения разработчика устройства или маркетолога) является браузер.

Web-клиент – как программа – браузер. Web-клиент как устройство – устройство, основным приложением которого (с точки зрения разработчика устройства или маркетолога) является браузер.

Web-сервер – сервер, хранящий и предоставляющий во внешнюю сеть данные, организованные в виде HTML-страниц.

Workflow – это автоматизация (полностью или частично) бизнес-процесса, при которой документы, информация или задания передаются для выполнения необходимых действий от одного участника к другому в соответствии с набором процедурных правил. Система workflow обязана поддерживать все компоненты процесса и их различные взаимосвязи (ролевые, информационные, временные, маршрутные и т.д.).

Workflow, Технология автоматизации деловых процессов – это современная технология компьютеризированной поддержки процессов управления предприятием (деловых процессов) в целом или какой-то их части. Она объединяет несколько сформировавшихся информационных технологий, таких как электронная почта, управление проектами, работа с базами данных и т.д.

Айпи (от англ. «**I**nternet **P**rotocol») – уникальный адрес. Каждый компьютер имеет свой IP, который предоставляет ему провайдер.

Айтишник – программист, специалист в информационных технологиях (ИТ). С английского аббревиатура IT (Information Technology) читается как «Ай Ти».

Актуальность информации – важность для настоящего времени, злободневность, насущность. Только вовремя полученная информация может быть полезна.

Аналитическая работа – комплексное исследование различной целевой направленности, предназначенное для выявления, структуризации и изучения опасных объективных и субъективных, потенциальных и реальных ситуаций, которые могут создать риск для экономической безопасности фирмы, ее деятельности или персонала, привести к материальным, финансовым или иным убыткам, падению престижа фирмы или ее продукции.

Аналитическая работа по выявлению каналов несанкционированного доступа к конфиденциальной информации – прогнозирование и выявление на основе комплексного исследования сложившихся или предполагаемых ситуаций состава и особенностей образования каналов несанкционированного доступа к конфиденциальной информации конкретной фирмы в единстве с изучением характера возможных угроз ее информационной безопасности.

Аналитическая работа с источником конфиденциальной информации – комплексное исследование максимального числа источников, владеющих или содержащих конфиденциальные сведения.

Аналитическая работа с каналом объективного распространения конфиденциальной информации – комплексное исследование максимального числа коммуникативных каналов, по которым перемещаются конфиденциальные сведения в санкционированном режиме.

Аппаратный сервер – узкоспециализированное решение со встроенным программным обеспечением в ПЗУ (англ. firmware; в отличие от компьютеров, где программное обеспечение необходимо устанавливать), определяющим специализацию и возможные предоставляемые услуги.

Аутентичность информации – избежание недостатка полноты или точности информации при ее санкционированных изменениях.

База данных (БД) (Database; Data base (DB) (фр. Base de donnees)) – совокупность связанных данных, организованных по определенным правилам, предусматривающим общие принципы описания, хранения и манипулирования, независимая от прикладных программ.

Байт (англ. byte) (русское обозначение: байт и «Б»; международное: B, byte) – единица хранения и обработки цифровой информации; совокупность битов, обрабатываемая компьютером одномоментно.

Безопасность (Safety; Security) – состояние защищенности жизненно важных интересов личности, общества и государства от внутренних и внешних угроз, точнее, безопасность – это защищенность жизненно важных интересов личности, общества и государства от внутренних и внешних угроз, состояние, при котором чему-либо или кому-либо не угрожает опасность.

Безопасность информационная – составная часть экономической безопасности предпринимательской деятельности.

Безопасность информационных ресурсов (информации) – защищенность информации во времени и пространстве от любых объективных и субъективных угроз (опасностей), возникающих в обычных условиях функционирования фирмы и условиях экстремальных ситуаций. Безопасность ценной документированной информации (документов) определяется уровнем ее защищенности от стихийных бедствий, других неуправляемых событий, пассивных и активных попыток злоумышленника создать потенциальную или реальную угрозу несанкционированного доступа к документам, делам, базам данных, а также опасностей неправомерного использования кем-либо ценных сведений, нарушения их сохранности, целостности конфиденциальности.

Безопасность маркетинговая – составная часть экономической безопасности предпринимательской деятельности.

Безопасность правовая – составная часть экономической безопасности предпринимательской деятельности.

Безопасность предполагает также защищенность конфиденциальной информации в информационных системах от случайных и преднамеренных воздействий естественного и искусственного свойства, направленных на изменение степени доступности ценных сведений в машинной и вне машинных сфер.

Безопасность сети (Network security) – меры, предохраняющие информационную сеть:

Безопасность физическая – составная часть экономической безопасности предпринимательской деятельности.

Безопасность экономическая – всесторонняя защищенность предпринимательской деятельности, деловых интересов каждого творческого коллектива, предприятия, фирмы и предпринимателя в большом и малом бизнесе во времени и пространстве.

Бит (англ. binary digit; также игра слов: англ. bit – немного) – одна из самых известных единиц количества информации, по Шеннону бит – это двоичный логарифм вероятности равновероятных событий или сумма произведений вероятности на двоичный логарифм.

Броузер (браузер) – browser – программа навигации и просмотра веб-ресурсов, позволяет запрашивать и просматривать файлы в Интернет. Обычно в комплекте с браузерами поставляются почтовые программы, средства работы с серверами новостей и средства общения в реальном времени.

