Государственное бюджетное образовательное учреждение высшего образования
Московской области

ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ

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

«УТВЕРЖДАЮ»
Проректор по учебной работе
_____ Е.К. Самаров
«__» июня 2021 г.

ИНСТИТУТ
ИНФОКОММУНИКАЦИОННЫХ СИСТЕМ И ТЕХНОЛОГИЙ

КАФЕДРА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

«БЕЗОПАСНОСТЬ ИНФОРМАЦИОННЫХ СИСТЕМ»

Направление подготовки: 09.03.02 Информационные системы и технологии
Профиль: информационные технологии в технических системах
Уровень высшего образования: бакалавриат
Форма обучения: очная, заочная

Королев 2021

Рабочая программа является составной частью основной профессиональной образовательной программы и проходит рецензирование со стороны работодателей в составе основной профессиональной образовательной программы. Рабочая программа актуализируется и корректируется ежегодно.

Автор: Журавлева Т.Ю.. **Рабочая программа дисциплины «Безопасность информационных систем». – Королев МО: МГОТУ, 2021 г. - 44 с.**

Рецензент: к.в.н. Соляной В.Н.

Рабочая программа составлена в соответствии с требованиями федерального государственного образовательного стандарта высшего образования (ФГОС ВО) по направлению подготовки бакалавров 09.03.02 Прикладная информатика Учебного плана, утвержденного Ученым советом МГОТУ.

Протокол № 13 от 22.06.2021 г.

Рабочая программа рассмотрена и одобрена на заседании кафедры:

Заведующий кафедрой (ФИО, ученая степень, звание, подпись)	Соляной В.Н., к.в.н.			
Год утверждения (переутверждения)	2021			
Номер и дата протокола заседания кафедры	№15 от 02.06.2021			

Рабочая программа согласована:

Руководитель ОПОП к.т.н., доц. Аббасова Т.С.

Рабочая программа рекомендована на заседании УМС:

Год утверждения (переутверждения)	2021			
Номер и дата протокола заседания УМС	№7 от 15.06.2021 г.			

1. Перечень планируемых результатов обучения по дисциплине (модулю), соотнесенных с планируемыми результатами освоения ОПОП

Целью изучения дисциплины является:

1. Формирование базовых знаний и практических навыков обеспечения безопасности информационных систем.
2. Развитие творческого и исследовательского подхода к изучению технических дисциплин студенчества.
3. Подготовка студентов к видам профессиональной деятельности: проектной, производственно-технологической, организационно-управленческой, аналитической и научно-исследовательской.
4. Приобретение студентами знаний и представлений об основных принципах и закономерностях функционирования современной вычислительной техники и их информационной безопасности.
5. Приобретение студентами теоретических сведений и практических навыков, позволяющих формировать устройства вычислительной техники в защищенном исполнении с заданными техническими характеристиками.

В процессе обучения студент приобретает и совершенствует следующие компетенции:

Общие профессиональные компетенции:

ОПК-4 Способен участвовать в разработке технической документации, связанной с профессиональной деятельностью с использованием стандартов, норм и правил;

Основными **задачами** дисциплины являются:

- формирование целостного компендиума знаний правовых и методических документов в области обеспечения безопасности информационных систем (ИС);
- изучение базовых моделей угроз информационной безопасности и возможных моделей нарушителей для обеспечения проектирования ИС;
- изучение национальных стандартов и методических положений по оценке информационной защищённости при анализе и проектировании защищённых ИС;
- подготовка студентов к деятельности, связанной с созданием, эксплуатацией и обслуживанием (сопровождением) защищённых ИС;
- привитие навыков работы с проектной и технической документацией по проектированию защищённых ИС и оценке их эффективности;
- формирование знаний по проведению аудита информационной безопасности в организации;
- изучение и привитие навыков применения национальных стандартов, нормативных и методических документов в области управления информационной безопасностью;
- формирование представлений о принципах обеспечения информационной безопасности при использовании вычислительной техники;
- изучение принципов построения и работы основных цифровых узлов;

• приобретение опыта выбора элементной базы и типовых цифровых узлов вычислительной техники.

Показатель освоения компетенции отражают следующие индикаторы:

Трудовые действия:

- владеть методами поиска, сбора и обработки, критического анализа и синтеза информации;
- методикой системного подхода для решения поставленных задач;
- методиками разработки цели и задач проекта;
- методами оценки потребности в ресурсах, продолжительности и стоимости проекта;
- навыками работы с нормативно-правовой документацией.

Необходимые умения:

- уметь применять методики поиска, сбора и обработки информации;
- осуществлять критический анализ и синтез информации, полученной из разных источников;
- применять системный подход для решения поставленных задач
- проводить анализ поставленной цели и формулировать задачи, которые необходимо решить для ее достижения;
- анализировать альтернативные варианты для достижения намеченных результатов;
- использовать нормативно-правовую документацию в сфере профессиональной деятельности.

Необходимые знания:

- знать методики поиска, сбора и обработки информации;
- актуальные российские и зарубежные источники информации в сфере профессиональной деятельности;
- метод системного анализа;
- теоретические основы построения систем защиты информации в компьютерных системах;
- виды ресурсов и ограничений для решения профессиональных задач; основные методы оценки разных способов решения задач;
- действующее законодательство и правовые нормы, регулирующие профессиональную деятельность.

2. Место дисциплины (модуля) в структуре ОПОП ВО

Дисциплина «Безопасность информационных систем»» относится к обязательным дисциплинам части Б1.В, формируемой участниками образовательных отношений, основной профессиональной образовательной программы подготовки бакалавров по направлению подготовки 09.03.02 «Информационные системы и технологии».

Дисциплина реализуется кафедрой информационной безопасности.

Изучение данной дисциплины базируется на ранее изученных дисциплинах модуля: «Математика», «Информатика» и компетенциях ОПК1,

ОПК-2, ОПК-5, ОПК-6, ОПК-7, ОПК-8, ПК-2, ПК-3, ПК-4, ПК-6, ПК-11, ПК-14.

3.**Объем дисциплины (модуля) и виды учебной работы**

Общая трудоемкость дисциплины для студентов очной формы составляет 6 зачетных единиц, 216 часов.

Таблица1

Виды занятий	Всего часов	Семестр 5	Семестр 6	Семестр 7	Семестр 9
Общая трудоемкость	**288**		**108**	**180**	**288**
ОЧНАЯ ФОРМА ОБУЧЕНИЯ					
Аудиторные занятия	**112**		**48**	**64**	
Лекции (Л)	**42**		**16**	**26**	
Практические занятия (ПЗ)	**70**		**32**	**38**	
Практическая подготовка	-		-	-	
Самостоятельная работа	**176**		**88**	**88**	
Курсовые работы (проекты)	-		-	-	
Расчетно-графические работы	-		-	-	
Контрольная работа, домашнее задание	+ -		+ -	+ -	
Текущий контроль знаний (7 - 8, 15 - 16 недели)	**тест**		**тест**	**тест**	
Вид итогового контроля	**Экзамен, Зачёт**		**Зачёт**	**Экзамен**	
ЗАОЧНАЯ ФОРМА ОБУЧЕНИЯ					
Аудиторные занятия	**32**				**32**
Лекции (Л)	**16**				**16**
Практические занятия (ПЗ)	**16**				**16**
Практическая подготовка	-				-
Самостоятельная работа	**256**				**256**
Курсовые, расчетно-графические работы	-				-
Контрольная работа, домашнее задание					
Вид итогового контроля	**Экзамен**				**Экзамен**

4. Содержание дисциплины

4.1.Темы дисциплины и виды занятий

Таблица 2

Наименование тем	Лекции, час. Оч/заоч	Практические занятия, Час Оч/заоч	Занятия в интерактивной форме, час Оч/заоч	Код компетенций
Тема 1. Введение в дисциплину безопасность информационных систем	**2/1**	**2/2**	**1/1**	**ОПК-4**
Тема 2. Актуальность проблемы обеспечения информационной безопасности для создаваемых защищенных информационных систем	**6/1**	**8/2**	**3/1**	
Тема 3. Основные угрозы и уязвимости информационных систем, возможные атаки на них	**8/1**	**10/2**	**4/1**	
Тема 4. Комплексное обеспечение информационной безопасности информационных систем. Способы атак на уровне приложений и меры по снижению их уязвимости	**6/1**	**10/2**	**6/0.5**	
Тема 5. Методология формирования задач защиты для объектов информатизации, интеграция средств информационной безопасности в единую технологическую среду построения защищенной ИС	**6/1**	**10/2**	**4/0.5**	
Тема 6. Проектирование комплексной системы защиты информации (КСЗИ) в ИС	**8/1**	**8/2**	**6/0.5**	
Тема 7. Типовая структура КСЗИ от несанкционированного доступа (НСД) в ИС. Концептуальные положения системы менеджмента информационной безопасности	**6/1**	**8/2**	**4/0.5**	

