АВТОНОМНАЯ НЕКОММЕРЧЕСКАЯ ОРГАНИЗАЦИЯ
ВЫСШЕГО ОБРАЗОВАНИЯ
«СЕВЕРО-КАВКАЗСКИЙ СОЦИАЛЬНЫЙ ИНСТИТУТ»

Утверждаю
Декан факультета ФИСТ
_____ Ж.В. Игнатенко
«21» 10 2020 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Методы и средства защиты информации организации

Направление подготовки 09.03.02 Информационные системы и технологии

Направленность (профиль) программы Информационные технологии в управлении предприятием

Квалификация выпускника бакалавр

Форма обучения очная, заочная

год начала подготовки – 2019

Разработана
ст. преподаватель, канд. пед. наук,
_____ Г.А. Бондарева

Согласована
зав. выпускающей кафедры
_____ А.Ю. Орлова

Рекомендована
на заседании кафедры
от «28» 10 2020 г.
протокол № 2
Зав. кафедрой
_____ А.Ю. Орлова

Одобрена
на заседании учебно-методической
комиссии факультета
от «28» 10 2020 г.
протокол № 2
Председатель УМК _____ Ж.В. Игнатенко

Ставрополь, 2020г.

Содержание

1. ЦЕЛИ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Целями освоения дисциплины «Методы и средства защиты информации организации» являются: формирование у студентов теоретических знаний об информационных угрозах и методах защиты информации, получения первичных навыков действий по обеспечению информационной безопасности информации в экономических и управленческих компьютерных системах организаций.

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОПОП

Дисциплина (Б.1.В.14) «Методы и средства защиты информации организации» входит в часть, формируемую участниками образовательных отношений, – обязательные дисциплины Блока 1 «Дисциплины (модули)» и находится в логической и содержательно-методической связи с другими дисциплинами.

Предшествующие дисциплины (курсы, модули, практики)	Последующие дисциплины (курсы, модули, практики)
Информационная безопасность Методы принятия решений в управлении Технологии программирования Информационные системы и технологии.	Проектирование информационных систем организаций Управление информационными рисками Администрирование компьютерных сетей. Технологическая (проектно-технологическая) практика.

Требования к «входным» знаниям, умениям и навыкам обучающегося, необходимым при освоении данной дисциплины и приобретенным в результате освоения предшествующих дисциплин:

Знать: теоретические основы эффективной работы с современными информационными системами; методы построения структур информационных систем, базовые алгоритмы их функционирования.

Уметь: осуществлять самостоятельный поиск необходимой информации по научно-информационным системам; выбирать программно-технические средства для достижения поставленных целей при работе с информацией.

Владеть: навыками работы офисным прикладным программным обеспечением.

3. ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОБУЧЕНИЯ ПО ДИСЦИПЛИНЕ

Формируемые компетенции (код компетенции, наименование)	Планируемые результаты обучения
ПК-3 Способен анализировать требования к программному обеспечению, разрабатывать технические спецификации на программные компоненты и их взаимодействие	**Знать** общие принципы организации защиты конфиденциальной информации, применяемые при разработке систем защиты информации на предприятии; основы нормативных документов об ответственности за разглашение конфиденциальной информации.
	Уметь использовать существующие типовые решения и шаблоны проектирования программного обеспечения, применять методы и средства проектирования программного обеспечения, структур данных, баз данных, программных интерфейсов; классифицировать угрозу конфиденциальной информации по ее проявлению на предприятии; применять на практике технические, программно-аппаратные и программные средства защиты информации
	Владеть навыками проведения анализа исполнения требований к ПО, выработки вариантов реализации требований к ПО, оценки и обоснования рекомендуемых решений по ПО4 содержанием уровней защиты информации в составе комплексной системы защиты информации на

	предприятии; навыками работы на рабочих станциях АИС предприятия по обеспечению возможных вариантов доступа пользователей к конфиденциальной информации.
ПК-5 Способен разрабатывать модели бизнес-процессов и адаптировать бизнес-процессы к возможностям ИС организации	**Знать** перечень организационных и организационно-технический мероприятий, выполняемых на предприятии по защите конфиденциальной информации; основные источники случайных (непреднамеренных) угроз на предприятии и их классификацию; умышленные угрозы воздействия на конфиденциальную информацию и их классификацию.
	Уметь применять средства построения модели бизнес-процесса, применять средства моделирование бизнес-процессов; классифицировать угрозу конфиденциальной информации по ее проявлению на предприятии.
	Владеть навыками разработки модели бизнес-процессов и предлагаемых изменений, согласования с заказчиком модели бизнес-процессов, моделирования бизнес – процессов.
ПК-8 Способен обеспечивать управление доступом к программно- аппаратным средствам информационных служб инфокоммуникационной системы (ИКС)	**Знать** инструкции по установке и эксплуатации компьютерного, периферийного и абонентского оборудования, типовые ошибки, возникающие при работе инфокоммуникационной системы, признаки их проявления при работе и методы устранения, структура модели взаимодействия открытых систем (OSI) ISO;
	Уметь идентифицировать права пользователей по доступу к программно- аппаратным средствам информационных служб инфокоммуникационной системы и ее составляющих, применять специальные программно-аппаратные средства контроля доступа пользователей к программно-аппаратным средствам информационных служб инфокоммуникационной системы, применять утилиты операционных систем по управлению и контролю доступа к компонентам ИКС.
	Владеть навыками управления, изменения и контроля соблюдения прав доступа пользователей к программно-аппаратным средствам информационных служб инфокоммуникационной системы, определения приемлемых для пользователей параметров работы сети в условиях нормальной обычной работы , использования современные методы контроля производительности инфокоммуникационных систем.
ПК-11 Способен разрабатывать политику и регламенты информационной безопасности, проводить аудит системы безопасности данных с подготовкой отчетов о состоянии и эффективности системы безопасности	**Знать** стандарты информационной безопасности, уязвимости инфокоммуникационных систем, классы информационной защищённости систем, угрозы безопасности и способы их предотвращения, структуру и содержание политики информационной безопасности, методы и средства обеспечения безопасности данных при работе с БД и при передаче в телекоммуникациях, характеристики систем и средств обеспечения безопасности, влияющие на производительность систем, средства и инструменты восстановления безопасности,

	законодательство Российской Федерации в области обеспечения информационной безопасности в информационных системах, методику разработки регламента аудита систем безопасности.
	Уметь выявлять угрозы информационной безопасности, факты нарушения регламентов обеспечения безопасности, разрабатывать мероприятия по обеспечению безопасности на уровне БД, настраивать программно-аппаратные средства защиты данных и процедуры выявления попыток несанкционированного доступа к данным, оценивать степень нагрузки различных инструментов обеспечения безопасности на производительность, планировать и осуществлять меры по устранению последствий нарушения регламентов обеспечения безопасности, настраивать параметры инструментов системы безопасности в соответствии с установленными критериями, разрабатывать комплекс организационно-технических мероприятий по обеспечению безопасности данных, оценивать степень защиты данных от угроз безопасности.
	Владеть навыками выявления действий, нарушающих регламент обеспечения безопасности, выбор наиболее эффективных путей снижения нагрузки при обеспечении заданного уровня безопасности данных, анализа возможных угроз для безопасности данных, выбора средств обеспечения информационной безопасности, настройки параметры инструментов системы безопасности в соответствии с установленными критериями, определения показателей и критериев эффективности системы безопасности, оценки уровня и состояния системы безопасности данных, определения возможностей оптимизации работы систем безопасности с целью уменьшения нагрузки на работу системы, выбора наиболее эффективных путей снижения нагрузки при обеспечении заданного уровня безопасности данных, выбора критериев оценки результатов аудита данных, разработки методик аудита системы безопасности данных, аудита системы безопасности и оценка ее эффективности.

4. ОБЪЕМ ДИСЦИПЛИНЫ И ВИДЫ УЧЕБНОЙ РАБОТЫ

Общий объем дисциплины составляет 4 зачетных единиц,144 академических часа.