Вебинар (от англ. «**web** based sem**inar**») – это семинар, презентация или лекция, которая проходит онлайн, в прямой трансляции в Интернете. Ну или запись этой трансляции.

Видеограмма – изображение электронного документа на экране дисплея. В полном смысле слова документом не является, представляет собой заверенную или незаверенную копию документа (как и факсограмма).

Виды информации – графическая или изобразительная, звуковая (акустическая), текстовая, числовая и видео информация.

Виндоус – операционная система Windows.

Виртуальный сервер, локальный сервер – комплект прогаммного обеспечения, обеспечивающий разработку сетевых программ в режиме клиент-сервер локально на одном компьютере без необходимости доступа к сети.

Владелец информационных ресурсов – субъект, осуществляющий владение и пользование указанным объектом и реализующий полномочия распоряжения в пределах, установленных законом и собственникам информационных ресурсов.

Вооружённые Силы (ВС) государства – снабжаемые правительством оборонительные и боевые организации, используемые в интересах государства.

Всемирная паутина (World Wide Web) – это информационная система, основными компонентами которой являются гипертекстовые документы. Доступ к веб-документам осуществляется при помощи веб-серверов.

Гигабайт (обозначение Гбайт) – кратная единица измерения количества информации, равная 230 = 1 073 741 824 байт (согласно предложению международной электротехнической комиссии является гибибайтом).

Государственные информационные системы – создаются в целях реализации полномочий государственных органов и обес-печения обмена информацией между этими органами, а также в иных установленных федеральными законами целях.

Государственные символы – это один из неотъемлемых атрибутов любого государства, олицетворяющих его идентичность и суверенитет. В Кыргызской Республике государственными символами являются – Государственный Флаг, Государственный Герб и Государственный гимн.

Государственный бюджет – важнейший финансовый документ страны. Он представляет собой совокупность финансовых смет всех ведомств, государственных служб, правительственных программ и т.д. В нём определяются потребности, подлежащие удовлетворению за счёт государственной казны, равно как указываются источники и размеры ожидаемых поступлений в государственную казну.

Государственный орган – это составная, относительно самостоятельная часть аппарата государства, с установленной законом структурой, осуществляющая функции государства и наделённая для этого властными полномочиями.

Гражданин – человек, принадлежащий к постоянному населению данного государства, пользующийся его защитой и наделенный совокупностью политических и иных прав и обязанностей.

Гуглить – искать информацию в поисковике Google.

Данные Data – сведения, полученные путем измерения, наблюдения, логических или арифметических операций и представленные в форме, пригодной для постоянного хранения, передачи и (автоматизированной) обработки.

Девайс (от англ. «device») – любое компактное устройство (смартфон, планшет, умные часы и т.д.).

Дезинформация – заведомо ложная информация, предоставляемая противнику или деловому партнёру для более эффективного ведения боевых действий, сотрудничества, проверки на утечку информации и направление её утечки, выявление потенциальных клиентов чёрного рынка.

Дефолтный (**по дефолту**, от англ. «default») – тот, что используется по умолчанию, стандартный.

Джуниор (от англ. «**Junior** Developer», **Джун, Июнь**) – младший программист, который не имеет опыта или он у него небольшой. Как правило, джуниорами называют всех новичков, которые начали работать в IT-индустрии.

Документ выделенного хранения – ценный документ, изъятый по какой-то причине из дела, оформленный в самостоятельное дело и переведенный на инвентарный вид учета.

Документ конфиденциальный – документ ограниченного доступа, на любом носителе, содержащий информацию, отражающую приоритетные достижения в сфере экономической, производственной, предпринимательской, управленческой и другой деятельности, а также информацию, состав которой является принадлежностью служебной деятельности.

Документ машиночитаемый – официальный документ, созданный дня обеспечения работы вычислительной техники.

Документ подлинный – документ, сведения об авторе, времени и месте создания которого, содержащиеся в самом докуете или выявленные иным путем, подтверждают достоверность его происхождения.

Документ секретный – документ на любом носителе, отнесенный к информационным ресурсам ограниченного доступа и содержащий сведения, составляющие государственную тайну, которые включены в утвержденный специальный перечень таких сведений.

Документ черновой – рукописный, машинописный или электронный документ, отражающий работу автора или редактора над его текстом.

Документирование – запись информации на различных носителях по установленным правилам.

Документирование конфиденциальной информации – этап стадии исполнения конфиденциального документа.

Документооборот – движение документов в организации с момента их создания или получения до завершения исполнения или отправки.

Документооборот (документопоток) защищенный – контролируемое движение конфиденциальной документированной информации по регламентированным пунктам приема, обработки, рассмотрения, исполнения, использования и хранения в жестких условиях организационного и технологического обеспечения безопасности как носителя информации, так и самой информации.

Документопоток – движение документов в определенном направлении для облегчения решения управленческих задач. Существует: входящий (входной), исходящий (выходной) и внутренний документопотоки.

Допуск к конфиденциальной информации – часть разрешительной (разграничительной) системы доступа персонала к конфиденциальной информации, представляет собой процедуру оформления права сотрудника фирмы или иного лица на доступ к информации ограниченного распространения и одновременно правовой акт согласия (разрешения) собственника или владельца информации на передачу ее для работы конкретному лицу.