Наименование тем	Лекции, час. Оч/заоч	Практические занятия, Час Оч/заоч	Занятия в интерактивной форме, час Оч/заоч	Код компетенций
применительно к ИС				
Тема 8. Методы и методики оценки качества (эффективности) ИБ при создании защищенных ИС	**6/1**	**8/2**	**4/1**	**ОПК-4**
Итого:	**48/8**	**64/16**	**32/6**	

4.2. Содержание тем дисциплины

Тема 1. Введение в дисциплину безопасность информационных систем

Значение, предмет изучения и краткое содержание дисциплины «Безопасность информационных систем». Место и роль дисциплины в процессе подготовки специалиста, связь с другими дисциплинами. Структура и содержание дисциплины. Виды занятий и контрольных мероприятий.

Названия тем, распределение их по видам аудиторных занятий. Форма проверки знаний. Научная, учебная и периодическая литература по предмету. Рекомендуемая литература. Знания и умения, которые должны быть приобретены студентами в процессе изучения дисциплины. Раскрытие основных понятий применительно к изучению курса. Законодательные акты, регулирующие информационную безопасность информационных (автоматизированных) систем.

Тема 2. Актуальность проблемы обеспечения информационной безопасности для создаваемых защищенных информационных систем

Основные причины обострения проблемы обеспечения информационной безопасности (ИБ) создаваемых защищённых ИС. Для чего необходимо обеспечение ИБ создаваемых защищённых ИС. Какие ИС необходимо защищать.

Тема 3. Основные угрозы и уязвимости информационных систем, возможные атаки на них

Основные угрозы и уязвимости информационных систем, возможные атаки на них. Виды и анализ угроз информационных систем, компьютерные вирусы, технология и способы вторжения в устойчивую работу информационных систем злоумышленников. Уязвимости ИС, возможные атаки на них. Базовые модели угроз для различных типов информационных систем. Особенности построения систем обнаружения атак (СОА) в ИС

Определение понятия угроза. Источники угроз и их характеристики. Перечень значимых угроз, оценка вероятностей их реализации, модель

нарушителя. Назначение этих параметров.

Тема 4. Комплексное обеспечение информационной безопасности информационных систем. Способы атак на уровне приложений и меры по снижению их уязвимости

Постановка проблемы комплексного обеспечения ИБ ИС. Что такое комплексность и почему следует обеспечивать комплексную ИБ для ИС. Отличительные черты обеспечения безопасности информационных систем. Способы атак на уровне приложений и меры по снижению их уязвимости. Исключение атак на уровне приложений.

Тема 5. Методология формирования задач защиты для объектов информатизации, интеграция средств информационной безопасности в единую технологическую среду построения защищенной ИС

Методология формирования задач защиты для объектов информатизации, интеграция средств информационной безопасности в единую технологическую среду построения защищенной ИС

Тема 6. Проектирование комплексной системы защиты информации (КСЗИ) в ИС

Этапы проектирования комплексной системы информационной безопасности ИС и требования к ним: предпроектное обследование, техническое задание, техническое проектирование, рабочее проектирование, испытания и внедрение в эксплуатацию, сопровождение при создании защищенных ИС.

Тема 7. Типовая структура КСЗИ от несанкционированного доступа (НСД) в ИС. Концептуальные положения системы менеджмента информационной безопасности применительно к ИС

Структура КСЗИ от НСД в ИС. Подсистемы КСЗИ. Подсистема контроля доступа. Подсистема охранно-пожарной сигнализации. Подсистема автоматического пожаротушения. Подсистема контроля параметров окружающей среды. Подсистема обеспечения бесперебойного энергоснабжения. Подсистема видеонаблюдения. Подсистема ИБ. Подсистема антивирусной защиты. Подсистема парольной защиты. Подсистема защиты электронных документов. Подсистема ИБ локальной вычислительной сети (ЛВС). Подсистема защиты систем и каналов связи. Подсистема ИБ технологий обработки информации. Подсистема ИБ фонда алгоритмов и программ (ФАП). Центр управления ключевыми системами.

Подсистема аудита ИБ. Структура документации системы менеджмента информационной безопасности в организации. Модель PDCA.

Алгоритм и матрица оценки рисков при обеспечении информационной безопасности в организации. Варианты обработки рисков.

Требования, предъявляемые к формированию политики безопасности организации. Структура и содержание политики безопасности организации применительно к компьютерным системам.

Тема 8. Методы и методики оценки качества (эффективности) ИБ при создании защищенных ИС

Что понимают под эффективностью ИБ при создании защищённых ИС и её оценкой. Какие существуют основные методы и методики оценки качества (эффективности) ИБ при создании защищенных ИС. Количественная и качественная оценка эффективности ИБ при создании защищенных ИС.

5. Перечень учебно-методического обеспечения для самостоятельной работы по дисциплине (модулю)

Методические указания для самостоятельной работы обучающихся по освоению дисциплины представлены в Приложении 2.

6. Фонд оценочных средств для проведения промежуточной аттестации обучающихся по дисциплине (модулю)

Структура фонда оценочных средств для проведения промежуточной аттестации обучающихся по дисциплине приведена в Приложении 1.

7. Перечень основной и дополнительной учебной литературы, необходимой для освоения дисциплины (модуля)

Основная литература:

1. Бирюков А. Информационная безопасность / А. Бирюков . - Москва : ДМК Пресс, 2017. - с. URL: https://e.lanbook.com/book/93278
2. Рябко Б.Я., Фионов А.Н. Основы современной криптографии и стеганографии – 2-е издание- М.: Горячая линия – Телеком, 2013. – 232с.

Дополнительная литература:

1. Гришина Н.В.Информационная безопасность предприятия : учебное пособие / Н.В. Гришина. - 2-е изд., доп. - М. ; М. : ФОРУМ : НИЦ ИНФРА-М, 2015. - 240 с. - (Высшее образование - бакалавриат)
2. Кияев, В. Безопасность информационных систем / В. Кияев; О. Граничин. - Москва : Национальный Открытый Университет «ИНТУИТ», 2016. - 192 с. URL: http://biblioclub.ru/index.php?page=book&id=429032

Рекомендуемая литература

1. В.А.Северин. Комплексная защита информации на предприятии. М.: Издательский дом «Городец»,2008.- 368с.

2. Мельников В.П. идр Информационная безопасность.М.: Издателский центр «Академия» , 2008.-336с.
3. А.И. Баранчиков, П.А. Баранчиков, А.Н. Пылькин Алгоритмы и модели ограничения доступа к записям баз данных. - М. Горячая линия – Телеком, 2011 – 182с.
4. А.Ф. Чепига Информационная безопасность автоматизированных систем. М.: «Гелиос АРВ», 2010. -336с.
5. В.Ф. Шаньгин Комплексная защита информации в корпоративных системах. М.: ИД «Форум»: ИНФРА-М., 2010.-592с.
6. О.А.Романов, С.А. Бабин, С.Г. Жданов Организационное обеспечение информационной безопасности М.: Издательский центр «Академия», 2008,-192.
7. Васильков А.В., Васильков А.А., Васильков И.А. Информационные системы и их безопасность М.: ФОРУМ, 2011,-528с.

8. Перечень ресурсов информационно-телекоммуникационной сети интернет, необходимых для освоения дисциплины (модуля)

1. ISO27000.ru (портал по ИБ, аналитика, информация по законодательству и стандартам, блоги, каталоги ресурсов и ПО).
2. wikIsec - Энциклопедия ИБ (публикации, статьи).
3. WinSecurity.ru (статьи, документация, новости по безопасности Windows).
4. Журнал Информационная безопасность (публикации, статьи, обзоры, форум).
5. http://www.minfin.ru - официальный сайт Министерства финансов Российской Федерации.
6. http://www.gov.ru - сервер органов государственной власти Российской Федерации.