Вид учебной работы	Всего часов		Триместр	
			8	8
	ОФО	ЗФО	ОФО	ЗФО
Контактная работа (всего)	**42,5**	**12,5**	**42,5**	**12,5**
в том числе:				
1) занятия лекционного типа (ЛК)	**20**	**4**	**20**	**4**
из них				
-лекций	20	4	20	4
2) занятия семинарского типа (ПЗ)	**20**	**8**	**20**	**8**
-семинары (С)				
-практические занятия (ПР)				
-лабораторные работы (ЛР)	20	8	20	8

3) групповые консультации	**2**		**2**	
4) индивидуальная работа				
5) промежуточная аттестация	**0,5**	**0,5**	**0,5**	**0,5**
Самостоятельная работа (всего) (СР)	**101,5**	**131,5**	**101,5**	**131,5**
в том числе:				
Курсовой проект (работа)				
Расчетно-графические работы				
Контрольная работа				
Реферат	10	10	10	10
Самоподготовка (самостоятельное изучение разделов, лекционного материала и материала учебников и учебных пособий, подготовка к лабораторным и практическим занятиям, контролю и т.д.)	65	113	65	113
Вид промежуточной аттестации (экзамен/экзамен)	26,5	8,5	26,5	8,5
Общий объем, час	**144**	**144**	**144**	**144**

5. СОДЕРЖАНИЕ И СТРУКТУРА ДИСЦИПЛИНЫ

5.1. Содержание дисциплины

№ раздела (темы)	Наименование раздела (темы)	Содержание раздела (темы)
1	Вводная лекция. Цели, задачи дисциплины. Основные понятия компьютерной безопасности	Цели, задачи дисциплины. Основные концептуальные положения системы защиты информации. Угрозы конфиденциальной информации Действия, приводящие к неправомерному овладению конфиденциальной информацией Коммерческая тайна. Критерии безопасности компьютерных систем. Классы безопасности компьютерных систем, категории требований безопасности компьютерных систем.
1.	Организационная и инженерно-техническая защита информации	Организационная защита. Инженерно-техническая защита. Физические средства защиты.
2.	Программные средства защиты	Основные направления использования программной защиты информации. Понятие вредоносных программ, их классификация, способы распространения вредоносных программ. Программно-технические методы обнаружения вирусов. Защита информации от несанкционированного доступа. Защита от копирования. Особенности защиты информации в персональных компьютерах.
3.	Криптографические методы защиты информации	Наука криптография. Основные направления использования некриптографической и криптографической защиты информации. Общие

		сведения о работе современных симметричных криптосистем (рассеивание, перемешивание, петля Фейстеля), управление ключами, электронная цифровая подпись. Общая технология шифрования. Технология шифрования речи.
4.	Алгоритмы цифровой подписи	Алгоритм цифровой подписи RSA. Алгоритм цифровой подписи Эль Гамаля. Отечественный стандарт цифровой подписи.
6.	Лицензирование и сертификация в области защиты информации	Понятия лицензирования и сертификации в области защиты информации, нормативная правовая база системы сертификации средств защиты информации, порядок проведения лицензирования.
7.	Многоуровневая защита корпоративных сетей	Многоуровневая защита корпоративных сетей. Защита информации в сетях. Требования к системам защиты информации.
8.	Особенности функционирования межсетевых экранов	Фильтрующие маршрутизаторы. Шлюзы прикладного уровня. Межсетевой экран – фильтрующий маршрутизатор. Межсетевой экран на основе двухпортового шлюза. Межсетевой экран – экранированная подсеть. Полностью контролируемые компьютерные системы. Частично контролируемые компьютерные системы.

5.2. Структура дисциплины

№ раздела (темы)	Наименование раздела (темы)	Всего *	Количество часов							
			Л		ЛР		К		СР	
			ОФО	ЗФО	ОФО	ЗФО	ОФО	ЗФО	ОФО	ЗФО
1	Вводная лекция. Цели, задачи дисциплины. Основные понятия компьютерной безопасности	10/14	2	-	-	-	-	-	8	14
2	Организационная и инженерно-техническая защита информации	12/16	2	1	2	1	-	-	8	14
3	Программные средства защиты	14/16	4	1	2	1	-	-	8	14
4	Криптографические методы защиты информации	18/16	4	1	6	1	-	-	8	14
5	Алгоритмы цифровой подписи	14/17	2	1	4	2	-	-	8	14
6	Лицензирование и сертификация в области защиты информации	10/14	2	-	-	-	-	-	8	14

7	Многоуровневая защита корпоративных сетей	14/16	2	-	4	2	-	-	8	14
8	Особенности функционирования межсетевых экранов	13/16	2	-	2	1	-	-	9	15
	Реферат	10/10							10	10
	Экзамен/Экзамен	29/9	-	-			2	-	27	9
	Общий объем	**144/144**	**20**	**4**	**20**	**8**	**2**	**-**	**102**	**132**

5.3. Занятия семинарского типа

№ п/п	№ раздела (темы)	Вид занятия	Наименование	Количество часов	
				ОФО	ЗФО
1	2	ЛР	Защита программного обеспечения от несанкционированного использования и копирования	2	1
2	2	ЛР	Профилактика проникновения вредоносного программного обеспечения	2	1
3	4	ЛР	Криптоанализ шифра простой замены	2	1
4	4	ЛР	Шифры перестановки на примере шифра Кардано	2	1
5	4	ЛР	Шифры многобуквенной замены на примере шифра Хилла	2	-
6	5	ЛР	Аутентификация документов на основе электронно-цифровой подписи	4	1
7	7	ЛР	Исследование элементов управления сетью в ОС Windows 7. Общий доступ к ресурсам.	2	1
8	7	ЛР	Обеспечение безопасности локальной сети	2	1
9	8	ЛР	Исследование возможностей межсетевого экрана	2	1

5.4. Курсовой проект (курсовая работа, расчетно-графическая работа, реферат, контрольная работа)

Типовые темы рефератов

1. Задачи, методы и средства защиты информации.
2. Источники утраты конфиденциальности и искажения информации.
3. Понятие конфиденциальности. Критерии выделения информации ограниченного распространения.
4. Легальные способы получения полезной информации.
5. Понятие информационного права. Предмет, методы и принципы информационного права.
6. Методы борьбы с фишинговыми атаками.
7. Законодательство о персональных данных.
8. Защита авторских прав.
9. Назначение, функции и типы систем видеозащиты.
10. Как подписывать с помощью ЭЦП электронные документы различных форматов.
11. Обзор угроз и технологий защиты Wi-Fi-сетей.
12. Проблемы внедрения дискового шифрования.

13. Борьба со спамом: основные подходы, классификация, примеры, прогнозы на будущее.
14. Особенности процессов аутентификации в корпоративной среде.
15. Квантовая криптография.

5.5. Самостоятельная работа

№ темы	Виды самостоятельной работы	Количество часов	
		ОФО	ЗФО
1	Изучение источников информации по теме. Подготовка к лабораторной работе	8	14
2	Изучение источников информации по теме. Подготовка к лабораторной работе	8	14
3	Изучение источников информации по теме. Подготовка к лабораторной работе	8	14
4	Изучение источников информации по теме. Подготовка к лабораторной работе	8	14
5	Изучение источников информации по теме. Подготовка к лабораторной работе	8	14
6	Изучение источников информации по теме. Подготовка к лабораторной работе	8	14
7	Изучение источников информации по теме. Подготовка к лабораторной работе	8	14
8	Изучение источников информации по теме. Подготовка к лабораторной работе	9	15
	Реферат	10	10
	Подготовка к аттестации	26,5	8,5

6. ОБРАЗОВАТЕЛЬНЫЕ ТЕХНОЛОГИИ

Информационные технологии, используемые при осуществлении образовательного процесса по дисциплине:

– сбор, хранение, систематизация, обработка и представление учебной и научной информации;

– обработка различного рода информации с применением современных информационных технологий;

– самостоятельный поиск дополнительного учебного и научного материала, с использованием поисковых систем и сайтов сети Интернет, электронных энциклопедий и баз данных;

– использование электронной почты для рассылки и асинхронного общения, чата преподавателей и обучающихся, переписки и обсуждения возникших учебных проблем для синхронного взаимодействия

дистанционные образовательные технологии (при необходимости).

Интерактивные и активные образовательные технологии

№ раздела (темы)	Вид занятия (Л, ПЗ, С, ЛР)	Используемые интерактивные образовательные технологии	Количество часов	
			ОФО	ЗФО
2	Л	Лекция-дискуссия	2	1
3	ЛР	Работа малыми группами	2	1
4	Л	Проблемная лекция.	2	1

5	ЛР	Работа малыми группами	2	1

Практическая подготовка обучающихся не предусмотрена

7. ФОНД ОЦЕНОЧНЫХ СРЕДСТВ (ОЦЕНОЧНЫЕ МАТЕРИАЛЫ) ДЛЯ ТЕКУЩЕГО КОНТРОЛЯ УСПЕВАЕМОСТИ, ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ

Фонд оценочных средств по дисциплине приводится в приложении и входит в рабочую программу дисциплины.

8. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

8.1. Основная литература

1. Внуков, А. А. Защита информации : учебное пособие для вузов / А. А. Внуков. — 3-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2020. — 161 с. — (Высшее образование). — ISBN 978-5-534-07248-8. — Текст : электронный // ЭБС Юрайт [сайт]. — URL: https://urait.ru/bcode/422772

2. Галатенко, В. А. Основы информационной безопасности : учебное пособие / В. А. Галатенко. — 3-е изд. — Москва : Интернет-Университет Информационных Технологий (ИНТУИТ), Ай Пи Ар Медиа, 2020. — 266 с. — ISBN 978-5-4497-0675-1. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. — URL: http://www.iprbookshop.ru/97562.html

8.2. Дополнительная литература

1. Казарин, О. В. Программно-аппаратные средства защиты информации. Защита программного обеспечения : учебник и практикум для вузов / О. В. Казарин, А. С. Забабурин. — Москва : Издательство Юрайт, 2020. — 312 с. — (Высшее образование). — ISBN 978-5-9916-9043-0. — Текст : электронный // ЭБС Юрайт [сайт]. — URL: https://urait.ru/bcode/452368

2. Запечников, С. В. Криптографические методы защиты информации : учебник для вузов / С. В. Запечников, О. В. Казарин, А. А. Тарасов. — Москва : Издательство Юрайт, 2020. — 309 с. — (Высшее образование). — ISBN 978-5-534-02574-3. — Текст : электронный // ЭБС Юрайт [сайт]. — URL: https://urait.ru/bcode/450538

8.3. Программное обеспечение

1. Microsoft Windows
2. Microsoft Office.

8.4. Профессиональные базы данных

1. База данных IT специалиста» [Электронный ресурс] – Режим доступа: http://info-comp.ru/
2. База данных бизнес-идей [Электронный ресурс] – Режим доступа: http://coolbusinessideas.info/
3. База данных «Стратегическое управление и планирование» [Электронный ресурс] – Режим доступа: http://www.stplan.ru/

8.5. Информационные справочные системы

1. Информационно-справочная система для программистов [Электронный ресурс] – Режим доступа :http://life-prog.ru
2. Справочно-правовая система «КонсультантПлюс» [Электронный ресурс] – Режим доступа http://www.consultant.ru/

8.6. Интернет-ресурсы

1. Электронная библиотечная система «IPRbooks» [Электронный ресурс] – Режим доступа :http://www.iprbookshop.ru/

2. Бесплатная электронная библиотека онлайн «Единое окно доступа к образовательным ресурсам» [Электронный ресурс] – Режим доступа: http://www.window.edu.ru

3. Национальный открытый университет Интуит – интернет университет информационных технологий [Электронный ресурс] – Режим доступа: http://www.intuit.ru/

4. Электронно-библиотечная система «ЮРАЙТ» [Электронный ресурс] – Режим доступа: https://biblio-online.ru/

5. Электронная библиотека «Все учебники» [Электронный ресурс] – Режим доступа http://www.vse-ychebniki.ru/

6. Русская виртуальная библиотека [Электронный ресурс] – Режим доступа: http://www.rvb.ru/

8.7. Методические указания по освоению дисциплины

Методические указания при работе над конспектом во время проведения лекции

В ходе лекционных занятий необходимо вести конспектирование учебного материала. Общие и утвердившиеся в практике правила и приемы конспектирования лекций:

Конспектирование лекций ведется в специально отведенной для этого тетради, каждый лист которой должен иметь поля, на которых делаются пометки из рекомендованной литературы, дополняющие материал прослушанной лекции, а также подчеркивающие особую важность тех или иных теоретических положений.

Необходимо записывать тему и план лекций, рекомендуемую литературу к теме. Записи разделов лекции должны иметь заголовки, подзаголовки, красные строки. Для выделения разделов, выводов, определений, основных идей можно использовать цветные карандаши и фломастеры.

Названные в лекции ссылки на первоисточники надо пометить на полях, чтобы при самостоятельной работе найти и вписать их.

В конспекте дословно записываются определения понятий, категорий и законов. Остальное должно быть записано своими словами.

Каждому обучающемуся необходимо выработать и использовать допустимые сокращения наиболее распространенных терминов и понятий.

В конспект следует заносить всё, что преподаватель пишет на доске, а также рекомендуемые схемы, таблицы, диаграммы и т.д.

Методические указания по подготовке к лабораторным работам

Целью практических занятий является углубление и закрепление теоретических знаний, полученных обучающимися на лекциях и в процессе самостоятельного изучения учебного материала, а, следовательно, формирование у них определенных умений и навыков.

В ходе подготовки к практическим и лабораторным работам необходимо прочитать конспект лекции, изучить основную литературу, ознакомиться с дополнительной литературой, выполнить выданные преподавателем задания. При этом учесть рекомендации преподавателя и требования программы. Дорабатывать свой конспект лекции, делая в нем соответствующие записи из литературы. Желательно при подготовке к практическим и лабораторным работам по дисциплине одновременно использовать несколько источников, раскрывающих заданные вопросы.

Методические указания по организации самостоятельной работы

Самостоятельная работа приводит обучающегося к получению нового знания, упорядочению и углублению имеющихся знаний, формированию у него профессиональных навыков и умений.

Самостоятельная работа выполняет ряд функций:

- развивающую;

- информационно-обучающую;
- ориентирующую и стимулирующую;
- воспитывающую;
- исследовательскую.

Виды самостоятельной работы, выполняемые в рамках курса:

1. Проработка и повторение лекционного материала
2. Подготовка к практическим занятиям
3. Подготовка к лабораторным занятиям
4. Реферат
5. Подготовка к аттестации

Обучающимся рекомендуется с самого начала освоения курса работать с литературой и предлагаемыми заданиями в форме подготовки к очередному аудиторному занятию. При этом актуализируются имеющиеся знания, а также создается база для усвоения нового материала, возникают вопросы, ответы на которые обучающийся получает в аудитории.

Можно отметить, что некоторые задания для самостоятельной работы по курсу имеют определенную специфику. При освоении курса обучающийся может пользоваться библиотекой вуза, которая в полной мере обеспечена соответствующей литературой. Значительную помощь в подготовке к очередному занятию может оказать имеющийся в учебно-методическом комплексе краткий конспект лекций.

Методические указания по работе с литературой

Всю литературу можно разделить на учебники и учебные пособия, оригинальные научные монографические источники, научные публикации в периодической печати. Из них можно выделить литературу основную (рекомендуемую), дополнительную и литературу для углубленного изучения дисциплины.

Изучение дисциплины следует начинать с учебника, поскольку учебник – это книга, в которой изложены основы научных знаний по определенному предмету в соответствии с целями и задачами обучения, установленными программой.

При работе с литературой следует учитывать, что имеются различные виды чтения, и каждый из них используется на определенных этапах освоения материала.

Предварительное чтение направлено на выявление в тексте незнакомых терминов и поиск их значения в справочной литературе. В частности, при чтении указанной литературы необходимо подробнейшим образом анализировать понятия.

Сквозное чтение предполагает прочтение материала от начала до конца. Сквозное чтение литературы из приведенного списка дает возможность обучающемуся сформировать свод основных понятий из изучаемой области и свободно владеть ими.

Выборочное – наоборот, имеет целью поиск и отбор материала. В рамках данного курса выборочное чтение, как способ освоения содержания курса, должно использоваться при подготовке к лабораторным практикумам по соответствующим разделам.

Аналитическое чтение – это критический разбор текста с последующим его конспектированием. Освоение указанных понятий будет наиболее эффективным в том случае, если при чтении текстов обучающийся будет задавать к этим текстам вопросы. Часть из этих вопросов сформулирована в приведенном в ФОС перечне вопросов для собеседования. Перечень этих вопросов ограничен, поэтому важно не только содержание вопросов, но сам принцип освоения литературы с помощью вопросов к текстам.

Целью изучающего чтения является глубокое и всестороннее понимание учебной информации.

Есть несколько приемов изучающего чтения:

1. Чтение по алгоритму предполагает разбиение информации на блоки: название; автор; источник; основная идея текста; фактический материал; анализ текста путем сопоставления имеющихся точек зрения по рассматриваемым вопросам; новизна.

2. Прием постановки вопросов к тексту имеет следующий алгоритм:

- медленно прочитать текст, стараясь понять смысл изложенного;
- выделить ключевые слова в тексте;
- постараться понять основные идеи, подтекст и общий замысел автора.

3. Прием тезирования заключается в формулировании тезисов в виде положений, утверждений, выводов.

К этому можно добавить и иные приемы: прием реферирования, прием комментирования.

Важной составляющей любого солидного научного издания является список литературы, на которую ссылается автор. При возникновении интереса к какой-то обсуждаемой в тексте проблеме всегда есть возможность обратиться к списку относящейся к ней литературы. В этом случае вся проблема как бы разбивается на составляющие части, каждая из которых может изучаться отдельно от других. При этом важно не терять из вида общий контекст и не погружаться чрезмерно в детали, потому что таким образом можно не увидеть главного.