Достоверность информации – в криптографии: общая точность и полнота информации. Достоверность информации обратно пропорциональна вероятности возникновения ошибок в информационной системе.

Достоверность информации – информация достоверна, если она отражает истинное положение дел. Достоверная информация помогает принять нам правильное решение.

Доступ к базам данным и файлам – санкционирование полномочным должностным лицом работы сотрудника с определенным составом конфиденциальных сведений и файлов.

Доступ к информации несанкционированный – случайное или преднамеренное овладение конфиденциальными сведениями и возможное опасное воздействие на них лиц, не имеющих права доступа к конкретной защищаемой информации. Доступ, не санкционированный полномочным должностным лицом, считается незаконным.

Доступ к информации санкционированный – часть разрешительной (разграничительной) системы доступа персонала к конфиденциальной информации, представляет собой практическую реализацию права сотрудника на работу с подобной информацией, необходимой ему для выполнения возложенных на него функций. Доступ санкционируется полномочным должностным лицом (первым руководителем, его заместителем, руководителем подразделения, службы или направления деятельности) в отношении конкретной информации и конкретного сотрудника фирмы.

Доступ к компьютеру – санкционирование полномочным должностным лицом работы сотрудника с определенным составом вычислительной техники.

Доступ к машинным носителям, находящимся вне ЭВМ – санкционирование полномочным должностным лицом работы сотрудника с определенным составом носителей информации.

Доступность информации – избежание временного или постоянного сокрытия информации от пользователей, получивших права доступа.

Единица хранения архивных документов – учетная и классификационная единица, представляющая собой физически обособленный документ или совокупность документов, имеющих самостоятельное значение.

Единицы – Единица измерения – конкретная величина, определенная и установленная по договоренности, с которой сопоставляются другие величины того же рода, для того чтобы выразить их размер по отношению к указанной величине.

Жизненный цикл информационной системы – непрерывный процесс, начинающийся с момента принятия решения о создании информационной системы и заканчивающийся в момент полного изъятия ее из эксплуатации.

Защита информации – совокупность методов и средств, обеспечивающих целостность, конфиденциальность, достоверность, аутентичность и доступность информации в условиях воздействия на нее угроз естественного или искусственного характера.

Защита информации в службе персонала – направление обеспечения безопасности информации фирмы в части сохранения конфиденциальности персональных данных, которые формируются в процессе документирования трудовых правоотношений сотрудников с фирмой.

Защита информации при ведении переговоров и совещаний – направление обеспечения безопасности информации, которое распространяется в процессе этих мероприятий.

Защищенность информационной системы Security – способность системы противостоять несанкционированному доступу к конфиденциальной информации, ее искажению или разрушению.

Злоумышленник Intruder – субъект, оказывающий на информационный процесс воздействия с целью вызвать его отклонение от условий нормального протекания. В криптографии считается, что в распоряжении злоумышленника имеются все необходимые для выполнения его задачи технические средства, созданные на данный момент. Злоумышленник – лицо (группа лиц), предполагающее совершить или умышленно совершающее противоправные действия с целью овладения информацией, составляющей тот или иной вид тайны.

Злоумышленник Intruder – субъект, оказывающий на информационный процесс воздействия с целью вызвать его отклонение от условий нормального протекания. В криптографии считается, что в распоряжении злоумышленника имеются все необходимые для выполнения его задачи технические средства, созданные на данный момент. Злоумышленник – лицо (группа лиц), предполагающее совершить или умышленно совершающее противоправные действия с целью овладения информацией, составляющей тот или иной вид тайны.

Идентификатор – персональное обозначение (код, шифр, имя, пропуск, персональная карточка определенного цвета с фотографией, магнитная или иная карта и т. п.), позволяющее однозначно выделить идентифицируемый объект среди других в полном множестве объектов. Используется в системах доступа.

Идентификация пользователя – отождествление лиц по их характеристикам или путем опознавания по приметам или документам в целях определение полномочий, связанных с доступом к конфиденциальной информации. Присвоение имени пользователю информационной системы, потребителю информации.

Инженерно-технический элемент системы защиты информации – комплекс организационно-технических, технических и технологических мероприятий защиты информации, предназначенных для пассивного и активного противодействия средствам технической разведки и формирования рубежей охраны территории, здания, помещений и оборудования с помощью совокупности технических средств.

Интранет (Intranet) – внутренняя частная сеть организации. Важно, что информация в ней хранится в том же формате, что и в World Wide Web (Internet).

Информатика (фр. Informatique; англ. Computer science) – наука о методах и процессах сбора, хранения, обработки, передачи, анализа и оценки информации с применением компьютерных технологий, обеспечивающих возможность её использования для принятия решений.

Информационная безопасность – состояние защищенности информационной среды общества, обеспечивающее ее формирование, использование и развитие в интересах граждан, организаций, государства.

Информационная открытость – это организационно-правовой режим деятельности любого участника социального взаимодействия, обеспечивающий любым участникам этого взаимодействия возможность получать необходимый и достаточный объем информации (сведений) о своей структуре, целях, задачах, финансовых и иных существенных условиях деятельности.

