МИНОБРНАУКИ РОССИИ

ВЛАДИВОСТОКСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

КАФЕДРА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Рабочая программа дисциплины (модуля)

УПРАВЛЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ

Специальность и специализация
10.05.03 Информационная безопасность автоматизированных систем. Безопасность открытых информационных систем

Год набора на ОПОП
2022

Форма обучения
очная

Владивосток 2023

Рабочая программа дисциплины (модуля) «Управление информационной безопасностью» составлена в соответствии с требованиями ФГОС ВО по направлению подготовки 10.05.03 Информационная безопасность автоматизированных систем (утв. приказом Минобрнауки России от 26.11.2020г. №1457) и Порядком организации и осуществления образовательной деятельности по образовательным программам высшего образования – программам бакалавриата, программам специалитета, программам магистратуры (утв. приказом Минобрнауки России от 06.04.2021 г. N245).

Составитель(и):

Шумик Е.Г., кандидат экономических наук, доцент, Кафедра математики и моделирования, Ekaterina.Shumik1@vvsu.ru

Утверждена на заседании кафедры информационной безопасности от «____»_____20__г. , протокол № _____

СОГЛАСОВАНО:

Заведующий кафедрой (разработчика)
Шумик Е.Г.

ДОКУМЕНТ ПОДПИСАН ЭЛЕКТРОННОЙ ПОДПИСЬЮ	
Сертификат	eg_1575874368
Номер транзакции	0000000000BBEC5A
Владелец	Шумик Е.Г.

1 Цель, планируемые результаты обучения по дисциплине (модулю)

Целью изучения дисциплины «Управление информационной безопасностью» является изучение основных понятий, методологии и практических приемов управления технической и организационной инфраструктурой обеспечения информационной безопасности на предприятии.

Задачей является:

- приобретение обучаемыми необходимого объема знаний и практических навыков в области стандартизации и нормотворчества в управлении информационной безопасностью, организации работы и разграничения полномочий персонала, ответственного за информационную безопасность;
- в рамках задач обеспечения информационной безопасности решать вопросы использования радиоэлектронной аппаратуры и других технических средств, используя современные методы и средства разрабатывать и оценивать модели и политику безопасности;
- формирование у обучаемых целостного представления об организации и содержании процессов управления информационной безопасностью на предприятии как результата внедрения системного подхода к решению задач обеспечения информационной безопасности;
- приобретение обучаемыми необходимого объема знаний и практических навыков в области практического решения задач защиты программ и данных программно-аппаратными средствами: и давать оценку качества предлагаемых решений; проектирования и реализации комплексной системы защиты информации, оценки их качество.

Планируемыми результатами обучения по дисциплине (модулю), являются знания, умения, навыки. Перечень планируемых результатов обучения по дисциплине (модулю), соотнесенных с планируемыми результатами освоения образовательной программы, представлен в таблице 1.

Таблица 1 – Компетенции, формируемые в результате изучения дисциплины (модуля)

Название ОПОП ВО, сокращенное	Код и формулировка компетенции	Код и формулировка индикатора достижения компетенции	Результаты обучения по дисциплине	
			Код результата	Формулировка результата
10.05.03 «Информационная безопасность автоматизированных систем» (ИБ)				

2 Место дисциплины (модуля) в структуре ОПОП

3. Объем дисциплины (модуля)

Объем дисциплины (модуля) в зачетных единицах с указанием количества академических часов, выделенных на контактную работу с обучающимися (по видам учебных занятий) и на самостоятельную работу, приведен в таблице 2.