Методические указания по написанию реферата

Написание реферата является

- одной из форм обучения студентов, направленной на организацию и повышение уровня самостоятельной работы студентов;
- одной из форм научной работы студентов, целью которой является расширение научного кругозора студентов, ознакомление с методологией научного поиска.

Реферат, как форма обучения студентов, - это краткий обзор максимального количества доступных публикаций по заданной теме, с элементами сопоставительного анализа данных материалов и с последующими выводами.

При проведении обзора должна проводиться и исследовательская работа, но объем ее ограничен, так как анализируются уже сделанные предыдущими исследователями выводы и в связи с небольшим объемом данной формы работы.

Темы рефератов определяются кафедрой и содержатся в программе курса. Преподаватель рекомендует литературу, которая может быть использована для написания реферата.

Целью написания рефератов является:

- привитие студентам навыков библиографического поиска необходимой литературы (на бумажных носителях, в электронном виде);
- привитие студентам навыков компактного изложения мнения авторов и своего суждения по выбранному вопросу в письменной форме, научно грамотным языком и в хорошем стиле;
- приобретение навыка грамотного оформления ссылок на используемые источники, правильного цитирования авторского текста;
- выявление и развитие у студента интереса к определенной научной и практической проблематике с тем, чтобы исследование ее в дальнейшем продолжалось в подготовке и написании курсовых и дипломной работы и дальнейших научных трудах.

Основные задачи студента при написании реферата:

- с максимальной полнотой использовать литературу по выбранной теме (как рекомендуемую, так и самостоятельно подобранную) для правильного понимания авторской позиции;
- верно (без искажения смысла) передать авторскую позицию в своей работе;
- уяснить для себя и изложить причины своего согласия (несогласия) с тем или иным автором по данной проблеме.

Требования к содержанию:

- материал, использованный в реферате, должен относится строго к выбранной теме;
- необходимо изложить основные аспекты проблемы не только грамотно, но и в соответствии с той или иной логикой (хронологической, тематической, событийной и др.)
- при изложении следует сгруппировать идеи разных авторов по общности точек зрения или по научным школам;

- реферат должен заканчиваться подведением итогов проведенной исследовательской работы: содержать краткий анализ-обоснование преимуществ той точки зрения по рассматриваемому вопросу, с которой Вы солидарны.

Структура реферата.

1. Начинается реферат с *титульного листа*.

Образец оформления титульного листа для реферата находится на сайте sksi.ru

2. За титульным листом следует *Содержание*. Содержание - это план реферата, в котором каждому разделу должен соответствовать номер страницы, на которой он находится.

3. *Текст* реферата. Он делится на три части: *введение, основная часть и заключение*.

а) *Введение* - раздел реферата, посвященный постановке проблемы, которая будет рассматриваться и обоснованию выбора темы.

б) *Основная часть* - это звено работы, в котором последовательно раскрывается выбранная тема. Основная часть может быть представлена как цельным текстом, так и разделена на главы. При необходимости текст реферата может дополняться иллюстрациями, таблицами, графиками, но ими не следует "перегружать" текст.

в) *Заключение* - данный раздел реферата должен быть представлен в виде выводов, которые готовятся на основе подготовленного текста. Выводы должны быть краткими и четкими. Также в заключении можно обозначить проблемы, которые "высветились" в ходе работы над рефератом, но не были раскрыты в работе.

4. *Список источников и литературы*. В данном списке называются как те источники, на которые ссылается студент при подготовке реферата, так и все иные, изученные им в связи с его подготовкой. В работе должно быть использовано не менее 5 разных источников. Работа, выполненная с использованием материала, содержащегося в одном научном источнике, является явным плагиатом и не принимается. Оформление Списка источников и литературы должно соответствовать требованиям библиографических стандартов (например,Воробьева Ф.И. Информатика. MS Excel 2010 [Электронный ресурс]: учебное пособие/ Воробьева Ф.И., Воробьев Е.С.— Электрон.текстовые данные.— Казань: Казанский национальный исследовательский технологический университет, 2014.— 100 с.— Режим доступа: http://www.iprbookshop.ru/62175.html.— ЭБС «IPRbooks»).

Объем работы должен быть, как правило, не менее 12 и не более 20 страниц. Работа должна выполняться через одинарный интервал 12 шрифтом, размеры оставляемых полей: левое - 25 мм, правое - 15 мм, нижнее - 20 мм, верхнее - 20 мм. Страницы должны быть пронумерованы.

Расстояние между названием части реферата или главы и последующим текстом должно быть равно трем интервалам. Фразы, начинающиеся с "красной" строки, печатаются с абзацным отступом от начала строки, равным 1 см.

При цитировании необходимо соблюдать следующие правила:

- текст цитаты заключается в кавычки и приводится без изменений, без произвольного сокращения цитируемого фрагмента (пропуск слов, предложений или абзацев допускается, если не влечет искажения всего фрагмента, и обозначается многоточием, которое ставится на месте пропуска) и без искажения смысла;
- каждая цитата должна сопровождаться ссылкой на источник, библиографическое описание которого должно приводиться в соответствии с требованиями библиографических стандартов (например,).

Оценивая реферат, преподаватель обращает внимание на:

- соответствие содержания выбранной теме;
- отсутствие в тексте отступлений от темы;
- соблюдение структуры работы, четка ли она и обоснованна;
- умение работать с научной литературой - вычленять проблему из контекста;
- умение логически мыслить;
- культуру письменной речи;

- умение оформлять научный текст (правильное применение и оформление ссылок, составление библиографии);

- умение правильно понять позицию авторов, работы которых использовались при написании реферата;

- способность верно, без искажения передать используемый авторский материал;

- соблюдение объема работы;

- аккуратность и правильность оформления, а также технического выполнения работы.

Реферат должен быть сдан для проверки в установленный срок.

Методические указания к разработке и проведению проблемной лекции.

Под проблемным обучением понимается такая организация учебного процесса, которая предполагает создание под руководством учителя проблемных ситуаций и активную самостоятельную деятельность учащихся по их разрешению, в результате чего и происходит творческое овладение предметными знаниями, умениями, навыками (ЗУН) и развитие творческих способностей.

Данный вид обучения:

1. направлен на самостоятельный поиск учащимися новых понятий и способов действий;
2. предполагает последовательное и целенаправленное выдвижение перед учащимися познавательных проблем, разрешение которых (под руководством учителя) приводит к активному усвоению новых знаний;
3. обеспечивает особый способ мышления, прочность знаний и творческое их применение в практической деятельности.

При проблемном обучении преподаватель не сообщает готовых знаний, а организует учащихся на их поиск: понятия, закономерности, теории познаются в ходе поиска, наблюдений, анализа фактов, мыслительной деятельности.

Необходимыми составляющими проблемного обучения являются следующие понятия: «проблема», «проблемная ситуация», «гипотеза», «эксперимент».

9. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Для реализации дисциплины необходимо следующее материально-техническое обеспечение:

- для проведения занятий лекционного типа - аудитория, оборудованная мультимедийными средствами обучения: проектором, ПК, экраном, доской;

- для проведения лабораторных занятий - компьютерный класс с предустановленным программным обеспечением, указанным в п.8.3.

- для проведения промежуточной аттестации - компьютерный класс с предустановленным программным обеспечением, указанным в п.8.3.

- практическая подготовка - компьютерный класс с предустановленным программным обеспечением, указанным в п.8.3.

- для самостоятельной работы: помещение для самостоятельной работы с возможностью подключения к информационно-коммуникационной сети «Интернет» и обеспечением доступа в электронную информационно-образовательную среду.

10. ОСОБЕННОСТИ ОСВОЕНИЯ ДИСЦИПЛИНЫ ЛИЦАМИ С ОГРАНИЧЕННЫМИ ВОЗМОЖНОСТЯМИ ЗДОРОВЬЯ

Обучающимся с ограниченными возможностями здоровья предоставляются специальные учебники, учебные пособия и дидактические материалы, специальные технические средства обучения коллективного и индивидуального пользования, услуги ассистента (тьютора), оказывающего обучающимся необходимую техническую помощь, а также услуги сурдопереводчиков и тифлосурдопереводчиков.

Освоение дисциплины обучающимися с ограниченными возможностями здоровья и инвалидами может быть организовано совместно с другими обучающимися, а также в отдельных группах.

Освоение дисциплины обучающимися с ограниченными возможностями здоровья и инвалидами осуществляется с учетом особенностей психофизического развития, индивидуальных возможностей и состояния здоровья.