Информационная система (автоматизированная информационная система) – это совокупность технических (аппаратных) и программных средств, а также работающих с ними пользователей (персонала), обеспечивающая информационную технологию выполнения установленных функций.

Информационно-технологическая инфраструктура (Information Technology Infrastructure) – все информационные технологии, используемые в рамках одной организации: компьютеры, сети, программное обеспечение и т.п.

Информационные ресурсы – отдельные документы и отдельные массивы документов, документы и массивы документов в информационных системах (библиотеках, архивах, фондах, банках данных, других информационных системах).

Информационные ресурсы ограниченного доступа – документы и массивы документов, содержащие сведения, отнесенные к тому или иному виду тонны и подлежащие защите, охране, наблюдению и контролю.

Информационный барьер – это противоречие между информационными запросами сообщества (общества) и имеющимися техническими возможностями их удовлетворения.

Информационный взрыв – постоянное увеличение скорости и объёмов публикаций (объёма информации) в масштабах планеты.

Информационный процесс – процесс получения, создания, сбора, обработки, накопления, хранения, поиска, распространения, представления и использования информации.

Информация – сведения о лицах, предметах, фактах, событиях, явлениях и процессах независимо от формы их представления.

Информация (в переводе от лат. informātiō – «разъяснение, представление, понятие о чём-либо», от лат. informare – «воображать, придавать вид, мыслить, форму, обучать;») – сведения независимо от формы их представления.

Информация защищаемая – синоним понятий информация секретная и информация конфиденциальная. Информация может быть отнесена к категории защищаемой, если ее содержание неизвестно конкуренту или противнику, а также, если указанная неизвестность дает определенные преимущества в политической, экономической или предпринимательской деятельности. При отнесении информации к защищаемой должны соблюдаться принципы законности, обоснованности, своевременности и др.

Информация конфиденциальная – документированная информация, относимая к одному из видов негосударственной тайны или персональным данным, доступ к которой ограничивается в соответствии с законами. Решение о таком ограничении принимает собственник или владелец указанной информации, т. е. он устанавливает правовой режим информации, являющейся его интеллектуальной собственностью (кроме персональных данных).

Информация ценная – информация, которая составляет интеллектуальную собственность предпринимателя или группы предпринимателей и дает им возможность производить качественную продукцию, товары и услуги, пользующиеся повышенным спросом на рынке, заключать выгодные сделки, находить новых клиентов, покупателей как самой продукции, так и технологии ее производства.

Источник конфиденциальной информации – объективно пассивный накопитель (концентратор) конфиденциальной информации. В научной литературе часто используется альтернативный для сферы защиты информации термин – «носитель конфиденциальной информации» по аналогии с термином «секретоноситель».

Источник угрозы конфиденциальной информации – объективные и субъективные явления, события, факторы, действия и обстоятельства, содержащие опасность для ценной информации. К объективным источникам можно отнести: экстремальные ситуации, несовершенство технических средств и др. Субъективные источники связаны с человеческим фактором и включают злоумышленников различного рода, посторонних лиц, посетителей, неквалифицированный или безответственный персонал, психически неполноценных людей, сотрудников, обиженных руководством фирмы, и др.

Канал несанкционированного доступа к информации – совокупность незащищенных или слабо защищенных фирмой направлений возможной утраты конфиденциальной информации, которые злоумышленник использует для получения необходимых сведений, преднамеренного незаконного доступа к защищаемой информации.

Кейс (от англ. **«case»**) – реальная ситуация/случай, которые произошли с автором.

Кибернетика (от др.-греч. κυβερνητική – «искусство управления») – наука об общих закономерностях получения, хранения, преобразования и передачи информации в сложных управляющих системах, будь то машины, живые организмы или общество.

Килобайт (русское обозначение: Кбайт; международное: Kbyte, KB) – единица измерения количества информации, равная 1024 байт.

Клиент – активное и отдельное от сервера программное обеспечение, использующее данные, поставляемые сервером путем передачи клиентских запросов серверу.

Конвертование (пакетирование) конфиденциальных документов – совокупность технических приемов, предотвращающих несанкционированное тайное вскрытие конвертов (пакетов) и извлечение из них конфиденциальных документов, а также прочтение текста без извлечения документа и даже вскрытия конверта.

Конституция (от лат. constitutio – устройство, установление, сложение) – основной закон государства, особый нормативный правовой акт, имеющий высшую юридическую силу.

Контроль доступа – регулярные проверочные действия по определению правомерности разрешений на доступ и доступа сотрудников фирмы и представителей других организационных

структур в помещения фирмы, к конфиденциальным документам, делам, базам данных, компьютерам и средствам связи.

Контроль доступа (Access auditing) – процесс защиты данных и программ от их использования объектами, не имеющими на это права.

Контроль эффективности системы защиты информации – анализ степени уязвимости конфиденциальной информации.

Конфиденциальная информация (Confidential information) – информация, доступ к которой ограничивается в соответствии с законодательством страны и уровнем доступа к информационному ресурсу. Конфиденциальная информация становится доступной или раскрытой только санкционированным лицам, объектам или процессам.

Конфиденциальность (лат. confidentia – доверие) – доверительность, секретность. Не оглашаемая, доверительная, задушевная беседа, письмо, сообщение, полученное по доверенности, тайное общение, тайные переговоры, беседы, документирование с использованием тайнописи.