Таблица 2 – Общая трудоемкость дисциплины

Название ОПОП ВО	Форма обучения	Часть УП	Семестр (ОФО) или курс (ЗФО, ОЗФО)	Трудоемкость	Объем контактной работы (час)						СРС	Форма аттестации
				(З.Е.)	Всего	Аудиторная			Внеаудиторная			
						лек.	прак.	лаб.	ПА	КСР		
10.05.03 Информационная безопасность автоматизированных систем	ОФО	С1.Б	10	4	83	36	36	0	1	10	61	ДЗ

4 Структура и содержание дисциплины (модуля)

4.1 Структура дисциплины (модуля) для ОФО

Тематический план, отражающий содержание дисциплины (перечень разделов и тем), структурированное по видам учебных занятий с указанием их объемов в соответствии с учебным планом, приведен в таблице 3.1

Таблица 3.1 – Разделы дисциплины (модуля), виды учебной деятельности и формы текущего контроля для ОФО

№	Название темы	Код результата обучения	Кол-во часов, отведенное на				Форма текущего контроля
			Лек	Практ	Лаб	СРС	
1	Введение в дисциплину	РД1, РД2	8	8	0	7	Тестовые задания, практические работы
2	Система управления информационной безопасностью автоматизированных систем.	РД1, РД2	8	8	0	18	Тестовые задания, практические работы
3	Аудит информационной безопасности	РД1, РД2	10	10	0	18	Тестовые задания, практические работы
4	Средства поддержки процессов управления информационной безопасностью автоматизированных систем	РД1, РД2	10	10	0	18	Тестовые задания, практические работы
Итого по таблице			**36**	**36**	**0**	**61**	

4.2 Содержание разделов и тем дисциплины (модуля) для ОФО

Ошибка SQL:!Coundn't execute query:EXECUTE doc_flow..RPD_disContent 2152032606, 1System.Data.SqlClient.SqlException (0x80131904): FOR XML не удалось сериализовать данные для узла "NoName", так как в нем содержится символ (0x0002), недопустимый в XML. Для получения этих данных с использованием FOR XML преобразуйте их в тип данных binary, varbinary или image data и воспользуйтесь директивой BINARY BASE64. в System.Data.SqlClient.SqlConnection.OnError(SqlException exception, Boolean breakConnection, Action`1 wrapCloseInAction) в System.Data.SqlClient.SqlInternalConnection.OnError(SqlException exception, Boolean breakConnection, Action`1 wrapCloseInAction) в System.Data.SqlClient.TdsParser.ThrowExceptionAndWarning(TdsParserStateObject stateObj, Boolean callerHasConnectionLock, Boolean asyncClose) в System.Data.SqlClient.TdsParser.TryRun(RunBehavior runBehavior, SqlCommand cmdHandler, SqlDataReader dataStream, BulkCopySimpleResultSet bulkCopyHandler, TdsParserStateObject stateObj, Boolean& dataReady) в System.Data.SqlClient.SqlDataReader.TryHasMoreRows(Boolean& moreRows) в System.Data.SqlClient.SqlDataReader.TryReadInternal(Boolean setTimeout, Boolean& more) в System.Data.SqlClient.SqlDataReader.Read() в

System.Data.Common.DataAdapter.FillLoadDataRow(SchemaMapping mapping) в System.Data.Common.DataAdapter.FillFromReader(DataSet dataset, DataTable datatable, String srcTable, DataReaderContainer dataReader, Int32 startRecord, Int32 maxRecords, DataColumn parentChapterColumn, Object parentChapterValue) в System.Data.Common.DataAdapter.Fill(DataSet dataSet, String srcTable, IDataReader dataReader, Int32 startRecord, Int32 maxRecords) в System.Data.Common.DbDataAdapter.FillInternal(DataSet dataset, DataTable[] datatables, Int32 startRecord, Int32 maxRecords, String srcTable, IDbCommand command, CommandBehavior behavior) в System.Data.Common.DbDataAdapter.Fill(DataSet dataSet, Int32 startRecord, Int32 maxRecords, String srcTable, IDbCommand command, CommandBehavior behavior) в System.Data.Common.DbDataAdapter.Fill(DataSet dataSet) в AUTH.DataBaseClient.Get_Data(String Query) в X:\dev\RTFReport\DataBaseClient.cs:строка 110 ClientConnectionId:65319b60-ad6a-4c45-94dd-936572ece59c Error Number: 6841, State: 1, Class: 16.!