В целях доступности получения среднего профессионального образования по образовательной программе лицами с ограниченными возможностями здоровья при освоении дисциплины обеспечивается:

1) для лиц с ограниченными возможностями здоровья по зрению:

– присутствие тьютора, оказывающий студенту необходимую техническую помощь с учетом индивидуальных особенностей (помогает занять рабочее место, передвигаться, прочитать и оформить задание, в том числе, записывая под диктовку),

– письменные задания, а также инструкции о порядке их выполнения оформляются увеличенным шрифтом,

– специальные учебники, учебные пособия и дидактические материалы (имеющие крупный шрифт или аудиофайлы),

– индивидуальное равномерное освещение не менее 300 люкс,

– при необходимости студенту для выполнения задания предоставляется увеличивающее устройство;

2) для лиц с ограниченными возможностями здоровья по слуху:

– присутствие ассистента, оказывающий студенту необходимую техническую помощь с учетом индивидуальных особенностей (помогает занять рабочее место, передвигаться, прочитать и оформить задание, в том числе, записывая под диктовку),

– обеспечивается наличие звукоусиливающей аппаратуры коллективного пользования, при необходимости обучающемуся предоставляется звукоусиливающая аппаратура индивидуального пользования;

– обеспечивается надлежащими звуковыми средствами воспроизведения информации;

3) для лиц с ограниченными возможностями здоровья, имеющих нарушения опорно-двигательного аппарата:

– письменные задания выполняются на компьютере со специализированным программным обеспечением или надиктовываются тьютору;

– по желанию студента задания могут выполняться в устной форме.

Приложение 1

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ (ОЦЕНОЧНЫЕ МАТЕРИАЛЫ) ДЛЯ ПРОВЕДЕНИЯ ТЕКУЩЕГО КОНТРОЛЯ УСПЕВАЕМОСТИ И ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ

По дисциплине «Методы и средства защиты информации организаций»

1. Показатели, критерии оценки освоения дисциплины

Результаты обучения	Показатели оценивания	Критерии оценивания	Процедуры оценивания
ПК-3 Способен анализировать требования к программному обеспечению, разрабатывать технические спецификации на программные компоненты и их взаимодействие			
Знает общие принципы организации защиты конфиденциальной информации, применяемые при разработке систем защиты информации на предприятии; основы нормативных документов об ответственности за разглашение конфиденциальной информации.	Демонстрация знаний общих принципов организации защиты конфиденциальной информации, применяемых при разработке систем защиты информации на предприятии; основ нормативных документов об ответственности за разглашение конфиденциальной информации.	Качество знаний общих принципов организации защиты конфиденциальной информации, применяемых при разработке систем защиты информации на предприятии; основ нормативных документов об ответственности за разглашение конфиденциальной информации.	устный опрос, тестирование
Умеет использовать существующие типовые решения и шаблоны проектирования программного обеспечения, применять методы и средства проектирования программного обеспечения, структур данных, баз данных, программных интерфейсов; классифицировать угрозу конфиденциальной информации по ее проявлению на предприятии; применять на практике технические, программно-аппаратные и программные средства	Демонстрация умений по использованию существующих типовых решений и шаблонов проектирования программного обеспечения, применению методов и средств проектирования программного обеспечения, структур данных, баз данных, программных интерфейсов; классифицировании угрозы конфиденциальной информации по ее проявлению на предприятии; применению на практике технических, программно-аппаратных	Методическая грамотность использования существующих типовых решений и шаблонов проектирования программного обеспечения, применению методов и средств проектирования программного обеспечения, структур данных, баз данных, программных интерфейсов; классифицировании угрозы конфиденциальной информации по ее проявлению на предприятии; применению на практике технических,	практические задания

защиты информации	и программные средства защиты информации.	программно-аппаратных и программные средства защиты информации.	
Владеет навыками проведения анализа исполнения требований к ПО, выработки вариантов реализации требований к ПО, оценки и обоснования рекомендуемых решений по ПО; содержанием уровней защиты информации в составе комплексной системы защиты информации на предприятии; навыками работы на рабочих станциях АИС предприятия по обеспечению возможных вариантов доступа пользователей к конфиденциальной информации.	Демонстрирует владение навыками проведения анализа исполнения требований к ПО, выработки вариантов реализации требований к ПО, оценки и обоснования рекомендуемых решений по ПО; содержанием уровней защиты информации в составе комплексной системы защиты информации на предприятии; навыками работы на рабочих станциях АИС предприятия по обеспечению возможных вариантов доступа пользователей к конфиденциальной информации.	Адекватность выбора методов проведения анализа исполнения требований к ПО, выработки вариантов реализации требований к ПО, оценки и обоснования рекомендуемых решений по ПО; содержанием уровней защиты информации в составе комплексной системы защиты информации на предприятии; навыками работы на рабочих станциях АИС предприятия по обеспечению возможных вариантов доступа пользователей к конфиденциальной информации.	практические задания
ПК-5 Способен разрабатывать модели бизнес-процессов и адаптировать бизнес-процессы к возможностям ИС организации			
Знает перечень организационных и организационно-технический мероприятий, выполняемых на предприятии по защите конфиденциальной информации; основные источники случайных (непреднамеренных) угроз на предприятии и их классификацию; умышленные угрозы воздействия на конфиденциальную информацию и их классификацию.	Демонстрация знаний в области организационных и организационно-технических мероприятий, выполняемых на предприятии по защите конфиденциальной информации; по основным источникам случайных (непреднамеренных) угроз на предприятии и их классификацию; по умышленным угрозам воздействия на конфиденциальную информацию и их классификацию.	Качество знаний в области организационных и организационно-технических мероприятий, выполняемых на предприятии по защите конфиденциальной информации; по основным источникам случайных (непреднамеренных) угроз на предприятии и их классификацию; по умышленным угрозам воздействия на конфиденциальную информацию и их классификацию.	устный опрос, тестирование
Умеет применять средства построения модели бизнес-процесса,	Демонстрация умений по применению средств построения модели	Методическая грамотность и корректность	практические задания

применять средства моделирование бизнес-процессов; классифицировать угрозу конфиденциальной информации по ее проявлению на предприятии.	бизнес-процесса, средств моделирования бизнес-процессов; классификации угроз конфиденциальной информации по ее проявлению на предприятии.	использования умений по применению средств построения модели бизнес-процесса, средств моделирования бизнес-процессов; классификации угроз конфиденциальной информации по ее проявлению на предприятии.	
Владеет навыками разработки модели бизнес-процессов и предлагаемых изменений, согласования с заказчиком модели бизнес-процессов, моделирования бизнес – процессов.	Демонстрирует владение навыками разработки модели бизнес-процессов и предлагаемых изменений, согласования с заказчиком модели бизнес-процессов, моделирования бизнес – процессов.	Адекватность выбора методов осуществления разработки модели бизнес-процессов и предлагаемых изменений, согласования с заказчиком модели бизнес-процессов, моделирования бизнес – процессов.	практические задания
ПК-8 Способен обеспечивать управление доступом к программно- аппаратным средствам информационных служб инфокоммуникационной системы (ИКС)			
Знает инструкции по установке и эксплуатации компьютерного, периферийного и абонентского оборудования, типовые ошибки, возникающие при работе инфокоммуникационной системы, признаки их проявления при работе и методы устранения, структура модели взаимодействия открытых систем (OSI) ISO;	Демонстрация знаний инструкций по установке и эксплуатации компьютерного, периферийного и абонентского оборудования, типовых ошибок, возникающих при работе инфокоммуникационной системы, признаки их проявления при работе и методы устранения, структуры модели взаимодействия открытых систем (OSI) ISO;	Полнота и качество знаний по установке и эксплуатации компьютерного, периферийного и абонентского оборудования, типовых ошибок, возникающих при работе инфокоммуникационной системы, признаки их проявления при работе и методы устранения, структуры модели взаимодействия открытых систем (OSI) ISO;	устный опрос, тестирование
Умеет идентифицировать права пользователей по доступу к программно-аппаратным средствам информационных служб инфокоммуникационной системы и ее составляющих, применять специальные программно-аппаратные	Демонстрация умений идентифицировать права пользователей по доступу к программно-аппаратным средствам информационных служб инфокоммуникационной системы и ее составляющих, применять специальные программно-аппаратные	Методическая грамотность и корректность использования умений идентифицировать права пользователей по доступу к программно-аппаратным средствам информационных служб инфокоммуникационной системы и ее	практические задания