9. Методические указания для обучающихся по освоению дисциплины (модуля)

Методические указания для обучающихся, по освоению дисциплины, приведены в Приложении 2.

10. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине (модуля)

Перечень программного обеспечения: *MSOffice, ПО комплекса «Основы компьютерно-информационной безопасности»*

Информационные справочные системы:

1. Ресурсы информационно-образовательной среды МГОТУ.
2. Рабочая программа и методическое обеспечение по дисциплине: «Безопасность информационных систем»

11. Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине

Лекционные занятия:

- аудитория, оснащенная презентационной техникой (проектор, экран);
- комплект электронных презентаций/слайдов.

Практические занятия:

- компьютерный класс с проектором для интерактивного обучения и проведения занятий в форме слайд-презентаций, оборудованный современными лицензионными программно-техническими средствами: операционная система не ниже WindowsXP, эмуляции виртуальных машин (VM-vare, VM-box или др.)
- рабочее место преподавателя, оснащенное компьютером с доступом в Интернет;
- рабочие места студентов, оснащенные компьютерами с доступом в Интернет.

Приложение 1
Фонд оценочных средств для проведения промежуточной аттестации обучающихся по дисциплине

ИНСТИТУТ
ИНФОКОММУНИКАЦИОННЫХ СИСТЕМ И ТЕХНОЛОГИЙ

КАФЕДРА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ДЛЯ ПРОВЕДЕНИЯ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ОБУЧАЮЩИХСЯ ПО ДИСЦИПЛИНЕ
БЕЗОПАСНОСТЬ ИНФОРМАЦИОННЫХ СИСТЕМ
(Приложение 1 к рабочей программе)

Направление подготовки: 09.03.02 Прикладная информатика
Профиль: Прикладная информатика в системах управления
Уровень высшего образования: бакалавриат
Форма обучения: очная, заочная

Королев
2021

Перечень компетенций с указанием этапов их формирования в процессе освоения образовательной программы

№ п/п	Индекс компе-тенции	Содержание компетенции (или ее части)*	Раздел дисциплины, обеспечивающий формирование компетенции (или ее части)	В результате изучения раздела дисциплины, обеспечивающего формирование компетенции (или ее части), обучающийся приобретает:		
				Трудовые действия	Необходимые умения	Необходимые знания
1	ОПК-4	Способен участвовать в разработке технической документации, связанной с профессиональной деятельностью с использованием стандартов, норм и правил	Тема 1-8	Владеть методами поиска, сбора и обработки, критического анализа и синтеза информации; методикой системного подхода для решения поставленных задач	Уметь применять методики поиска, сбора и обработки информации; осуществлять критический анализ и синтез информации, полученной из разных источников; применять системный подход для решения поставленных задач	Знать методики поиска, сбора и обработки информации; актуальные российские и зарубежные источники информации в сфере профессиональной деятельности; метод системного анализа. .

2.Описание показателей и критериев оценивания компетенций на различных этапах их формирования, описание шкал оценивания

Код компетенции	Инструменты, оценивающие сформированность компетенции	Показатель оценивания компетенции	Критерии оценки
ОПК-4	Доклад в форме презентации	А) полностью сформирована (компетенция освоена на высоком уровне) – 5 баллов Б) частично сформирована: •компетенция освоена на продвинутом уровне – 4 балла; •компетенция освоена на базовом уровне – 3 балла; В) не сформирована (компетенция не освоена) – 2 и менее баллов	Проводится устно с использованием мультимедийных систем, а также с использованием технических средств Время, отведенное на процедуру – 10 - 15 мин. Неявка – 0. Критерии оценки: 1.Соответствие представленной презентации заявленной тематике (1 балл). 2.Качество источников и их количество при подготовке доклада и разработке презентации (1 балл). 3.Владение информацией и способность отвечать на вопросы аудитории (1 балл). 4.Качество самой представленной презентации (1 балл). 5.Оригинальность подхода и всестороннее раскрытие выбранной тематики (1 балл). Максимальная сумма баллов - 5 баллов. Результаты оценочной процедуры представляются обучающимся непосредственно в день проведения презентации – для текущего контроля. Оценка проставляется в электронный журнал.
ОПК-4	Доклад в форме презентации	А) полностью сформирована (компетенция освоена на высоком уровне) – 5 баллов Б) частично сформирована: •компетенция освоена на продвинутом уровне – 4 балла; •компетенция	Проводится устно с использованием мультимедийных систем, а также с использованием технических средств Время, отведенное на процедуру – 10 - 15 мин. Неявка – 0. Критерии оценки: 1.Соответствие представленной презентации заявленной тематике (1

Код компетенции	Инструменты, оценивающие сформированность компетенции	Показатель оценивания компетенции	Критерии оценки
		освоена на базовом уровне – 3 балла; В) не сформирована (компетенция не освоена) – 2 и менее баллов	балл). 2.Качество источников и их количество при подготовке доклада и разработке презентации (1 балл). 3.Владение информацией и способность отвечать на вопросы аудитории (1 балл). 4.Качество самой представленной презентации (1 балл). 5.Оригинальность подхода и всестороннее раскрытие выбранной тематики (1 балл). Максимальная сумма баллов - 5 баллов. Результаты оценочной процедуры представляются обучающимся непосредственно в день проведения презентации – для текущего контроля. Оценка проставляется в электронный журнал.
ОПК-4	Контрольная работа	**А) полностью сформирована** (компетенция освоена на высоком уровне) – 5 баллов **Б) частично сформирована:** •компетенция освоена на **продвинутом уровне** – 4 балла; •компетенция освоена **на базовом уровне** – 3 балла; **В) не сформирована** (компетенция не освоена) – 2 и менее баллов	Проводится в форме письменной контрольной работы (электронный документ). Время, отведенное на процедуру – 40 - 60 мин. Неявка – 0. Критерии оценки: 1.Соответствие содержания контрольной работы заявленной тематике (1 балл). 2.Качество источников и их количество при подготовке работы (1 балл). 3.Владение информацией и способность отвечать на вопросы аудитории (1 балл). 4.Качество самой представленной работы (1 балл). 5.Оригинальность подхода и всестороннее раскрытие выбранной тематики (1 балл). Максимальная сумма баллов

Код компетенции	Инструменты, оценивающие сформированность компетенции	Показатель оценивания компетенции	Критерии оценки
			- 5 баллов. Результаты оценочной процедуры представляются обучающимся в срок не позднее 1 недели после проведения процедуры – для текущего контроля. Оценка проставляется в электронный журнал.

3. Типовые контрольные, практические задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций в процессе освоения образовательной программы

Тематика докладов в презентационной форме:

1. Информационная безопасность сетевого периметра организации на основе применения технологии «тонкого клиента».
2. Информационная безопасность системы «клиент – банк» на основе технологии «толстого клиента».
3. Базовая модель угроз для информационных систем, обрабатывающих персональные данные.
4. Базовая модель угроз для государственных информационных систем.
5. Возможные модели нарушителей сетевого периметра организации.
6. Информационная безопасность модели Интернет - банкинга.
7. Информационная безопасность расчетов банковскими картами в Интернете.
8. Управление информационной безопасностью в организации.
9. Оценка и обработка рисков информационной безопасности.
10. Управление рисками информационной безопасности.
11. Документальное и инструментальное обеспечение управления рисками информационной безопасности.
12. Классификация технических каналов утечки информации для информационных систем.
13. Физическая природа побочных электромагнитных излучений в технических средствах обработки информации.
14. Наводки электромагнитных излучений при обработке информации в информационных системах.