5 Методические указания для обучающихся по изучению и реализации дисциплины (модуля)

5.1 Методические рекомендации обучающимся по изучению дисциплины и по обеспечению самостоятельной работы

Самостоятельная работа студентов (СРС) — это деятельность учащихся, которую они совершают без непосредственной помощи и указаний преподавателя, руководствуясь сформировавшимися ранее представлениями о порядке и правильности выполнения операций. Цель СРС в процессе обучения заключается, как в усвоении знаний, так и в формировании умений и навыков по их использованию в новых условиях на новом учебном материале. Самостоятельная работа призвана обеспечивать возможность осуществления студентами самостоятельной познавательной деятельности в обучении, и является видом учебного труда, способствующего формированию у студентов самостоятельности. В данной учебной программе приведен перечень основных и дополнительных источников, которые предлагается изучить в процессе облучения по дисциплине. Кроме того, для расширения и углубления знаний по данной дисциплине целесообразно использовать: научные публикации в тематических журналах; полнотекстовые базы данных библиотеки; имеющиеся в библиотеках вуза и региона публикаций на электронных и бумажных носителях. Успешное освоение дисциплины предполагает активную работу студентов на всех занятиях аудиторной формы: лекций и практических занятий, выполнение аттестационный мероприятий, эффективную самостоятельную работу. В процессе изучения дисциплины студенту необходимо ориентироваться на самостоятельную проработку лекционного материала, подготовку к практическим занятиям, выполнение тестов, кейсовых заданий, самостоятельное изучение некоторых разделов курса Для проведения занятий лекционного типа используются учебно-наглядные пособия в форме презентационных материалов, обеспечивающих тематические иллюстрации, соответствующие темам лекций, представленным в пункте 5 настоящей РПД.

5.2 Особенности организации обучения для лиц с ограниченными возможностями здоровья и инвалидов

При необходимости обучающимся из числа лиц с ограниченными возможностями здоровья и инвалидов (по заявлению обучающегося) предоставляется учебная информация в доступных формах с учетом их индивидуальных психофизических особенностей:

- для лиц с нарушениями зрения: в печатной форме увеличенным шрифтом; в форме электронного документа; индивидуальные консультации с привлечением тифлосурдопереводчика; индивидуальные задания, консультации и др.

- для лиц с нарушениями слуха: в печатной форме; в форме электронного документа; индивидуальные консультации с привлечением сурдопереводчика; индивидуальные задания, консультации и др.

- для лиц с нарушениями опорно-двигательного аппарата: в печатной форме; в форме электронного документа; индивидуальные задания, консультации и др.

6 Фонд оценочных средств для проведения текущего контроля и промежуточной аттестации обучающихся по дисциплине (модулю)

В соответствии с требованиями ФГОС ВО для аттестации обучающихся на соответствие их персональных достижений планируемым результатам обучения по дисциплине (модулю) созданы фонды оценочных средств. Типовые контрольные задания, методические материалы, определяющие процедуры оценивания знаний, умений и навыков, а также критерии и показатели, необходимые для оценки знаний, умений, навыков и характеризующие этапы формирования компетенций в процессе освоения образовательной программы, представлены в Приложении 1.

7 Учебно-методическое и информационное обеспечение дисциплины (модуля)

7.1 Основная литература

1. Зырянова, Т. Ю. Управление информационной безопасностью : учебное пособие / Т. Ю. Зырянова. — Екатеринбург : , 2023. — 96 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/369482 (дата обращения: 28.02.2024). — Режим доступа: для авториз. пользователей.