средства контроля доступа пользователей к программно-аппаратным средствам информационных служб инфокоммуникационной системы, применять утилиты операционных систем по управлению и контролю доступа к компонентам ИКС.	средства контроля доступа пользователей к программно-аппаратным средствам информационных служб инфокоммуникационной системы, применять утилиты операционных систем по управлению и контролю доступа к компонентам ИКС.	составляющих, применять специальные программно-аппаратные средства контроля доступа пользователей к программно-аппаратным средствам информационных служб инфокоммуникационной системы, применять утилиты операционных систем по управлению и контролю доступа к компонентам ИКС.	
Владеет навыками управления, изменения и контроля соблюдения прав доступа пользователей к программно-аппаратным средствам информационных служб инфокоммуникационной системы, определения приемлемых для пользователей параметров работы сети в условиях нормальной обычной работы , использования современные методы контроля производительности инфокоммуникационных систем.	Демонстрирует владение навыками управления, изменения и контроля соблюдения прав доступа пользователей к программно-аппаратным средствам информационных служб инфокоммуникационной системы, определения приемлемых для пользователей параметров работы сети в условиях нормальной обычной работы , использования современные методы контроля производительности инфокоммуникационных систем.	Адекватность выбора методов управления, изменения и контроля соблюдения прав доступа пользователей к программно-аппаратным средствам информационных служб инфокоммуникационной системы, определения приемлемых для пользователей параметров работы сети в условиях нормальной обычной работы , использования современные методы контроля производительности инфокоммуникационных систем.	практические задания
ПК-11 Способен разрабатывать политику и регламенты информационной безопасности, проводить аудит системы безопасности данных с подготовкой отчетов о состоянии и эффективности системы безопасности			
Знает стандарты информационной безопасности, уязвимости инфокоммуникационных систем, классы информационной защищённости систем, угрозы безопасности и способы их предотвращения, структуру и содержание политики информационной	Демонстрация знаний стандартов информационной безопасности, уязвимости инфокоммуникационных систем, классов информационной защищённости систем, угроз безопасности и способы их предотвращения, структуры и содержание политики	Качество и полнота знаний стандартов информационной безопасности, уязвимости инфокоммуникационных систем, классов информационной защищённости систем, угроз безопасности и способы их предотвращения, структуры и содержание политики	устный опрос, тестирование

безопасности, методы и средства обеспечения безопасности данных при работе с БД и при передаче в телекоммуникациях, характеристики систем и средств обеспечения безопасности, влияющие на производительность систем, средства и инструменты восстановления безопасности, законодательство Российской Федерации в области обеспечения информационной безопасности в информационных системах, методику разработки регламента аудита систем безопасности.	информационной безопасности, методов и средств обеспечения безопасности данных при работе с БД и при передаче в телекоммуникациях, характеристик систем и средств обеспечения безопасности, влияющих на производительность систем, средств и инструментов восстановления безопасности, законодательства Российской Федерации в области обеспечения информационной безопасности в информационных системах, методик разработки регламента аудита систем безопасности.	информационной безопасности, методов и средств обеспечения безопасности данных при работе с БД и при передаче в телекоммуникациях, характеристик систем и средств обеспечения безопасности, влияющих на производительность систем, средств и инструментов восстановления безопасности, законодательства Российской Федерации в области обеспечения информационной безопасности в информационных системах, методик разработки регламента аудита систем безопасности	
Умеет выявлять угрозы информационной безопасности, факты нарушения регламентов обеспечения безопасности, разрабатывать мероприятия по обеспечению безопасности на уровне БД, настраивать программно-аппаратные средства защиты данных и процедуры выявления попыток несанкционированного доступа к данным, оценивать степень нагрузки различных инструментов обеспечения безопасности на производительность, планировать и осуществлять меры по устранению последствий нарушения регламентов	Демонстрация умений по выявлению угроз информационной безопасности, факты нарушения регламентов обеспечения безопасности, разработке мероприятий по обеспечению безопасности на уровне БД, настройке программно-аппаратных средств защиты данных и процедуры выявления попыток несанкционированного доступа к данным, оценке степени нагрузки различных инструментов обеспечения безопасности на производительность, планирования и осуществления меры по устранению последствий нарушения регламентов	Методическая грамотность и корректность использования умений по выявлению угроз информационной безопасности, факты нарушения регламентов обеспечения безопасности, разработке мероприятий по обеспечению безопасности на уровне БД, настройке программно-аппаратных средств защиты данных и процедуры выявления попыток несанкционированного доступа к данным, оценке степени нагрузки различных инструментов обеспечения безопасности на производительность, планирования и	практические задания

обеспечения безопасности, настраивать параметры инструментов системы безопасности в соответствии с установленными критериями, разрабатывать комплекс организационно-технических мероприятий по обеспечению безопасности данных, оценивать степень защиты данных от угроз безопасности.	обеспечения безопасности, настройке параметров инструментов системы безопасности в соответствии с установленными критериями, разработке комплекса организационно-технических мероприятий по обеспечению безопасности данных, оценке степени защиты данных от угроз безопасности.	осуществления меры по устранению последствий нарушения регламентов обеспечения безопасности, настройке параметров инструментов системы безопасности в соответствии с установленными критериями, разработке комплекса организационно-технических мероприятий по обеспечению безопасности данных, оценке степени защиты данных от угроз безопасности.	
Владеет навыками выявления действий, нарушающих регламент обеспечения безопасности, выбор наиболее эффективных путей снижения нагрузки при обеспечении заданного уровня безопасности данных, анализа возможных угроз для безопасности данных, выбора средств обеспечения информационной безопасности, настройки параметры инструментов системы безопасности в соответствии с установленными критериями, определения показателей и критериев эффективности системы безопасности, оценки уровня и состояния системы безопасности данных, определения возможностей оптимизации работы	Демонстрирует владение навыками выявления действий, нарушающих регламент обеспечения безопасности, выбор наиболее эффективных путей снижения нагрузки при обеспечении заданного уровня безопасности данных, анализа возможных угроз для безопасности данных, выбора средств обеспечения информационной безопасности, настройки параметры инструментов системы безопасности в соответствии с установленными критериями, определения показателей и критериев эффективности системы безопасности, оценки уровня и состояния системы безопасности данных, определения возможностей	Адекватность выбора методов выявления действий, нарушающих регламент обеспечения безопасности, выбор наиболее эффективных путей снижения нагрузки при обеспечении заданного уровня безопасности данных, анализа возможных угроз для безопасности данных, выбора средств обеспечения информационной безопасности, настройки параметры инструментов системы безопасности в соответствии с установленными критериями, определения показателей и критериев эффективности системы безопасности, оценки уровня и состояния системы безопасности данных, определения возможностей	практические задания

систем безопасности с целью уменьшения нагрузки на работу системы, выбора наиболее эффективных путей снижения нагрузки при обеспечении заданного уровня безопасности данных, выбора критериев оценки результатов аудита данных, разработки методик аудита системы безопасности данных, аудита системы безопасности и оценка ее эффективности.	оптимизации работы систем безопасности с целью уменьшения нагрузки на работу системы, выбора наиболее эффективных путей снижения нагрузки при обеспечении заданного уровня безопасности данных, выбора критериев оценки результатов аудита данных, разработки методик аудита системы безопасности данных, аудита системы безопасности и оценка ее эффективности.	оптимизации работы систем безопасности с целью уменьшения нагрузки на работу системы, выбора наиболее эффективных путей снижения нагрузки при обеспечении заданного уровня безопасности данных, выбора критериев оценки результатов аудита данных, разработки методик аудита системы безопасности данных, аудита системы безопасности и оценка ее эффективности.	
ПК-3, ПК-5, ПК-8, ПК-11			Промежуточная аттестация: экзамен

2. Методические материалы, определяющие процедуры оценивания

2.1. Методические материалы, определяющие процедуры оценивания в рамках текущего контроля успеваемости

Устные опросы проводятся во время лекций, практических занятий и возможны при проведении промежуточной аттестации в качестве дополнительного испытания при недостаточности результатов тестирования. Основные вопросы для устного опроса доводятся до сведения студентов на предыдущем занятии.

Количество вопросов определяется преподавателем.

Время проведения опроса от 10 минут до 1 академического часа.

Устные опросы строятся так, чтобы вовлечь в тему обсуждения максимальное количество обучающихся в группе, проводить параллели с уже пройденным учебным материалом данной дисциплины и смежными курсами, находить удачные примеры из современной действительности, что увеличивает эффективность усвоения материала на ассоциациях.

Критерии и шкала оценки устного опроса

Развернутый ответ студента должен представлять собой связное, логически последовательное сообщение на заданную тему, показывать его умение применять определения, правила в конкретных случаях.

«отлично» ставится, если:

1) студент полно излагает материал, дает правильное определение основных понятий;

2) обнаруживает понимание материала, может обосновать свои суждения, применить знания на практике, привести необходимые примеры не только из учебника, но и самостоятельно составленные;

3) излагает материал последовательно и правильно с точки зрения норм литературного языка.