15. Технические каналы утечки информации при передаче ее по каналам связи.
16. Средства выявления каналов утечки информации.
17. Технический контроль эффективности мер защиты информации.
18. Скрытие и защита информации от утечки по техническим каналам.
19. Защита информационных систем от несанкционированного доступа.
20. Классификация АС, СВТ и МЭ по требованиям защиты информации от несанкционированного доступа.
21. Классификация ПО по уровню контроля отсутствия не декларированных возможностей.
22. Схема защищенного информационного обмена при использовании симметричных методов защиты информации.
23. Схема защищенного информационного обмена при использовании криптографических алгоритмов с открытыми ключами.
24. Место ЭЦП в ряду криптографических механизмов. История возникновения ЭЦП в России. Общее правило создания ЭЦП. Общее правило верификации ЭЦП.
25. Применение и информационная безопасность режима электронной кодовой книги. Режима сцепления блоков шифротекста. Режима обратной связи по шифротексту.
26. Функция хеширования и асиметричные алгоритмы.
27. Информационная безопасность и защита электронных транзакций протокол (SSL). Схема работы протокола SET.
28. Информационная безопасность и правила обмена электронными документами. Общие требования, предъявляемые к ЭД (пакетам ЭД).
29. Информационная безопасность при составление и направление ЭД участником – отправителем.
30. Информационная безопасность и порядок контроля ЭД, полученных от участников – отправителей. Порядок оформления ЭД, подтверждающих исполнение ЭД участников.
31. Информационная безопасность и порядок приема к исполнению ЭД участником – получателем. Порядок хранения и уничтожения ЭД.

Тематика заданий на контрольную работу:

1. Общая характеристика принципов, методов и механизмов обеспечения компьютерной безопасности. Основы обеспечения безопасности информации в компьютерных системах.

2. Исследование объекта защиты информации и анализ его защищённости по видам угроз, классам каналов несанкционированного по-

лучения информации, причинам нарушения целостности информации и потенциально возможным злоумышленным действиям.

3. Проектирование архитектуры системы защиты информации выбранного объекта и оценка его уровня защищённости.

4. Виды и анализ угроз автоматизированных систем, компьютерные вирусы, технология и способы вторжения в устойчивую работу автоматизированных систем злоумышленников.

5. Совершенствование системы защиты информации предприятия (фирмы) на основе комплексного применения современных средств защиты информации.

6. Разработка и обоснование требований к системе защиты информации предприятия (фирмы) и рекомендаций по её эффективному наращиванию.

7. Направления повышения эффективности существующей системы защиты и методика применения средств защиты информации на выбранных объектах исследования.

8. Разработка проекта создания системы защиты информации на выбранных типовых офисных объектах.

9. Основные виды атак на компьютерные системы (КС), их классификация.

10. Проблемы обеспечения информационной безопасности в проводных КС.

11. Беспроводной доступ к локальным сетям. Угрозы и уязвимости в беспроводных компьютерных системах.

12. Компьютерная преступность в экономических областях.

13. Компьютерные вирусы в современных информационных системах.

14. Информационные угрозы современным экономическим объектам.

15. Безопасность информации в коммерческой деятельности.

16. Становление и развитие промышленного шпионажа.

17. Модель распространения прав доступа Take-Grant. Цель использования модели Take-Grant. Основные элементы модели Take-Grant. Формальное описание модели Take-Grant.

18. Описание систем защиты с помощью матрицы доступа. Таблицы, описывающие права доступа субъектов к объектам. Описание модели Харрисона-Руззо-Ульмана (HRU).

19. Направления повышения эффективности существующей системы защиты и методика применения средств защиты информации на выбранных объектах исследования.

20. Общий подход к построению систем, реализующих мандатную (полномочную) политику безопасности в модели BL (Белла-Лападулы).

21. Назначение модели Белла-Лападулы. Описание модели Белла-Лападулы (BL). Основная теорема безопасности модели Белла-Лападулы.

22. ЭЦП и проблемы безопасности.

23. Методики оценки защиты информации.

24. Защита информации в социальных сетях.

25. Информационная безопасность виртуальных сетей.

4. Методические материалы, определяющие процедуры оценивания знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций

Формой контроля знаний по дисциплине «Безопасность информационных систем» являются две текущие аттестации в виде тестов в течение каждого семестра и промежуточная аттестация в виде зачета (5 семестр) и экзамена (6 семестр).

Неделя текущего контроля	Вид оценочного средства	Код компетенций, оценивающий знания, умения, навыки	Содержание оценочного средства	Требования к выполнению	Срок сдачи (неделя семестра)	Критерии оценки по содержанию и качеству с указанием баллов
7-8 (4-й семестр)	тестирование	ОПК-4	20 вопросов	Компьютерное тестирование ; время отведенное на процедуру - 30 минут	Результаты тестирования предоставляются в день проведения процедуры	Критерии оценки определяются процентным соотношением. Не явка - Удовлетворительно - от 51% правильных ответов. Хорошо - от 70%. Отлично – от 90%.
15-16 (4-й семестр)	тестирование	ОПК-4	20 вопросов	Компьютерное тестирование; время отведенное на процедуру – 30 минут	Результаты тестирования предоставляются в день проведения процедуры	Критерии оценки определяются процентным соотношением. Не явка -0 Удовлетворительно - от 51%

Неделя текущего контроля	Вид оценочного средства	Код компетенций, оценивающий знания, умения, навыки	Содержание оценочного средства	Требования к выполнению	Срок сдачи (неделя семестра)	Критерии оценки по содержанию и качеству с указанием баллов
						правильных ответов. Хорошо - от 70%. Отлично – от 90%. Максимальная оценка – 5 баллов.
(4-й семестр)	Экзамен	ОПК-4	3 вопроса	Экзамен проводится в письменной форме, путем ответа на вопросы. Время, отведенное на процедуру – 30 минут.	Результаты предоставляются в день проведения экзамена	Критерии оценки: «**Отлично**»: 1. знание основных понятий предмета; 2. умение использовать и применять полученные знания на практике; 3. работа на практических занятиях; 4. знание основных научных теорий, изучаемых предметов; 5. ответ на вопросы билета. «**Хорошо**»: • знание основных понятий предмета; • умение использовать и применять полученные знания на практике;

Неделя текущего контроля	Вид оценочного средства	Код компетенций, оценивающий знания, умения, навыки	Содержание оценочного средства	Требования к выполнению	Срок сдачи (неделя семестра)	Критерии оценки по содержанию и качеству с указанием баллов
						• работа на практических занятиях; • знание основных научных теорий, изучаемых предметов; • ответы на вопросы билета • неправильно решено практическое задание «У**довлетворительно**»: 1.демонстрирует частичные знания по темам дисциплин; 2. незнание неумение использовать и применять полученные знания на практике; 3. не работал на практических занятиях; «**Неудовлетворительно**»: 1.демонстрирует частичные знания по темам дисциплин; 2. незнание основных понятий предмета; 3. неумение использовать и

Неделя текущего контроля	Вид оценочного средства	Код компетенций, оценивающий знания, умения, навыки	Содержание оценочного средства	Требования к выполнению	Срок сдачи (неделя семестра)	Критерии оценки по содержанию и качеству с указанием баллов
						применять полученные знания на практике; 4. не работал на практических занятиях; 5. не отвечает на вопросы.

4.1. Типовые вопросы, выносимые на тестирование

Тесты используются в режиме промежуточного контроля. По форме заданий выбраны закрытые тесты (с выборочным ответом). Каждому вопросу соответствует один вариант ответа.

1. Функции КСЗИ:
   создание механизмов защиты, сводящие до минимума возможность воздействия дестабилизирующих факторов на защищаемую информацию; непрерывное и оптимальное управление механизмами комплексной защиты +
   обеспечение конфиденциальности, целостности, доступности информации
   обеспечение криптографической, программной и аппаратной защиты информации
   обеспечение защиты людей, материальных носителей, автоматизированных систем
2. Требование безопасности повторного использования объектов противоречит:
   инкапсуляции +
   наследованию
   полиморфизму
3. Уровни модели OSI, по возрастанию:
   физический, канальный, сетевой, транспортный, сеансовый, представления, прикладной +
   сетевой, канальный, транспортный, сеансовый, прикладной, представления, физический
   прикладной, представления, физический, канальный, сетевой, транспортный, сеансовый

физический, сетевой, канальный, транспортный, сеансовый, представления, прикладной