2. Поздняк, И. С. Планирование и управление информационной безопасностью : учебное пособие / И. С. Поздняк, И. С. Макаров, Л. Р. Чупахина. — Самара : ПГУТИ, 2020. — 69 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/255569 (дата обращения: 28.02.2024). — Режим доступа: для авториз. пользователей.

7.2 Дополнительная литература

1. Ванюшина, А. В. Основы информационной безопасности : учебно-методическое пособие / А. В. Ванюшина, С. Ю. Рыбаков. — Москва :МТУСИ, 2022. — 22 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/333701 (дата обращения: 28.02.2024). — Режим доступа: для авториз. пользователей.

2. Зенков, А. В. Информационная безопасность и защита информации : учебное пособие для вузов / А. В. Зенков. — Москва : Издательство Юрайт, 2021. — 104 с. — (Высшее образование). — ISBN 978-5-534-14590-8. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/477968 (дата обращения: 12.04.2024).

3. Николаев, Н. С., Управление информационной безопасностью : учебник / Н. С. Николаев. — Москва : КноРус, 2021. — 188 с. — ISBN 978-5-406-07325-4. — URL: https://book.ru/book/939841 (дата обращения: 26.02.2024). — Текст : электронный.

7.3 Ресурсы информационно-телекоммуникационной сети "Интернет", включая профессиональные базы данных и информационно-справочные системы (при необходимости):

1. Образовательная платформа "ЮРАЙТ"
2. Электронно-библиотечная система "BOOK.ru"

3. Электронно-библиотечная система "ЛАНЬ"

4. Open Academic Journals Index (OAJI). Профессиональная база данных - Режим доступа: http://oaji.net/

5. Президентская библиотека им. Б.Н.Ельцина (база данных различных профессиональных областей) - Режим доступа: https://www.prlib.ru/

6. Информационно-справочная система "Консультант Плюс" - Режим доступа: http://www.consultant.ru/

8 Материально-техническое обеспечение дисциплины (модуля) и перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине (модулю), включая перечень программного обеспечения

Основное оборудование:

· Компьютеры
· Проектор

Программное обеспечение:

· Microsoft Office 2003 Suites Russian
· Microsoft Windows XP Professional

МИНОБРНАУКИ РОССИИ

ВЛАДИВОСТОКСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

КАФЕДРА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Фонд оценочных средств
для проведения текущего контроля
и промежуточной аттестации по дисциплине (модулю)

УПРАВЛЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ

Специальность и специализация

10.05.03 Информационная безопасность автоматизированных систем. Безопасность открытых информационных систем

Год набора на ОПОП
2022

Форма обучения
очная

Владивосток 2023

1 Перечень формируемых компетенций

Название ОПОП ВО, сокращенное	Код и формулировка компетенции	Код и формулировка индикатора достижения компетенции
10.05.03 «Информационная безопасность автоматизированных систем» (ИБ)		

Компетенция считается сформированной на данном этапе в случае, если полученные результаты обучения по дисциплине оценены положительно (диапазон критериев оценивания результатов обучения «зачтено», «удовлетворительно», «хорошо», «отлично»). В случае отсутствия положительной оценки компетенция на данном этапе считается несформированной.

2 Показатели оценивания планируемых результатов обучения

Таблица заполняется в соответствии с разделом 1 Рабочей программы дисциплины (модуля).

3 Перечень оценочных средств

Таблица 3 – Перечень оценочных средств по дисциплине (модулю)

Контролируемые планируемые результаты обучения		Контролируемые темы дисциплины	Наименование оценочного средства и представление его в ФОС	
			Текущий контроль	Промежуточная аттестация
Очная форма обучения				
РД1	Знание : принципы формирования политики информационной безопасности в информационных системах	1.1. Введение в дисциплину	Практическая работа	Список вопросов
			Тест	Список вопросов
		1.2. Система управления информационной безопасностью автоматизированных систем.	Практическая работа	Список вопросов
			Тест	Список вопросов
		1.3. Аудит информационной безопасности	Практическая работа	Список вопросов
			Тест	Список вопросов
		1.4. Средства поддержки процессов управления информационной безопасностью автоматизированных систем	Практическая работа	Список вопросов
			Тест	Список вопросов
РД2	Умение : разрабатывать политику информационной безопасности автом	1.1. Введение в дисциплину	Практическая работа	Список вопросов