«хорошо» - студент дает ответ, удовлетворяющий тем же требованиям, что и для «отлично», но допускает 1–2 ошибки, которые сам же исправляет, и 1–2 недочета в последовательности и языковом оформлении излагаемого.

«удовлетворительно» – студент обнаруживает знание и понимание основных положений данной темы, но:

1) излагает материал неполно и допускает неточности в определении понятий или формулировке правил;

2) не умеет достаточно глубоко и доказательно обосновать свои суждения и привести свои примеры;

3) излагает материал непоследовательно и допускает ошибки в языковом оформлении излагаемого.

«неудовлетворительно» ставится, если студент обнаруживает незнание большей части соответствующего вопроса, допускает ошибки в формулировке определений и правил, искажающие их смысл, беспорядочно и неуверенно излагает материал. Оценка «2» отмечает такие недостатки в подготовке, которые являются серьезным препятствием к успешному овладению последующим материалом.

Практические задания выполняются студентами на практических занятиях. Студентам необходимо выполнить практические задания, указанные преподавателем. Результаты работы сохранить в файлах. После выполнения заданий необходимо преподавателю продемонстрировать результаты работы и быть готовым ответить на вопросы и продемонстрировать выполнение отдельных пунктов заданий. Защита выполненных практических заданий осуществляется на практическом занятии.

Критерии и шкала оценки практических заданий

«отлично» ставится, если: студент самостоятельно и правильно решил учебно-профессиональную задачу, уверенно, логично, последовательно и аргументировано излагал свое решение, используя изученные понятия.

«хорошо» ставится, если: студент самостоятельно и в основном правильно решил учебно-профессиональную задачу, уверенно, логично, последовательно и аргументировано излагал свое решение, используя изученные понятия.

«удовлетворительно» ставится, если: студент в основном решил учебно-профессиональную задачу, допустил несущественные ошибки, слабо аргументировал свое решение, используя в основном изученные понятия.

«неудовлетворительно» ставится, если: студент не решил учебно-профессиональную задачу.

Тестирование – универсальный инструмент определения уровня обученности студентов на всех этапах образовательного процесса, в том числе для оценки уровня остаточных знаний.

Тестирование студентов проводится во время отводимое на практические занятия или во время указанное преподавателем. Индивидуальное тестовое задание выдаётся обучающемуся в бумажном формате или формируется посредством тестовой программы для ПЭВМ, если занятие проводится в специально оборудованном помещении.

Критерии и шкала оценки тестирования

«отлично» - студент выполняет правильно 86-100 % тестовых заданий.

«хорошо» - студент выполняет правильно 71-85 % тестовых заданий.

«удовлетворительно» - студент выполняет правильно 51-70% тестовых заданий.

«неудовлетворительно» - студент выполняет правильно до 50% тестовых заданий

2.2. Методические материалы, определяющие процедуры оценивания в рамках промежуточной аттестации

Промежуточная аттестация по дисциплине проводится в форме устного **экзамена** по расписанию экзаменационной сессии.

Вопросы к экзамену доводятся до сведения студентов заранее.

Билет к экзамену содержит 2 вопроса.

При подготовке к ответу пользование учебниками, учебно-методическими пособиями, средствами связи и электронными ресурсами на любых носителях запрещено.

Время на подготовку ответа – от 30 до 45 минут.

По истечении времени подготовки ответа, студент отвечает на вопросы экзаменационного билета. На ответ студента по каждому вопросу билета отводится, как правило, 3-5 минут.

После ответа студента преподаватель может задать дополнительные (уточняющие) вопросы в пределах предметной области экзаменационного задания.

После окончания ответа преподаватель объявляет обучающемуся оценку по результатам экзамена, а также вносит эту оценку в экзаменационную ведомость, зачетную книжку.

Критерии и шкала оценки экзамена

«отлично» ставится, если:

- студент глубоко и всесторонне усвоил программный материал;
- уверенно, логично, последовательно и грамотно его излагает;
- опираясь на знания основной и дополнительной литературы, тесно привязывает усвоенные научные положения с практической деятельностью;
- умело обосновывает и аргументирует выдвигаемые им идеи;
- делает выводы и обобщения;
- свободно владеет системой понятий по дисциплине.

«хорошо» ставится, если:

- студент твердо усвоил программный материал, грамотно и по существу излагает его, опираясь на знания основной литературы;
- не допускает существенных неточностей;
- увязывает усвоенные знания с практической деятельностью бакалавра;
- аргументирует научные положения;
- делает выводы и обобщения;
- владеет системой понятий по дисциплине.

«удовлетворительно» ставится, если:

- студент усвоил только основной программный материал, по существу излагает его, опираясь на знания только основной литературы;
- допускает несущественные ошибки и неточности;
- испытывает затруднения в практическом применении знаний;
- слабо аргументирует научные положения;
- затрудняется в формулировании выводов и обобщений;
- частично владеет системой понятий по дисциплине.

«неудовлетворительно» ставится, если:

- студент не усвоил значительной части программного материала;
- допускает существенные ошибки и неточности при рассмотрении проблем;
- испытывает трудности в практическом применении знаний;
- не может аргументировать научные положения;
- не формулирует выводов и обобщений.

3. Типовые контрольные задания

Типовые задания для текущего контроля успеваемости

3.1. Типовые вопросы для устного опроса при текущем контроле

Основные концептуальные положения системы защиты информации.

1. Угрозы конфиденциальной информации
2. Действия, приводящие к неправомерному овладению конфиденциальной информацией
3. Коммерческая тайна.
4. Критерии безопасности компьютерных систем.
5. Классы безопасности компьютерных систем, категории требований безопасности компьютерных систем.
6. Организационная защита.
7. Инженерно-техническая защита.
8. Физические средства защиты.
9. Основные направления использования программной защиты информации.
10. Понятие вредоносных программ, их классификация, способы распространения вредоносных программ.
11. Программно-технические методы обнаружения вирусов.
12. Защита информации от несанкционированного доступа.
13. Защита от копирования.
14. Особенности защиты информации в персональных компьютерах.
15. Наука криптография.
16. Основные направления использования некриптографической защиты информации.
17. Основные направления использования криптографической защиты информации.
18. Общие сведения о работе современных симметричных криптосистем (рассеивание, перемешивание, петля Фейстеля),
19. Управление ключами.
20. Электронная цифровая подпись.
21. Общая технология шифрования.
22. Технология шифрования речи.
23. Алгоритм цифровой подписи RSA.
24. Алгоритм цифровой подписи Эль Гамаля.
25. Отечественный стандарт цифровой подписи.
26. Понятия лицензирования в области защиты информации, порядок проведения лицензирования.
27. Понятия сертификации в области защиты информации, нормативная правовая база системы сертификации.
28. Многоуровневая защита корпоративных сетей.
29. Защита информации в сетях.
30. Требования к системам защиты информации.
31. Фильтрующие маршрутизаторы.
32. Шлюзы прикладного уровня.
33. Межсетевой экран – фильтрующий маршрутизатор.
34. Межсетевой экран на основе двухпортового шлюза.
35. Межсетевой экран – экранированная подсеть.
36. Полностью контролируемые компьютерные системы.
37. Частично контролируемые компьютерные системы.

3.2 Типовые тестовые задания для текущего контроля

1. Деятельность, направленная на предотвращение воздействия на защищаемую информацию с нарушением установленных прав и (или) правил на изменение информации, приводящего к ее искажению, уничтожению, блокированию доступа к информации, а также к утрате, уничтожению или сбою функционирования носителя информации, это:

а) защита информации от агентурной разведки;
б) защита информации от непреднамеренного воздействия;
в) защита информации от несанкционированного воздействия;
г) защита информации от разведки.

2. Состояние защищенности информационной среды общества, обеспечивающее ее формирование, использование и развитие в интересах граждан, организаций и государства, это:

а) информационная революция;
б) информационная среда общества;
в) информационная сфера;
г) информационная безопасность;
д) информационная инфраструктура.

3. Информация, для которой установлен специальный режим сбора, хранения, обработки, распространения и использования, это:

а) информация о гражданах;
б) информационный продукт;
в) информационный процесс;
г) информация с ограниченным доступом;
д) информационная безопасность.

4. Информация с ограниченным доступом разделяется на:

а) секретную и конфиденциальную;
б) секретную и несекретную;
в) открытую и конфиденциальную;
г) секретную и совершенно секретную;
д) секретную и несекретную.

5. Сведения, составляющие государственную тайну, имеют гриф секретности:

а) совершенно секретно;
б) несекретно;
в) особой важности;
г) секретно;
д) конфиденциально.