4. Предположим, что при разграничении доступа учитывается семантика программ. В таком случае на игровую программу могут быть наложены следующие ограничения:
   запрет на чтение каких-либо файлов, кроме конфигурационных
   запрет на изменение каких-либо файлов, кроме конфигурационных +
   запрет на установление сетевых соединений
5. Уровни модели TCP/IP, по возрастанию:
   канальный, сетевой, транспортный, прикладной +
   транспортный, канальный, сетевой, прикладной
   канальный, транспортный, сетевой, прикладной
   прикладной, сетевой, транспортный, канальный
6. К какому уровню модели TCP\IP относятся следующие протоколы HTTP, RTP, FTP, DNS:
   прикладной +
   транспортный
   сетевой
   канальный
7. В число граней, позволяющих структурировать средства достижения информационной безопасности, входят:
   меры обеспечения целостности
   административные меры +
   меры административного воздействия
8. Что входит в функции систем мониторинга:
   выявление состояния систем
   установка отношений между объектами
   установка соответствия правил и обязанностей
   все варианты верны +
9. Какие существуют подходы по построению защищенных операционных систем применяемых в АС:
   фрагментарный и комплексный +
   фрагментарный и операционный.
   комплексный и позиционный.
   системный и позиционный.
10. Дублирование сообщений является угрозой:
    доступности
    конфиденциальности
    целостности +
11. Какие существуют методы оценки качества КСИБ:
    метод оценки уязвимости Хоффмана +
    экспертная оценка +
    сигнатурный метод
    качественный метод.
12. Самыми опасными источниками внутренних угроз являются:
    некомпетентные руководители +

обиженные сотрудники
любопытные администраторы

13. Для внедрения бомб чаще всего используются ошибки типа:
отсутствие проверок кодов возврата
переполнение буфера +
нарушение целостности транзакций
14. В число целей политики безопасности верхнего уровня входят:
решение сформировать или пересмотреть комплексную программу безопасности +
обеспечение базы для соблюдения законов и правил +
обеспечение конфиденциальности почтовых сообщений
15. В число целей программы безопасности верхнего уровня входят:
управление рисками +
определение ответственных за информационные сервисы
определение мер наказания за нарушения политики безопасности
16. Что означает обеспечение целостности баз данных.

это соответствие информации базы данных её внутренней логике, структуре и заданным правилам. +
это полное значение информации базы данных в котором действуют установленные правила
это информация, работающая по установленной структуре базы данных.
это логическая операция обеспечивающая полноту информации и соблюдающая условия того, что информация не будет изменена.
17. В рамках программы безопасности нижнего уровня осуществляются:
стратегическое планирование
повседневное администрирование +
отслеживание слабых мест защиты +
18. Политика безопасности строится на основе:
общих представлений об ИС организации
изучения политик родственных организаций
анализа рисков +
19. В число целей политики безопасности верхнего уровня входят:
формулировка административных решений по важнейшим аспектам реализации программы безопасности +
выбор методов аутентификации пользователей
обеспечение базы для соблюдения законов и правил +
20. Основные механизмы защиты применяемые в ОС:
идентификации / аутентификации
разграничения доступа
аудита
все перечисленные варианты верны. +

4.3. Типовые вопросы, выносимые на экзамен (4 семестр)

1. Предмет, цель и задачи обеспечения информационной безопасности в организации.
2. Дайте определение конфигурации информационных ресурсов компьютерных систем, в чем заключается их администрирование.
3. Дайте определение и приведите классификацию угроз безопасности информации для информационных систем.
4. Выбор мер защиты информации для их реализации в информационной системе в рамках ее системы защиты информации.
5. Идентификация и аутентификация субъектов доступа и объектов доступа.
6. Управление доступом субъектов доступа к объектам доступа.
7. Ограничение программной среды в защищенных АС.
8. Защита машинных носителей информации в АС.
9. Регистрация событий безопасности в информационной системе.
10. Антивирусная защита в информационной системе.
11. Обнаружение (предотвращение) вторжений в информационную систему.
12. Контроль защищенности информации в информационной системе.
13. Обеспечение целостности информационной системы и информации
14. Обеспечение доступности информации в информационной системе.
15. Защита информационной системы, ее средств и систем связи и передачи данных.
16. Классификация СВТ по уровню защищённости от НСД к информации. Перечень показателей защищённости СВТ и совокупности описывающих их требований. Характеристика классов защищённости СВТ от НСД к информации.
17. Виды и анализ угроз автоматизированных систем, компьютерные вирусы, технология и способы вторжения в устойчивую работу автоматизированных систем злоумышленников.
18. Базовая модель угроз ИСПДн.
19. Уязвимости АС, возможные атаки на них.
20. Классификация АС, подлежащих защите от НСД к информации. Требования по защите информации в АС различных классов. Этапы классификации АС. Исходные данные для классификации АС. Выбор класса защищённости АС.
21. Структура документации системы менеджмента информационной безопасности в организации. Модель PDCA.
22. Алгоритм и матрица оценки рисков при обеспечении информационной безопасности в организации. Варианты обработки рисков.
23. Классификация методов криптографического закрытия информации.
24. Аппаратные и программные средства реализации шифров.
25. Особенности использования вычислительной техники в криптографии; вопросы организации сетей связи с аппаратурой шифрования; ключевые системы.
26. Организация защиты в распределенных сетях с использованием виртуальных частных сетей.

27. Электронные цифровые подписи (электронные подписи).
28. Криптографические хеш-функции.
29. Криптографические протоколы.
30. Основные подходы к реализации PKI.
31. Симметричные криптосистемы.
32. Симметричные методы шифрования.
33. Алгоритмы блочного шифрования.
34. Режимы применения блочных шифров.
35. Потоковые шифры.
36. Комбинированные методы шифрования.
37. Асимметричные системы шифрования.
38. Применение асимметричных алгоритмов.
39. Средства криптографической защиты, разработанные компаниями: Инфотекс, Крипто-Про, ОКБ Сапр, Аладдин и Adobe, MS Windows, Cisco.
40. Хранилище сертификатов ОС MS Windows.
41. Перечислите защитные механизмы, реализуемые программно-аппаратными комплексами (средствами) защиты информации в компьютерных системах (ПЭВМ). Дайте определение понятию - «субъект доступа», какие процедуры реализуются при его обращении к компьютерной системе.
42. Перечислите методы противодействия дизассемблированию программ для ЭВМ, охарактеризуйте их.
43. В чем заключается процедура простой аутентификации, какими способами она производится, поясните схематично ее реализацию с использованием пароля.
44. Перечислите основные модели разграничения доступа, действующие в операционных системах, и поясните, в чем они заключаются. Дайте определение понятиям «матрица доступа» и «домен безопасности».
45. Поясните использование односторонней хэш-функции для проверки пароля при аутентификации пользователя ресурсов компьютерной системы.
46. Чем достигается защита средств управления, коммутации и внутреннего монтажа компьютерных систем (ПЭВМ), из чего состоит и как действует единая система контроля вскрытия устройств (СКВУ).
47. Для чего создается система разграничения доступа (СРД) компьютерной системы, какие функциональные блоки она включает. Поясните работу функциональной схемы диспетчера доступа.
48. В чем заключается биометрическая аутентификация пользователей, какие у нее достоинства и недостатки.
49. Дайте определение основным понятиям процесса разграничения доступа к объектам операционной системы (ОС): «объект доступа»; «метод доступа»; «субъект доступа»; «право доступа». Каким требованиям должны удовлетворять правила разграничения доступа.
50. Приведите примеры сущностей субъекта доступа для подтверждения своей подлинности при осуществлении аутентификации в компьютерной системе (ПЭВМ).

51. Какими способами блокируется угроза несанкционированного копирования информации ПЭВМ, в чем они заключаются, раскройте их содержание.

52. В зависимости от предъявления субъектом доступа каких сущностей можно разделить процессы аутентификации в компьютерных системах (ПЭВМ)?

53. Основные подходы к защите данных от НСД: какие действия выполняются при организации доступа к оборудованию и ПО компьютерных систем (ПЭВМ); оценка эффективности наращивания средств контроля доступа по кривой роста относительного уровня обеспечения безопасности компьютерных систем (ПЭВМ).

54. Перечислите атрибутивные идентификаторы, используемые для идентификации субъекта доступа в КС, и коротко дайте им определение.

55. Какие основные функции выполняет подсистема защиты операционных систем (ОС), дайте коротко им определение. В чем заключается процедура аудита применительно к ОС, чем она обусловлена, каким требованиям она должна удовлетворять.

56. Какую последовательность действий включает общий алгоритм механизма защиты от несанкционированного использования программ в «чужой» среде.

57. Раскройте методы аутентификации, использующие пароли и PIN-коды.

58. Перечислите и раскройте способы строгой аутентификации.

59. Какие существуют криптосистемы шифрования, раскройте их смысл функционирования.