	атизированной системы	1.2. Система управления информационной безопасностью автоматизированных систем.	Практическая работа	Список вопросов
		1.3. Аудит информационной безопасности	Практическая работа	Список вопросов
		1.4. Средства поддержки процессов управления информационной безопасностью автоматизированных систем	Практическая работа	Список вопросов

4 Описание процедуры оценивания

Качество сформированности компетенций на данном этапе оценивается по результатам текущих и промежуточных аттестаций при помощи количественной оценки, выраженной в баллах. Максимальная сумма баллов по дисциплине (модулю) равна 100 баллам.

Вид учебной деятельности	Оценочное средство			
	Тест	Практическая работа	Экзамен	Итого
Лекционное занятие	40			40
Практическое занятие		40		40
Промежуточная аттестация			20	20
Итого	40	40	20	100

Сумма баллов, набранных студентом по всем видам учебной деятельности в рамках дисциплины, переводится в оценку в соответствии с таблицей.

Сумма баллов по дисциплине	Оценка по промежуточной аттестации	Характеристика качества сформированности компетенции
от 91 до 100	«зачтено» / «отлично»	Студент демонстрирует сформированность дисциплинарных компетенций, обнаруживает всестороннее, систематическое и глубокое знание учебного материала, усвоил основную литературу и знаком с дополнительной литературой, рекомендованной программой, умеет свободно выполнять практические задания, предусмотренные программой, свободно оперирует приобретенными знаниями, умениями, применяет их в ситуациях повышенной сложности.
от 76 до 90	«зачтено» / «хорошо»	Студент демонстрирует сформированность дисциплинарных компетенций: основные знания, умения освоены, но допускаются незначительные ошибки, нет очности, затруднения при аналитических операциях, переносе знаний и умений на новые, нестандартные ситуации.
от 61 до 75	«зачтено» / «удовлетворительно»	Студент демонстрирует сформированность дисциплинарных компетенций: в ходе контрольных мероприятий допускаются значительные ошибки, проявляется отсутствие отдельных знаний, умений, навыков по некоторым дисциплинарным компетенциям, студент испытывает значительные затруднения при оперировании знаниями и умениями при их переносе на новые ситуации.
от 41 до 60	«не зачтено» / «неудовлетворительно»	У студента не сформированы дисциплинарные компетенции, проявляется недостаточность знаний, умений, навыков.
от 0 до 40	«не зачтено» / «неудовлетворительно»	Дисциплинарные компетенции не сформированы. Проявляется полное или практически полное отсутствие знаний, умений, навыков.

5 Примерные оценочные средства

5.1 Примеры заданий для выполнения практических работ

Практическая работа 1. Анализ источников, каналов распространения и каналов утечки информации

Цель работы: формирование навыка работы с нормативными документами по исследуемому вопросу; анализ угроз информационной безопасности

Практическая работа 2. Проведение анализа информации на предмет целостности

Цель работы изучить понятие целостности информации, проанализировать риски информационной безопасности.

Раздел 3. Основы защиты информации

Практическая работа 3. Требования к безопасности информационных систем.

Цель работы: закрепление теоретических знаний по вопросам сертификации средств защиты информации по требованиям безопасности информации.

Практическая работа 4. Требования к безопасности информационных систем в России.

Цель работы: закрепление теоретических знаний в области правового обеспечения информационной безопасности.

Практическая работа 5. Определение классов защищенности средств вычислительной техники от несанкционированного доступа.