Криптографический элемент системы защиты информации –комплекс способов и средств защиты конфиденциальной информации методами криптографии.

Криптография – тайнопись, система разнообразных способов изменения формы отображения информации (текста, речи), позволяющих сделать содержание информации непонятным для лиц, не владеющих знанием использованного шифра.

Кыргызская Республика – страна в Центральной Азии, государство в западной и центральной части горного массива Тянь-Шань.

Лицензирование в области защиты информации – установленное законодательством право заниматься работами по защите информации для стороннего заказчика.

Математика (др.-греч. μᾰθημᾰτικά [1] <др.-греч. μάθημα – изучение, наука) – наука о структурах, порядке и отношениях, исторически сложившаяся на основе операций подсчёта, измерения и описания формы объектов [2]. Математические объекты создаются путём идеализации свойств реальных или других математических объектов и записи этих свойств на формальном языке. Математика не относится к естественным наукам, но широко используется в них как для точной формулировки их содержания, так и для получения новых результатов. Математика – фундаментальная наука, предоставляющая (общие) языковые средства другим наукам; тем самым она выявляет их структурную взаимосвязь и способствует нахождению самых общих законов природы.

Машинограмма – документ, изготовленный автоматически средствами вычислительной техники (например, с помощью принтера) на бумажном носителе в человеко-читаемой форме и предназначенный для оформления в установленном порядке.

Мегабайт (русское обозначение: Мбайт; международное: Mbyte, MB) – единица измерения количества информации, обозначающая, в зависимости от контекста, 1 000 000 (106) или 1 048 576 (220) байт.

Метаданные (Metadata) – данные о данных: каталоги, справочники, реестры, базы метаданных, содержащие сведения о составе данных, содержании, статусе, происхождении, местонахождении, качестве, форматах и формах представления, условиях доступа, приобретения и использования, авторских, имущественных и смежных с ними правах на данные и др.

Методы защиты информации – выборочно применяемые универсальные и специфические способы (приемы, меры, мероприятия) реализации элементов системы защиты информации и входящих в них содержательных частей для формирования комплексной и индивидуальной структуры данной системы.

Методы легального получения информации – вид «невинного шпионажа», отличающийся правовой безопасностью, но предопределяющий возникновение интереса к конкурирующей фирме, необходимости обнаружения или формирования и использования каналов несанкционированного доступа к ее ценной, конфиденциальной информации.

Методы нелегального получения информации – всегда носят незаконный характер и используются в целях несанкционированного доступа.

Налоговая система – это совокупность налогов и сборов, взимаемых с плательщиков в порядке и на условиях, определенных Налоговым кодексом.

Нарушение безопасности информации – событие, при котором компрометируется один или несколько аспектов безопасности информации (доступность, конфиденциальность, целостность и достоверность).

Нормативно-методическое обеспечение системы защиты информации – комплекс документов, регламентирующих процесс функционирования системы защиты информации, сформированной в целях безопасности информации конкретной фирмы, а также регламентирующих функционирование службы безопасности этой фирмы.

Носитель информации – (информационный носитель) любой материальный объект или среда, содержащий (несущий) информацию (И), способный достаточно длительное время сохранять в своей структуре занесённую в/на него информацию камень, дерево и т.п.

Нуб (нубчик, нубас, нубарь, нубак) – новичок или человек у которого ничего не получается, или он не знает, как правильно делать. Неопытный, новенький.

Обработка данных (Data processing; Performing data) – процесс выполнения последовательности операций над данными. Обработка данных может осуществляться в интерактивном и фоновом режимах.

Обработка изданных документов – технологическая стадия, в процессе которой выполняются технологические этапы процедуры и операции по отправке документов адресатам или передаче внутренних документов для использования в управлении основной деятельностью фирмы.

Обязательство о неразглашении конфиденциальных сведений – правовой документ, добровольное письменное согласие претендента на должность, сотрудника фирмы или иного лица на ограничение его права в отношении использования конфиденциальной информации фирмы.

Политика информационной безопасности (Security policy) – совокупность правил, определяющих и ограничивающих виды деятельности объектов и участников, системы информационной безопасности.

Пользователь (потребитель) информационных ресурсов – лицо (субъект), обращающееся к информационной системе или посреднику за получением необходимой ему информации и пользующееся ею. Пользователь не может участвовать в проектировании, модернизация или эксплуатации, контроле эффективности системы защиты информации.

Портал – большой и сложный сайт, где интегрировано много информации различного рода.

Почтовый сервер (Mail Server) – компьютер, отвечающий за прием, хранение и обработку электронной почты.

Право – основное понятие юриспруденции, один из видов регуляторов общественных отношений; система общеобязательных, формально-определённых, гарантированных государством правил поведения.

Право информационное – совокупность законодательных информационно-правовых норм, регулирующих общественные отношения в информационной сфере и являющихся гарантированным инструментом охраны интеллектуальной информационной собственности (информационного продукта) юридических и физических лиц.

Правовой элемент системы защиты информации – юридическое закрепление взаимоотношений фирмы и государства по поводу правомерности использования системы защиты информации, фирмы и персонала по поводу обязанности персонала соблюдать установленные собственником информации ограничительные и технологические меры защитного характера, а также ответственности персонала за нарушение порядка защиты информации.