60. Раскройте основные процедуры формирования электронной цифровой подписи и функции хэширования.

61. Как осуществляется управление криптоключами, требования к распределению ключей, методы распределения ключей.

62. Раскройте классификацию и жизненный цикл компьютерных вирусов.

63. Перечислите методы ограничения доступа к компонентам ЭВМ, какие применяют средства для ограничения доступа к компонентам ЭВМ.

64. В чем заключается задача идентификации пользователя, дайте определение понятию протокола идентификации.

65. В чем заключается локальная и удаленная идентификация, что такое идентифицирующая информация.

66. Какие существуют способы хранения идентифицирующей информации, их связь с ключевыми системами.

1.

Приложение 2
Методические указания для обучающихся по освоению дисциплины

ИНСТИТУТ
ИНФОКОММУНИКАЦИОННЫХ СИСТЕМ И ТЕХНОЛОГИЙ

КАФЕДРА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ БЕЗОПАНОСТЬ ИНФОРМАЦИОННЫХ СИСТЕМ

(Приложение 2 к рабочей программе)

Направление подготовки: 09.03.02 Прикладная информатика
Профиль: Прикладная информатика в системах управления
Уровень высшего образования: бакалавриат
Форма обучения: очная, заочная

Королев
2021

1. Общие положения

Цель дисциплины:

- формирование базовых знаний и практических навыков обеспечения безопасности информационных систем;
- развитие творческого и исследовательского подхода к изучению технических дисциплин студенчества;
- подготовка студентов к видам профессиональной деятельности: проектной, производственно-технологической, организационно-управленческой, аналитической и научно-исследовательской;
- приобретение студентами знаний и представлений об основных принципах и закономерностях функционирования современной вычислительной техники;
- приобретение студентами теоретических сведений и практических навыков, позволяющих формировать устройства вычислительной техники с заданными техническими характеристиками.

Задачи дисциплины:

- формирование целостного компендиума знаний правовых и методических документов в области обеспечения безопасности информационных систем (ИС);
- изучение базовых моделей угроз информационной безопасности и возможных моделей нарушителей для обеспечения проектирования ИС;
- изучение национальных стандартов и методических положений по оценке информационной защищённости при анализе и проектировании защищённых ИС;
- подготовка студентов к деятельности, связанной с созданием, эксплуатацией и обслуживанием (сопровождением) защищённых ИС;
- привитие навыков работы с проектной и технической документацией по проектированию защищённых ИС и оценке их эффективности.
- формирование знаний по проведению аудита информационной безопасности в организации;
- изучение и привитие навыков применения национальных стандартов, нормативных и методических документов в области управления информационной безопасностью;
- формирование представлений о принципах обеспечения информационной безопасности при использовании вычислительной техники;
- изучение принципов построения и работы основных цифровых узлов;
- приобретение опыта выбора элементной базы и типовых цифровых узлов вычислительной техники.

2. Указания по проведению практических занятий

Практическое занятие 1. **Предмет и задачи программно-аппаратной защиты информации.**

Образовательные технологии: технология формирования ключевых компетентностей.

Вид практического занятия: смешанная форма практического занятия.

Учебные вопросы:

1. Компьютерная система (КС). Структура и компоненты КС. Классы и типы КС. Сети ЭВМ.
2. Основные понятия программно-аппаратной защиты информации: электронный документ (ЭД) и их типы; виды информации в КС; информационные потоки в КС; понятие исполняемого модуля.
3. Уязвимость компьютерных систем: понятие доступа, субъект и объект доступа; понятие несанкционированного доступа (НСД); классы и виды НСД; несанкционированное копирование программ как особый вид НСД; понятие злоумышленника; злоумышленник в криптографии и при решении проблем компьютерной безопасности (КБ).

Практическое занятие 2. **Идентификация пользователей КС - субъектов доступа к данным.**

Образовательные технологии: технология активного метода обучения.

Вид практического занятия: смешанная форма практического занятия.

Учебные вопросы:

1. Понятие идентификации пользователя.
2. Задача идентификации пользователя.
3. Понятие протокола идентификации.
4. Локальная и удаленная идентификация.
5. Идентифицирующая информация. Понятие идентифицирующей информации.
6. Способы хранения идентифицирующей информации, связь с ключевыми системами.

Практическое занятие 3. **Средства и методы ограничения доступа к файлам.**

Образовательные технологии: технология проблемного обучения.

Вид практического занятия: смешанная форма практического занятия.

Учебные вопросы:

1. Основные подходы к защите данных от НСД: шифрование; контроль доступа; разграничения доступа; файл как объект доступа; оценка надежности систем ограничения доступа - сведение к задаче оценки стойкости.
2. Организация доступа к файлам: иерархический доступ к файлам; понятие атрибутов доступа; организация доступа к файлам в различных ОС; защита сетевого файлового ресурса на примерах организации доступа в ОС UNIX, Novell NetWare и т. д.

3. Фиксация доступа к файлам: способы фиксации фактов доступа; журналы доступа; критерии информативности журналов доступа; выявление следов несанкционированного доступа к файлам; метод инициированного НСД.

4. Доступ к данным со стороны процесса: понятие доступа к данным со стороны процесса; отличия от доступа со стороны пользователя; понятие и примеры скрытого доступа; надежность систем ограничения доступа.

5. Особенности защиты данных от изменения: зашита массивов информации от изменения (имитозащита); криптографическая постановка защиты от изменения данных; подходы к решению задачи защиты данных от изменения; подход на основе формирования имитоприставки (MAC), способы построения MAC; подход на основе формирования хэш-функции, требования к построению и способы реализации; формирование электронной цифровой подписи (ЭЦП); особенности защиты ЭД и исполняемых файлов; проблема самоконтроля исполняемых модулей.

Практическое занятие 4. Программно-аппаратные средства шифрования

Образовательные технологии: технология развивающего обучения.

Вид практического занятия: смешанная форма практического занятия.

Учебные вопросы:

1. Построение программно-аппаратных комплексов шифрования: аппаратные и программно-аппаратные средства криптозащиты данных; построение аппаратных компонент криптозащиты данных, специализированные СБИС как носители алгоритма шифрования.

2. Защита алгоритма шифрования, принцип чувствительной области и принцип главного ключа.

3. Необходимые и достаточные функции аппаратного средства криптозащиты, проектирование модулей криптопреобразований на основе сигнальных процессоров.

4. Плата Криптон-3 (Криптон-4): архитектура платы; организация интерфейса с приложениями. 5. Другие программно-аппаратные СКЗД.

Практическое занятие 5. Защита программ от несанкционированного копирования

Образовательные технологии: технология проблемно-модульного обучения.

Вид практического занятия: смешанная форма практического занятия.

Учебные вопросы:

1. Несанкционированное копирование программ: несанкционированное копирование программ как тип НСД; юридические аспекты несанкционированного копирования программ; общее понятие защиты от копирования. Разновидности задач защиты от копирования.

2. Подходы к задаче защиты от копирования: привязка ПО к аппаратному окружению и физическим носителям как единственное средство защиты от копирования ПО; привязка программ к гибким магнитным дискам

(ГМД); структура данных на ГМД; управление контроллером ГМД; способы создания некопируемых меток; точное измерение характеристик форматирования дорожки; технология «слабых битов»; физические метки и технология работы с ними; привязка программ к жестким магнитным дискам (ЖМД); особенности привязки к ЖМД; виды меток на ЖМД; привязка к прочим компонентам штатного оборудования ПЭВМ; привязка к внешним (добавляемым) элементам ПЭВМ; привязка к портовым ключам; использование дополнительных плат расширения; методы «водяных знаков» и методы «отпечатков пальцев».

Практическое занятие 6. Защита программ от изучения

Образовательные технологии: технология проблемно-модульного обучения.

Вид практического занятия: смешанная форма практического занятия.

Учебные вопросы:

1. Изучение и обратное проектирование ПО: понятие изучения и обратного проектирования ПО; цели и задачи изучения работы ПО; способы изучения ПО: статическое и динамическое изучение; роль программной и аппаратной среды; временная надежность (невозможность обеспечения гарантированной надежности).
2. Задачи защиты от изучения и способы их решения: защита от отладки; динамическое преобразование кода; итеративный программный замок А. Долгина; принцип ловушек и избыточного кода; защита от дизассемблирования; принцип внешней загрузки файлов; динамическая модификация программы; защита от трассировки по прерываниям.
3. Аспекты проблемы защиты от исследования: способы ассоциирования защиты и программного обеспечения; оценка надежности защиты от отладки.
4. Вирусы: защита от разрушающих программных воздействий; вирусы как особый класс разрушающих программных воздействий; необходимые и достаточные условия недопущения разрушающего воздействия; понятие изолированной программной среды.