Цель работы: изучить и проанализировать руководящий документ "Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации".

Практическая работа 6. Анализ терминов и определений информационной безопасности

Цель работы проанализировать ГОСТ Р 53114-2008 Защита информации.

Обеспечение информационной безопасности в организации. Основные термины и определения.

Практическая работа 7. Оценка безопасности информации на объектах ее обработки

Цель работы ознакомиться с проблемами реализации политик безопасности в компьютерных системах.

Практическая работа 8. Классификация автоматизированных систем обработки информации по классу защиты информации

Цель работы закрепление знаний основного понятийного аппарата, применяемого в области защиты информации, формирование навыка работы с нормативными документами по исследуемому вопросу.

Краткие методические указания

На выполнение одной практической работы отводится не менее одного двухчасового занятия. После выполнения каждой работы студент должен представить отчет о ее выполнении, а также, по указаниям преподавателя, выполнить дополнительные практические задания

Шкала оценки

Оценка	Баллы	Описание
5	4-5	Оценка «отлично» выставляется, если студент выполнил работу, правильно применил методы нео бходимые для решения поставленных задач.
4	2-3	Оценка «хорошо» выставляется, если студент выполнил работу, правильно применил методы, но совершил логические ошибки.
3	1	Оценка «удовлетворительно» выставляется, если студент выполнил работу, но применил методы не все необходимые методы для решения поставленных задач.
2	0	Оценка «неудовлетворительно» выставляется в случае, если студент не выполнил работу и/или н еверно применил методы необходимые для решения поставленных задач

5.2 Примеры тестовых заданий

1. Что такое домен безопасности?

а) собрание участников безопасности, имеющих единый центр, использующий

единую базу, единую групповую и локальную политики, ограничение времени работы учётной записи и прочие параметры, значительно упрощающие работу системного администратора организации, если в ней эксплуатируется большое число компьютеров

b) виртуальная частная сеть с единым центром управления

c) локальная сеть, не имеющая выхода в сети связи общего пользования

d) сетевая операционная система

2. Какое из требований необязательно для операционных систем, сертифицированных по 5 классу РД СВТ?

a) Должны быть предусмотрены средства управления, ограничивающие распространение прав на доступ

b) ОС должна содержать механизм, претворяющий в жизнь дискреционные правила разграничения доступа

c) Контроль доступа должен быть применим к каждому объекту и каждому субъекту (индивиду или группе равноправных индивидов)

d) В ОС должен быть реализован диспетчер доступа, т.е. средство, осуществляющее перехват всех обращений субъектов к объектам, а также разграничение доступа в соответствии с заданным принципом разграничения доступа

3. Присутствуют ли в ОС семейства Windows механизмы, осуществляющие криптографические преобразования?

a) нет

b) присутствуют механизмы ЭЦП и хеширования

c) присутствуют механизмы обмена ключами

d) присутствуют механизмы для симметричного шифрования данных

4. Что такое PAM?

a) набор библиотек подключаемых модулей шифрования

b) набор открытых библиотек подключаемых модулей аутентификации

c) набор открытых библиотек подключаемых модулей резервного восстановления

d) набор открытых библиотек подключаемых модулей доверенной загрузки

5. Открытой распределенной информационной системой (open distributed information system) называется система:

a. располагающая службами, пользование которыми возможно при использовании стандартных синтаксиса и семантики

b. располагающая службами, пользование которыми возможно при использовании специальных синтаксиса и семантики

c. располагающая службами, пользование которыми возможно при использовании стандартных синтаксиса и семантики

d. не располагающая службами, пользование которыми возможно при использовании стандартных синтаксиса и семантики

6. Угроза это:

a) совокупность сообщений, направленных на запугивание

b) совокупность условий и факторов, определяющих потенциальную или реально существующую опасность возникновения инцидента, который может привести к нанесению ущерба изделию ИТ или его владельцу.