Провайдер – компания, предоставляющая услуги доступа Интернет и возможно, другие услуги, такие как хостинг, e-mail и др. Большинство провайдеров предоставляет доступ в Интернет посредством модема частным лицам.

Программно-аппаратный элемент системы защиты информации – комплекс специальных методов и средств защиты информации в автоматизированных системах и сетях.

Программное обеспечение (ПО) (Software) – комплекс программ, обеспечивающих обработку или передачу данных, предназначенных для многократного использования и применения разными пользователями.

Программный сервер, серверное программное обеспечение (server) – (англ. server от англ. to serve – служить) – в информационных технологиях – программный компонент вычислительной системы, выполняющий сервисные (обслуживающие) функции по запросу клиента, предоставляя ему доступ к определённым ресурсам или услугам. Пассивная сторона системы клиент-сервер.

Противодействие злоумышленнику – целенаправленное создание неблагоприятных условий и трудно преодолимых препятствий (рубежей) для лица, пытающегося совершить несанкционированный доступ и овладение конфиденциальной информацией фирмы. Может быть пассивным и активным. При пассивном противодействии система защиты информации функционирует в обычном режиме, ведется плановая аналитическая и контрольная работа с источниками и каналами

распространения информации, организационными и техническими каналами возможного несанкционированного доступа к конфиденциальной информации. Активное противодействие предполагает подключение дополнительных организационных и технических методов защиты информации (например, закрытие доступа к определенным категориям информации, организацию усиленной охраны здания и помещений, ограничение деловых связей фирмы и др.).

Рабочая станция – периферийный компьютер в составе локальной вычислительной сети (ЛВС), играющий роль интерфейса по отношению к серверу.

Разглашение конфиденциальной информации – несанкционированный выход конфиденциальных сведений и документов за пределы круга лиц, которым они были доверены или стали известны по службе. Разглашение (огласка, оглашение) информации происходит по вине персонала – случайно, ошибочно или умышленно, добровольно (инициативно) или под воздействием угроз, шантажа, применения наркотических средств, психотропных препаратов.

Раздробление тайны – классифицированное (иерархическое) дробление предметной совокупности конфиденциальной информации на тематические группы, отдельные элементы, части, известные разным сотрудникам фирмы.

Разрешительная (разграничительная) система доступа к информации – совокупность обязательных норм, устанавливаемых первым руководителем или коллективным органом руководства фирмой с целью закрепления за руководителями и сотрудниками права использования для выполнения служебных обязанностей выделенных помещений, рабочих мест, определенного состава документов и конфиденциальных сведений.

Режим конфиденциальности – комплекс мер, входящих в состав действующей в фирме системы защиты информации и обеспечивающих особый правовой статус организации работы сотрудников фирмы.

Секрет – см. Тайна.

Секретность данных (Secrecy) – свойство данных быть известными и доступными только тому кругу субъектов, для которого они предназначены.

Семиотика – комплекс научных теорий, изучающих свойства знаковых систем.

Сервер (server) – объект, предоставляющий сервис другим объектам по их запросам. В Интернете – компьютер, подключенный к сети, или выполняющаяся на нем программа, предоставляющие клиентам доступ к общим ресурсам и управляющие этими ресурсами.

Сервер баз данных, сервер БД – программное обеспечение, обслуживающее базу данных и отвечающее за целостность и сохранность данных, а также обеспечивающее операции ввода-вывода при доступе клиента к информации, то есть то же самое, что корпоративная СУБД.

Сервер доступа к данным – программный компонент СУБД, обслуживающий базу данных и отдающий данные по запросам.

Сервер-компьютер – компьютер, выполняющий только серверные задачи, или компьютер (или иное аппаратное обеспечение), специализированный (по форм-фактору и/или ресурсам) для использования в качестве аппаратной базы для программных серверов.

Сертификация систем и средств защиты информации – аналитические действия по определению эффективности систем защиты информационных ресурсов, качества программных, аппаратных и иных средств защиты. Выполняется специализированной организацией, имеющей соответствующую лицензию. В соответствии с положительными результатами анализа выдается сертификат, удостоверяющий возможность использования указанных систем и средств защиты для обеспечения информационной безопасности фирмы.

Система зашиты информации – совокупность направлений, методов, средств и мероприятий, снижающих уязвимость информации и препятствующих несанкционированному доступу к информации, ее разглашению или утечке.

Система обеспечения безопасности (Security system) – совокупность стандартных защитных мер: криптографическое кодирование, паролирование, присваивание идентификатора, электронная цифровая подпись и т.д.

Система охраны здания, помещений, транспорта и персонала – комплекс организационных и технических мероприятий, реализующих одну из основных функций службы безопасности фирмы.

Системы общения on line – это специализированные средства, позволяющие в реальном времени организовать общение пользователей по каналам компьютерной связи.

Скрин (**скриншот,** от англ. **«screenshot»**) – снимок экрана.

Служба безопасности – самостоятельное структурное подразделение фирмы, обеспечивающее экономическую безопасностью функционирования. В негосударственных структурах подобная служба создается по усмотрению руководящего органа фирмы.

Справочно-информационный банк данных автоматизированный – структурированная совокупность сведений о документах, хранящихся в памяти ЭВМ.

Справочно-информационный банк данных по конфиденциальным документам – структурированная совокупность применяемых учетных форм.