Тема № 7. Концептуальные положения системы менеджмента информационной безопасности применительно к компьютерным системам

Практическое занятие 7

Образовательные технологии: технология проблемно-модульного обучения.

Вид практического занятия: смешанная форма практического занятия.

Тема и содержание практического занятия: Структура документации системы менеджмента информационной безопасности в организации. Модель PDCA. Алгоритм и матрица оценки рисков при обеспечении информационной безопасности в организации. Варианты обработки рисков.

Требования, предъявляемые к формированию политики безопасности организации. Структура и содержание политики безопасности организации применительно к компьютерным системам.

Цель работы: получить практические знания и навыки об управлении информационной безопасностью и формированию политики информационной безопасности в организации.

Учебные вопросы:

1. Структура документации системы менеджмента информационной безопасности в организации. Модель PDCA.

2. Алгоритм и матрица оценки рисков при обеспечении информационной безопасности в организации. Варианты обработки рисков.

3. Требования, предъявляемые к формированию политики безопасности организации.

4. Структура и содержание политики безопасности организации применительно к компьютерным системам.

5. Цель работы: получить практические знания и навыки об управлении информационной безопасностью и формированию политики информационной безопасности в организации.

Тема № 8. Методология обследования и проектирования защищенных информационных (автоматизированных) систем

Практическое занятие 8

Образовательные технологии: технология проблемно-модульного обучения.

Вид практического занятия: смешанная форма практического занятия.

Тема и содержание практического занятия: Сущность построения системы защиты информации. Оптимальные механизмы обеспечения защиты информации и механизмы управления. Выбор способа постановки задачи. Методы построения защищённых АС. Принципы проектирования. Структурный принцип и принцип модульного проектирования. Три основных конструкции для проектирования. Преимущества использования модульного принципа.

Корректность реализации и верификация информационных (автоматизированных) систем. Понятие корректности или правильности проверяемого объекта. Спецификация требований программного обеспечения.

Представления функциональных требований. Рекомендации к структуре и методам описания программных требований. Основные ключевые требования «хорошей спецификации». Требования к программной спецификации. Основные подходы к определению спецификаций требований.

Теория безопасных систем (TCB). Понятие «доверенная вычислительная среда» (trusted computing base-TCB). Дискретная природа характеристики «безопасный». Характеристика «доверенный». Доверенная вычислительная среда. Набор компонентов, составляющий доверенную

вычислительную среду. Этапы разработки защищённой АС. Процесс создания автоматизированных систем в защищенном исполнении (ГОСТ Р 51583—2014). Цель создания АСЗИ.

Цель работы: получить практические знания и навыки об этапах и содержании работ по проектированию защищенных информационных (автоматизированных) систем.

Учебные вопросы:

1. Сущность построения системы защиты информации. Оптимальные механизмы обеспечения защиты информации и механизмы управления. Выбор способа постановки задачи.
2. Методы построения защищённых АС. Два основных метода проектирования. Метод проектирования «снизу вверх». Недостатки метода проектирования «снизу вверх».
3. Иерархический метод построения защищённой АС («сверху вниз»).
4. Принципы проектирования. Структурный принцип и принцип модульного проектирования.
5. Три основных конструкции для проектирования. Использование элемента DO-WHILE для организации цикла. Конструкция принятия двоичного решения IF-THEN-ELSE. Преимущества использования модульного принципа.
6. Корректность реализации и верификация информационных (автоматизированных) систем. Понятие корректности или правильности проверяемого объекта.
7. Спецификация требований программного обеспечения. Функциональные критерии и характеристики. Неформализованные представления разработчика. Спецификация требований программного обеспечения (Software Requirements Specification).
8. Представления функциональных требований. Рекомендации к структуре и методам описания программных требований. Основные ключевые требования «хорошей спецификации». Требования к программной спецификации. Основные подходы к определению спецификаций требований.
9. Теория безопасных систем (TCB). Понятие «доверенная вычислительная среда» (trusted computing base-TCB).
10. Дискретная природа характеристики «безопасный». Характеристика «доверенный». Доверенная вычислительная среда. Набор компонентов, составляющий доверенную вычислительную среду.
11. Этапы разработки защищённой автоматизированной системы (АСЗИ). Процесс создания автоматизированных систем в защищенном исполнении (ГОСТ Р 51583—2014). Цель создания АСЗИ.

3. Указания по проведению лабораторного практикума

Не предусмотрено учебным планом.

4. Указания по проведению самостоятельной работы студентов

№ п/п	Наименование блока (раздела) дисциплины	Виды СРС
1	*Актуальность проблемы обеспечения информационной безопасности для создаваемых защищенных информационных систем*	*Подготовка рефератов, письменная работа, самостоятельное изучение тем.* Примерная тематика *рефератов (докладов, письменных работ и т.д.):* *1. Место информационной безопасности в системе национальной безопасности.* *2. Современная концепция информационной безопасности.* *3. Цели и концептуальные основы защиты информации.* *4. Проблематика защиты информации в АСЗИ.* *5. Проблематика защиты информации в ИСПДн.* *6. Проблематика защиты информации в АСУ ТП КВО (объектов КИИ).* *7. Классификация компьютерных систем, подлежащих защите в зависимости от обрабатываемой информации и функционального назначения.* *8. Классификация АС по уровню защищённости от НСД к информации.* *9. Классификация СВТ по уровню защищённости от НСД к информации. Перечень показателей защищённости СВТ и совокупности описывающих их требований. Характеристика классов защищённости СВТ от НСД к информации.* *10. Классификация МЭ по уровню защищённости от НСД к информации.*
2	*Основные угрозы и уязвимости информационных систем, возможные атаки на них*	*Подготовка рефератов, письменная работа, самостоятельное изучение тем, создание презентаций.* Примерная тематика *рефератов (докладов, письменных работ и т.д.):* *1. Виды и анализ угроз автоматизированных систем.* *2. Компьютерные вирусы, технология и способы вторжения в устойчивую работу автоматизированных систем злоумышленников.* *3. Базовая модель угроз ИСПДн.* 4. *Уязвимости АС, возможные атаки на них*. 5. *Модели нарушителей объектов защиты информации*.
3	*Комплексное обеспечение информационной безопасности информационных систем. Способы атак на уровне приложений и*	*Подготовка рефератов, письменная работа, самостоятельное изучение тем.* Примерная тематика *рефератов (докладов, письменных работ и т.д.):* *1. Требования по защите информации в АС различных классов.* *2. Этапы классификации АС. Исходные данные для классификации АС. Выбор класса защищённости АС.*

	меры по снижению их уязвимости	*3. Структура документации системы менеджмента информационной безопасности в организации. Модель PDCA.* *4. Алгоритм и матрица оценки рисков при обеспечении информационной безопасности в организации. Варианты обработки рисков.* ***5.** Сущность построения системы защиты информации. Оптимальные механизмы обеспечения защиты информации и механизмы управления. Выбор способа постановки задачи.*
4	*Методология формирования задач защиты для объектов информатизации, интеграция средств информационной безопасности в единую технологическую среду построения защищенной ИС*	*Подготовка рефератов, письменная работа, самостоятельное изучение тем, создание презентаций.* Примерная тематика *рефератов (докладов, письменных работ и т.д.):* *1. Задачи аттестации объектов информатизации в соответствии с нормативно-методическими документами.* *2. Аттестация АС по требованиям безопасности информации.* *3. Аттестация ЗП по требованиям безопасности информации.* *4. Описание систем защиты с помощью матрицы доступа. Таблицы, описывающие права доступа субъектов к объектам. Описание модели Харрисона-Руззо-Ульмана (HRU).* *5. Модель распространения прав доступа Take-Grant. Цель использования модели Take-Grant. Основные элементы модели Take-Grant. Формальное описание модели Take-Grant.* *6. Три основных конструкции для проектирования. Использование элемента DO-WHILE для организации цикла. Конструкция принятия двоичного решения IF-THEN-ELSE. Преимущества использования модульного принципа.*
5	*Проектирование комплексной системы защиты информации (КСЗИ) в ИС*	*Подготовка рефератов, письменная работа, самостоятельное изучение тем, создание презентаций.* Примерная тематика *рефератов (докладов, письменных работ и т.д.):* *1. Комплексные системы защиты информации.* *2. Методы построения защищённых АС. Принципы проектирования.* *3. Структурный принцип и принцип модульного проектирования защищённых АС. Преимущества использования модульного принципа.* *4. Три основных конструкции для проектирования защищённых АС.* *5. Этапы разработки защищённой автоматизированной системы (АСЗИ). Процесс создания автоматизированных систем в защищенном исполнении (ГОСТ Р 51583—2014). Цель создания АСЗИ.*
6	*Типовая структура КСЗИ от*	*Подготовка рефератов, письменная работа, самостоятельное изучение тем, создание презентаций.* Примерная тематика *рефератов (докладов, письменных*