c) совокупность сообщений, направленных на причинение вреда

d) любое действие, направленное на причинение ущерба

7. Классами защищённости автоматизированных систем от несанкционированного доступа являются:

a) 1Е

b) 2А

c) 2В

d) 3Б

8. Определите класс автоматизированной системы по следующим классификационным признакам: АС, в которых работает один пользователь, допущенный ко

всей информации АС, размещенной на носителях одного уровня конфиденциальности, обрабатывается “Коммерческая тайна”.

a) 2Б

b) 1Г

c) 1Д

d) 3Б

9. Определите класс автоматизированной системы по следующим классификационным признакам: многопользовательские АС, в которых одновременно обрабатывается и (или) хранится информация разных уровней конфиденциальности. И все пользователи имеют равные права доступа ко всей информации АС, обрабатывается “Служебная тайна” и общедоступная информация:

a) 2Б

b) 2А

c) 1Г

d) 1Д

10. Методы и средства защиты информации бывают:

a) Технические (аппаратные)

b) Программные

c) Прикладные

d) Организационные

11. Информация по категории доступа классифицируется как:

a) Конфиденциальная

b) Общедоступная

c) Особо конфиденциальная

d) Ограниченного доступа

12. Уязвимость это:

a) Совокупность действий, направленная на преодоление системы защиты

b) Злонамеренное внедрение специального ПО

c) Слабость в средствах защиты, которую можно использовать для нарушения системы или содержащейся в ней информации.

d) Результат действия вируса

13. Прерывание это:

a) временное прекращение процесса

b) остановка процесса

c) временное прекращение процесса, вызванное событием, внешним по отношению к этому процессу, и совершенное таким образом, что процесс может быть продолжен

d) событие, при котором меняется нормальная последовательность команд, выполняемых процессором

14. Что такое тупиковая ситуация для процесса?

a) невозможность выделения процессу требуемого ресурса

b) ситуация, когда процесс ожидает некоторого события, которое никогда не произойдет

c) прерывание процесса операционной системой

d) критическая системная ошибка во время выполнения процесса

15. В каком порядке задаются права доступа в ОС Linux?

a) группа-владелец- остальные

b) владелец-группа-остальные

c) остальные-владелец-группа

d) остальные-группа-владелец

16. Что такое ACL?

a) средство для хранения паролей

b) сценарий входа в систему

c) список управления доступом

d) инструмент мандатного управления доступом в ОС

17. Что из перечисленного не содержится в маркере доступа пользователя?

a) идентификатор пользователя

b) привилегии пользователя

c) идентификатор сеанса работы пользователя, к которому относится маркер доступа

d) уровень доступа пользователя в системе

18. Какова должна быть минимальная длина пароля в случае смены ежеквартально?

a) 13 символов

b) 12 символов

c) 8 символов

d) 6 символов

19. Что из перечисленного не является требование к подсистеме регистрации и учета:

a) использование идентификационного и аутентификационного механизма

b) запрос на доступ к защищаемому ресурсу (открытие файла, запуск программы и т.д.)

c) обеспечение доверенной загрузки ОС

d) действия по изменению ПРД

Краткие методические указания

Тестовые задания состоят из вопроса и нескольких вариантов ответа. Решение представляет собой указание номера вопроса и букву, которой обозначен правильный, по мнению студента, вариант ответа. В течение семестра проводится 4 теста по 4 темам на лекционных занятиях, в каждом тесте от 5 до 10 вопросов.

Шкала оценки

Оценка	Баллы*	Описание
5	8-10	Студент ответил безошибочно
4	5-7	Студент совершил 1 ошибку в ответах на тест
3	3-4	Студент совершил 2 ошибки в ответах на тест
2	0-2	Студент совершил 3 и более ошибок в ответах на тест

5.3 Экзаменационные вопросы

1. Основные понятия информационной безопасности. Защита информации. Управление информационной безопасностью. Модель безопасности. Прямое воздействие.