Средства защиты информации – технические, криптографические, программные и другие средства, входящие в структуру отдельных элементов системы защиты информации и предназначенные для обеспечения защиты сведений, составляющих тайну фирмы, а также средства, в которых они реализованы, или предназначены для контроля эффективности системы защиты информации.

Сроки конфиденциальности информации – временной период ограничения доступа персонала и иных лиц к конфиденциальной информации. Характеризуется большим разбросом во времени – от нескольких часов до нескольких лет.

Структура данных (Data structure) – организационная схема записи или массива, в соответствии с которой упорядочены данные, с тем чтобы их можно было интерпретировать и выполнять над ними определенные операции.

Субъективность информации – информация существует только во взаимосвязи с субъектом, передающим эту информацию, и зависит от человеческого сознания. Информация – это субъективное отражение внешнего объективного мира.

Суд – орган государства, осуществляющий правосудие в форме рассмотрения и разрешения уголовных, гражданских, административных и иных категорий дел в установленном законом конкретного государства процессуальном порядке.

Телеконференция – это система обмена информацией между множеством пользователей.

Теория информации – раздел прикладной математики, радиотехники (теория обработки сигналов) и информатики, относящийся к измерению количества информации, её свойств и устанавливающий предельные соотношения для систем передачи данных. Как и любая математическая теория, теория, оперирует математическими моделями, а не реальными физическими объектами (источниками и каналами связи). Использует, главным образом, математический аппарат теории вероятностей и математической статистики.

Теория управления – наука о принципах и методах управления различными системами, процессами и объектами.

Технические средства охраны, сигнализации и идентификации – специальные сооружения, оборудование и приборы, создающие препятствия на пути злоумышленника и оповещающие персонал охраны о попытке несанкционированного проникновения в здание фирмы, хранилища, другие охраняемые, выделенные помещения, к компьютерам, средствам связи.

Технологическая система обработки и хранения конфиденциальных документов автоматизированная – комплекс организационных и технологических процедур и операций с документами, выполняемый на базе вычислительной техники и средств связи. Система, как и традиционная, делопроизводственная, обеспечивает конкретные потребности персонала в конфиденциальной информации.

Технологическая система обработки и хранения конфиденциальных документов – упорядоченный комплекс организационных и технологических процедур и операций, обеспечивающих служб и технических средств, предназначенных для практической реализации задач, стоящих пред функциональными элементами (стадиями) документопотока.

Технология информационная защищенная – совокупность комплексных технологических систем, организационных структур, ограничительных методов и технических средств, предназначенных для традиционной и (или) автоматизированной обработки **конфиденциальной информации и документов**, решающих задачи информационного обеспечения управленческой и производственной деятельности в жестких условиях информационной безопасности обрабатываемых информационных ресурсов.

Точность информации – определяется степенью ее близости к реальному состоянию объекта, процесса, явления и т.п.

Транзакция – одно действие или их последовательность, выполняемых одним или несколькими пользователями (прикладными программами) с целью осуществления доступа или

изменения информации, воспринимаемых как единое целое и переводящих ее из одного непротиворечивого (согласованного) состояния в другое непротиворечивое состояние.

Трафик (Traffic) – поток данных, передаваемых по сети.

ТС (**топик стартер**, от англ. «topic starter») – человек, который начал обсуждение определенной темы на определенном ресурсе (чаще всего, на форуме).

Угроза безопасности (Threat) – в широком смысле – потенциальное нарушение безопасности. Угроза безопасности – в системах обработки данных – потенциальное действие или событие, которое может привести к нарушению одного или более аспектов безопасности информационной системы.

Угроза безопасности конфиденциальной информации – единичное или комплексное, реальное или потенциальное, активное или пассивное проявление злоумышленных возможностей внешних или внутренних источников угрозы конфиденциальной информации создавать неблагоприятные события, оказывать дестабилизирующее воздействие на защищаемую информацию.

Универсальный (сетевой) сервер – особый вид серверной программы, не предоставляющий никаких услуг самостоятельно. Вместо этого универсальные серверы предоставляют серверам услуг упрощенный интерфейс к ресурсам меж процессного взаимодействия и/или унифицированный доступ клиентов к различным услугам.

Уничтожение документов, дел и носителей информации – комплекс технологических приемов и правил, исключающих возможность ознакомления посторонних лиц с уничтожаемыми конфиденциальными материалами или подмены материалов.

Управление данными (Data management) – процесс, связанный с накоплением, организацией, запоминанием, обновлением, хранением данных и поиском информации.

Установление грифа конфиденциальности – этап стадии исполнения конфиденциального документа на любом носителе.

Утечка конфиденциальной информации – неконтролируемый выход конфиденциальной информации за пределы фирмы или охраняемой зоны. Связана с возможным перехватом информации злоумышленником с помощью технических средств разведки.

Утрата информацией конфиденциальности – переход информации в категорию общедоступной, известной конкуренту, информации открытого доступа. Санкционированной может быть только одна причина – снятие с традиционного или элект-ронного документа грифа конфиденциальности в соответствии с установленными в фирме правилами. Несанкционированных причин может быть несколько, но все они являются следствием утраты конфиденциальности информации.

Уязвимость информации – объективное свойство информации подвергаться различного рода воздействиям (опасностям, угрозам), нарушающим ее целостность, достоверность и конфи-денциальность.