6. К конфиденциальной информации относится:

а) служебная тайна;
б) государственная тайна;
в) персональные данные;
г) коммерческая тайна;
д) профессиональная тайна.

7. Защита от утечки информации, это:

а) защита от несанкционированного воздействия;
б) защита от разглашения;
в) защита от несанкционированного доступа;
г) защита от непреднамеренного воздействия;
д) защита от разведки.

8. Степень соответствия результатов защиты информации поставленной цели защиты информации, это:

а) цель защиты информации;
б) безопасность информации;
в) активная стратегия;
г) доступность информации;
д) эффективность защиты информации.

9. Длина ключевого элемента в алгоритме шифрования DES:

а) 24 элемента;

б) 32 элемента;
в) 48 элементов;
г) 56 элементов;
д) 64 элемента.

10. Количество циклов шифрования в алгоритме DES равно:

а) 8;
б) 16;
в) 24;
г) 32;
д) 64.

11. Объем ключа в алгоритме DES равен:

а) 32 бит;
б) 48 бит;
в) 56 бит;
г) 64 бит;
д) 256 бит.

12. Длина ключевого элемента в ГОСТ блочного шифрования равна:

а) 24;
б) 23;
в) 48;
г) 56;
д) 64.

13. Количество циклов шифрования в ГОСТ блочного шифрования равно:

а) 8;
б) 16;
в) 24;
г) 32;
д) 64.

14. Объем ключа в ГОСТ блочного шифрования равен:

а) 32 бит;
б) 64 бит;
в) 128 бит;
г) 256 бит;
д) 512 бит.

15. В основе композиционных блочных шифров лежат следующие преобразования:

а) замена;
б) рассеивание;
в) подстановка;
г) имитовставка;
д) перемешивание.

16. В каких криптосистемах открытый ключ и криптограмма могут передаваться по незащищенным каналам:

а) в классических симметричных криптосистемах;
б) в криптосистемах с депонированием ключей;
в) при шифровании методом гаммирования;
г) в асимметричных криптосистемах;
д) с применением поточных шифров.

17. В криптосистеме RSA открытый ключ, секретный ключ, сообщение и криптограмма должны принадлежать:

а) множеству действительных чисел;
б) множеству целых чисел;
в) множеству простых чисел;

г) множеству случайных чисел.

18. Секретный ключ в криптосистеме RSA вычисляется:

а) отправителем;

б) получателем;

в) противником.

19. Для вычисления секретного ключа в криптосистеме RSA применяется:

а) расширенный алгоритм Евклида;

б) метод Вернама;

в) система Вижинера;

г) алгоритм Эль Гамаля.

20. Проверка принадлежности субъекту доступа предъявленного им идентификатора, подтверждение подлинности, это:

а) аутентификация;

б) идентификация;

в) предоставление полномочий.

21. Функция, осуществляющая отображение элементов некоторого множества в индекс линейного множества, это:

а) хэш-функция;

б) функция гаммирования;

в) функция генераций ключей;

г) функция дешифрования.

22. Система электронной цифровой подписи включает в себя:

а) процедуру постановки подписи;

б) процедуру идентификации;

в) процедуру аутентификации;

г) процедуру проверки подписи.

23. В качестве подписываемого документа может быть использован:

а) текстовый файл;

б) звуковой файл;

в) любой файл;

г) программный файл.

24. Для сжатия подписываемого документа до нескольких десятков или сотен бит используются:

а) программы – архиваторы;

б) хэш-функции;

в) выработка имитовставки;

г) режим гаммирования.

25. Защищаемые государством сведения в области его военной, внешнеполитической, экономической, разведывательной, контрразведывательной и оперативной деятельности, распространение которых может нанести ущерб безопасности Российской Федерации, это:

а) военная тайна;

б) конфиденциальная тайна;

в) государственная тайна;

г) служебная тайна.

26. Решить сравнение 5 * x = mod 22:

а) x=9;

б) x=18;

в) x=11.

27. Решить сравнение 7 * x = mod 22:

а) x=8;

б) x=19;

в) x=15.

Ответы

№ вопроса	Ответ	№ вопроса	Ответ	№ вопроса	Ответ
1	*в*	11	*в*	21	*а*
2	*г*	12	*б*	22	*а, г*
3	*г*	13	*г*	23	*а, б, в, г*
4	*а*	14	*г*	24	*б*
5	*а, в, г*	15	*б, д*	25	*в*
6	*а, в, г, д*	16	*г*	26	*а)*
7	*б, в, д*	17	*б*	27	*б)*
8	*д*	18	*б*		
9	*в*	19	*а*		
10	*б*	20	*а*		

3.3 Типовые практические задания

Средства обеспечения безопасности ОС Windows

Цель: изучить модель безопасности операционной системы Windows, получить навыки практического использования ее средств обеспечения безопасности.

Задание

1. Снимите запрет на чтение папки forTesting для пользователя testUser. Используя команду cacls запретите этому пользователю доступ к файлам с расширением txt в папке forTesting. Убедитесь в недоступности файлов для пользователя.

2. Командой cacls запретите пользователю все права на доступ к папке forTesting и разреште полный доступ к вложенной папке forTesting\Docs. Убедитесь в доступности папки forTesting\Docs для пользователя. Удалите у пользователя testUser привилегию SeChangeNotifyPrivilege. Попробуйте получить доступ к папке forTesting\Docs. Объясните результат.

3. Запустите файловый менеджер от имени пользователя testUser и создайте в нем папку newFolder на диске C. Для папки newFolder очистите весь список ACL командой cacls. Попробуйте теперь получить доступ к папке от имени администратора и от имени пользователя. Кто и как теперь может вернуть доступ к папке? Верните полный доступ к папке для всех пользователей.

4. Создайте в разделе HKLM\Software реестра раздел testKey. Запретите пользователю testUser создание новых разделов в этом разделе реестра. Создайте для раздела HKLM\Software\testKey SACL, позволяющий протоколировать отказы при создании новых подразделов, а также успехи при перечислении подразделов и запросе значений (предварительно проверьте, что в локальной политике безопасности соответствующий тип аудита включен). Попробуйте от имени пользователя testUser запустить regedit.exe и создать раздел в HKLM\Software. Убедитесь, что записи аудита были размещены в журнале безопасности (eventvwr.msc).

5. Подготовьте отчет о проделанной работе в текстовом файле, сопровождая его скриншотами выполняемых действий. В отчет необходимо включить ответы на контрольные вопросы и выводы по проделанной работе. Если в процессе работы у Вас создан файл в какой-то программе, то его прилагают к отчету в формате той программы, в которой он создан.

Типовые задания для промежуточной аттестации

3.4. Типовые контрольные вопросы для устного опроса на экзамене

1. Основные концептуальные положения системы защиты информации.
2. Угрозы конфиденциальной информации
3. Действия, приводящие к неправомерному овладению конфиденциальной информацией
4. Коммерческая тайна.
5. Критерии безопасности компьютерных систем.
6. Классы безопасности компьютерных систем, категории требований безопасности компьютерных систем.
7. Организационная защита.
8. Инженерно-техническая защита.
9. Физические средства защиты.
10. Основные направления использования программной защиты информации.
11. Понятие вредоносных программ, их классификация, способы распространения вредоносных программ.
12. Программно-технические методы обнаружения вирусов.
13. Защита информации от несанкционированного доступа.
14. Защита от копирования.
15. Особенности защиты информации в персональных компьютерах.
16. Наука криптография.
17. Основные направления использования некриптографической защиты информации.
18. Основные направления использования криптографической защиты информации.
19. Общие сведения о работе современных симметричных криптосистем (рассеивание, перемешивание, петля Фейстеля),
20. Управление ключами.
21. Электронная цифровая подпись.
22. Общая технология шифрования.
23. Технология шифрования речи.
24. Алгоритм цифровой подписи RSA.
25. Алгоритм цифровой подписи Эль Гамаля.
26. Отечественный стандарт цифровой подписи.
27. Понятия лицензирования в области защиты информации, порядок проведения лицензирования.
28. Понятия сертификации в области защиты информации, нормативная правовая база системы сертификации.
29. Многоуровневая защита корпоративных сетей.
30. Защита информации в сетях.
31. Требования к системам защиты информации.
32. Фильтрующие маршрутизаторы.
33. Шлюзы прикладного уровня.
34. Межсетевой экран – фильтрующий маршрутизатор.
35. Межсетевой экран на основе двухпортового шлюза.
36. Межсетевой экран – экранированная подсеть.
37. Полностью контролируемые компьютерные системы.
38. Частично контролируемые компьютерные системы.