2. Понятие защищенной системы.

3. Как изменялся подход к задаче защите информации? Три этапа развития защиты информации.

4. Теория защиты информации. Основные составные части теории защиты информации.

5. Современная постановка задачи защиты информации.

6. Угроза, атака, источники угроз. Что такое окно опасности. Критерии классификации угроз.

7. Наиболее распространенные угрозы доступности.

8. Программные угрозы доступности.

9. Основные угрозы целостности. Статическая и динамическая целостность.

10. Основные угрозы конфиденциальности.

11. Таксономия угроз безопасности. Что такое уязвимость защиты? Таксономия угроз безопасности. Ошибки в системах защиты.

12. Что такое антивирусная программа? Вирусная сигнатура. Виды антивирусных программ.

13. Основополагающие принципы решения задачи закрытия каналов несанкционированного доступа.

14. Понятие политики и модели безопасности. Структура монитора обращений.

15. Методы идентификации и аутентификации. Способы аутентификации –

пользователь «знает», пользователь «имеет» и пользователь «есть».

16. Базовые представления моделей безопасности. Субъекты, объекты и доступ.

17. Произвольное управление доступом субъектов к объектам и контроль за распространением прав доступа. Модель Харрисона-Руззо-Ульмана..

18. Мандатная модель Белла-Лападулы. Свойство простой безопасности. Свойства ограничения. Свойство самостоятельной защиты. Правила перехода.

19. Какая главная задача стандартов информационной безопасности? «Оранжевая книга» США. Базовые требования безопасности. Четыре группы критериев безопасности.

20. Европейские критерии безопасности информационных технологий. Адекватность средств защиты. Уровни безопасности системы.

21. Основные руководящие документы Гостехкомиссии по вопросам защиты от несанкционированного доступа к информации. Классы защищенности.

22. ГОСТ Р ИСО МЭК 15048-2002 «Общие критерии оценки безопасности информационных технологий». Профиль защиты. функции безопасности. Предложения безопасности.

23. Основные функции организационно-правовой базы защиты информации. Виды информационных ресурсов. Какую информацию относят к защищаемой?

24. Признаки защищаемой информации. Владельцы защищаемой информации. Понятие «государственная тайна».

25. Криптографические механизмы и примитивы. Базовые методы преобразования информации, используемые в криптографии. Основные группы методов защитных преобразований. Методы перестановки, подстановки, аддитивные и комбинированные.

26. Криптография с симметричными ключами. Алгоритм DES, ГОСТ 28147-80, IDEA. Преимущества и недостатки криптографии с симметричными ключами.

27. Ассиметричные алгоритмы шифрования. Криптосистема с открытым ключом RSA. ХЭШ- функция. Понятие односторонней функции. Коллизия хэш-функции.

28. Иерархический метод разработки защищенных систем. Понятие доверенной вычислительной среды (trusted computing base - TCB).

Краткие методические указания

Для подготовки к экзамену студенту необходимо изучить лекционный материал, а так же материал представленный в дополнительных источниках

Шкала оценки

Оценка	Баллы	Описание
5	14-20	Оценка «отлично» выставляется студенту, если он глубоко и прочно усвоил программный ма териал исчерпывающе, последовательно, четко и логически стройно его излагает, умеет тесно увязывать теорию с практикой.
4	8-12	Оценка «хорошо» выставляется студенту, если он твердо знает материал, грамотно и по суще ству излагает его, не допуская существенных неточностей в ответе на вопрос, правильно при меняет теоретические положения при решении практических вопросов и задач.
3	2-6	Оценка «удовлетворительно» выставляется студенту, если он имеет знания только основного материала, но не усвоил его деталей, допускает неточности, недостаточно правильные форму лировки.
2	0-2	Оценка «неудовлетворительно» выставляется студенту, который не знает значительной част и программного материала, допускает существенные ошибки.