Файл-сервер – программный сервер для обеспечения доступа к файлам на диске сервера. Прежде всего это серверы передачи файлов по заказу, по протоколам FTP, TFTP, SFTP и HTTP. Протокол HTTP ориентирован на передачу текстовых файлов, но серверы могут отдавать в качестве запрошенных файлов и произвольные данные, например, динамически созданные веб-страницы, картинки, музыку и т.п.

Фальсификация документов – изготовление и использование в каких-либо целях ложного документа, в том числе злоумышленной подмены подлинного документа в целом или его отдельных частей поддельными, изготовленными для приобретения незаконных прав, выполнения противоправных действий в отношении фирмы или ее персонала.

Физика (от др.-греч, φύσις – природа) – область естествознания: наука о простейших и, вместе с тем, наиболее общих законах природы, о материи, её структуре и движении.

Хакер (Hacker) (от англ. Hack – кромсать) – лицо, совершающее различного рода незаконные действия в сфере информатики, несанкционированное проникновение в чужие компьютерные сети и получение из них информации, незаконные снятие защиты с программных продуктов и их копирование, создание и распространения компьютерных вирусов и т.п. Действия хакера образуют различные составы уголовных преступлений и гражданских правонарушений.

Хакер (Hacker) киберпреступник – специалист, занимающийся поиском слабых мест в вычислительных системах и осуществлением атак на данные системы.

Хостинг (Hosting) – предоставление в аренду вычислительных мощностей и ресурсов провайдера для размещения информационных ресурсов Заказчика, а также хранения, обработки и

передачи специфической информации в интересах последнего, как правило, на базе арендной платы. Это позволяет клиенту разместить свой ресурс (WWW-сайт) на оборудовании хостинг-провайдера, не используя при этом собственного. Плюсы этой услуги очевидны – это отсутствие нагрузки по администрированию серверного программного обеспечения и оборудования.

Хранение конфиденциальных документов и дел – нахождение документов и дел в специальном хранилище, обеспечивающем их сохранность. Осуществляется службой конфиденциальной документации в отношении неисполненных и исполненных документов.

Целостность данных (Data integrity) – свойство, при выполнении которого данные сохраняют заранее определенный вид и качество.

Чрезвычайное положение (ЧП) – особый правовой режим деятельности органов государственной власти и управления, предприятий, учреждений и организаций, вводимый в стране или отдельных её районах для защиты от внешней или внутренней угрозы, поддержания общественного порядка.

Чувствительная информация (критическая информация) (Sensitive information) – информация, несанкционированное раскрытие, модификация или сокрытие которой может привести к ощутимому убытку или (денежному) ущербу.

Чувствительная информация (критическая информация) (Sensitive information) – информация, несанкционированное раскрытие, модификация или сокрытие которой может привести к ощутимому убытку или (денежному) ущербу.

Шифр – совокупность условных знаков для преобразования информации в вид, исключающий ее восстановление (дешифрование и прочтение) в условиях отсутствия у злоумышленника ключа для раскрытия шифра.

Шифрование – криптографическое (математическое, алгоритмическое) преобразование информации с целью получения шифрованного текста или устной речи

Шпионаж – похищение, добывание, собирание и передача с целью корыстного использования или выдачи конкуренту (противнику) сведений, составляющих тайну.

Шпионаж промышленный – получение предпринимателем самостоятельно или с помощью соответствующих специалистов (злоумышленников), обманным или иным незаконным путем конфиденциальной информации с целью овладения ею для достижения технического, технологического или коммерческого преимущества, банкротства конкурента.

Шпионаж экономический – широкое понятие, которое охватывает такие виды шпионажа, как промышленный, коммерческий, научно-технический, производственный и др.

Штатные средства – совокупность программного и аппаратного обеспечения рассматриваемой информационной системы.

Экстремальная (чрезвычайная) ситуация – явление, событие, нарушающее нормальное функционирование фирмы, работу персонала, создающее опасность для целостности и сохранности здания, помещений, оборудования и документации фирмы, угрожающее жизни и здоровью сотрудников. Экстремальные ситуации объективного характера связаны со стихийными бедствиями (ураганами, наводнениями и др.), неуправляемыми процессами, военными действиями, кризисами, авариями энергоснабжения и водоснабжения и другими подобными событиями. Экстремальные ситуации могут быть случайного (фатального) характера – возгорание оборудования и коммуникаций, разрушение конструкций, а также связаны с неосторожностью и безответственностью персонала (возгорания от неосторожного обращения с огнем, курения на рабочих местах, неумелой эксплуатации оборудования и др.).

Электронная почта (e-mail) – это система пересылки электронной корреспонденции между пользователями телекоммуникационной сети.

Электронное правительство (англ. e-Government) – пакет технологий и набор сопутствующих организационных мер, нормативно-правового обеспечения для организации цифрового взаимодействия между органами государственной власти различных ветвей власти, гражданами, организации и другими субъектами экономики.

Юриспруденция (лат. jūris prūdentia – «правоведение», от лат. jūs, род. п. jūris – «право» и лат. prūdentia – «предвидение», «знание») – наука, изучающая свойства государства и права; совокупность правовых знаний; практическая деятельность юристов и система их подготовки.