	несанкционированного доступа (НСД) в ИС. Концептуальные положения системы менеджмента информационной безопасности применительно к ИС	*работ и т.д.):* *1. Система разграничения доступа (СРД) и её функции. Средства для СРД. Реализация СРД.* *2. Построение модели нарушителя безопасности АС.* *3. Уровни возможностей, предоставляемые нарушителям штатными средствами АС и СВТ.* *4. Корректность реализации и верификация информационных (автоматизированных) систем. Понятие корректности или правильности проверяемого объекта.* *5. Спецификация требований программного обеспечения. Функциональные критерии и характеристики. Неформализованные представления разработчика. Спецификация требований программного обеспечения (Software Requirements Specification).*
7	*Методы и методики оценки качества (эффективности) ИБ при создании защищенных ИС*	*Подготовка рефератов, письменная работа, самостоятельное изучение тем, создание презентаций.* Примерная тематика *рефератов (докладов, письменных работ и т.д.):* *1. Оценка эффективности защиты информации на объектах информатизации.* *2. Перечень основных документов ФСТЭК России по вопросам защиты информации.* *3. Лицензирование и сертификация в области защиты информации.*

5. Указания по проведению контрольных работ для студентов

Учебным планом для бакалавров предусмотрено написание одной контрольной работы, что является одним из условий успешного освоения ими основных положений данной дисциплины и служит допуском к сдаче экзамена по курсу во время зачетной сессии.

Задания в контрольной работе разрабатываются преподавателем кафедры «Информационная безопасность» МГОТУ.

Цель выполняемой работы: закрепить знания и умения в области применения систем безопасности в информационных системах, а также продемонстрировать умения в области систематизирования и обобщения изучаемой информации.

Основные задачи выполняемой работы:

1. Закрепление полученных теоретических знаний;
2. Оценка применения практических навыков бакалавра в будущей практической работе;

Процесс написания контрольной работы делится на следующие этапы:

1. Определение темы контрольной работы
2. Изучение литературы, относящейся к теме контрольной работы
3. Оформление контрольной работы
4. Представление ее на кафедру для регистрации

5. Защита контрольной работы

Подготовку контрольной работы следует начинать с повторения соответствующих разделов учебника, учебных пособий, конспектов лекций.

Требования к содержанию контрольной работы:

В содержании контрольной работы необходимо показать знание рекомендованной литературы по данному заданию, при этом правильно пользоваться первоисточником и избегать чрезмерного цитирования. При использовании цитат необходимо указывать точные ссылки на используемый источник: указание автора (авторов), название работы, место издания, страницы. Кроме основной литературы рекомендуется использовать дополнительную литературу и источники сети Интернет (с детальным указанием сайта, т.е. копирование ссылки и даты обращения). Если в период выполнения контрольной работы были приняты новые законы или нормативно-правовые акты, относящиеся к излагаемой теме, их необходимо изучить и использовать при ее выполнении. Важно обратить внимание на различные концептуальные подходы по исследуемой тематике.

Оформление библиографического списка осуществляется в соответствие с установленными нормами и правилами ГОСТ.

Порядок выполнения контрольной работы:

Контрольная работа излагается логически последовательно, грамотно, разборчиво.

Структура контрольной работы:

- титульный лист, который содержит полное название высшего учебного заведения, название кафедры, реализующей данную дисциплину, название (тема) контрольной работы, фамилию, инициалы автора, также необходимо указать номер группы, фамилию и инициалы, а также должность, ученое звание и степень научного руководителя (преподавателя), проверяющего контрольную работу.
- оглавление;
  введение;
- основная часть;
- заключение;
- список используемых источников;
- приложения.

В конце работы ставится подпись студента и дата сдачи. Страницы контрольной работы должны быть пронумерованы. Номер страницы ставится в нижнем правом углу.

Объем контрольной работы должен составлять 10-15 страниц машинописного текста. Размер шрифта №14 (Times New Roman), полуторный интервал, стандартный лист формата А4. Поля: верхнее -20 мм, нижнее-20мм, левое -30 мм, правое -15 мм.

Дополнительно контрольная работа может иметь приложения (схемы, графики, диаграммы).

По всем возникающим вопросам обучающемуся следует обращаться за консультацией на кафедру. Срок выполнения контрольной работы определяется кафедрой. Срок проверки контрольной работы – 3 дня с момента необходимой фиксированной даты сдачи.

Порядок защиты контрольной работы:

Контрольная работа подлежит обязательной защите. В установленной преподавателем срок студент должен сдать контрольную работу и быть готов ответить на вопросы и замечания. Оценка работы производится по четырех бальной системе: «ОТЛИЧНО», «ХОРОШО», «УДОВЛЕТВОРИТЕЛЬНО», «НЕУДОВЛЕТВОРИТЕЛЬНО». После сдачи работы не возвращаются и хранятся в фонде кафедры.

Тематика контрольной работы:

1. Информационная безопасность сетевого периметра организации на основе применения технологии «тонкого клиента».
2. Информационная безопасность системы «клиент – банк» на основе технологии «толстого клиента».
3. Базовая модель угроз для информационных систем, обрабатывающих персональные данные.
4. Базовая модель угроз для государственных информационных систем.
5. Возможные модели нарушителей сетевого периметра организации.
6. Информационная безопасность модели Интернет - банкинга.
7. Информационная безопасность расчетов банковскими картами в Интернете.
8. Управление информационной безопасностью в организации.
9. Оценка и обработка рисков информационной безопасности.
10. Управление рисками информационной безопасности.
11. Документальное и инструментальное обеспечение управления рисками информационной безопасности.
12. Классификация технических каналов утечки информации для информационных систем.
13. Физическая природа побочных электромагнитных излучений в технических средствах обработки информации.
14. Наводки электромагнитных излучений при обработке информации в информационных системах.
15. Технические каналы утечки информации при передаче ее по каналам связи.
16. Средства выявления каналов утечки информации.
17. Технический контроль эффективности мер защиты информации.
18. Скрытие и защита информации от утечки по техническим каналам.
19. Защита информационных систем от несанкционированного доступа.

20. Классификация АС, СВТ и МЭ по требованиям защиты информации от несанкционированного доступа.
21. Классификация ПО по уровню контроля отсутствия не декларированных возможностей.
22. Схема защищенного информационного обмена при использовании симметричных методов защиты информации.
23. Схема защищенного информационного обмена при использовании криптографических алгоритмов с открытыми ключами.
24. Место ЭЦП в ряду криптографических механизмов. История возникновения ЭЦП в России. Общее правило создания ЭЦП. Общее правило верификации ЭЦП.
25. Применение и информационная безопасность режима электронной кодовой книги. Режима сцепления блоков шифротекста. Режима обратной связи по шифротексту.
26. Функция хеширования и асиметричные алгоритмы.
27. Информационная безопасность и защита электронных транзакций протокол (SSL). Схема работы протокола SET.
28. Информационная безопасность и правила обмена электронными документами. Общие требования, предъявляемые к ЭД (пакетам ЭД).
29. Информационная безопасность при составление и направление ЭД участником – отправителем.
30. Информационная безопасность и порядок контроля ЭД, полученных от участников – отправителей. Порядок оформления ЭД, подтверждающих исполнение ЭД участников.
31. Информационная безопасность и порядок приема к исполнению ЭД участником – получателем. Порядок хранения и уничтожения ЭД.

6. Перечень основной и дополнительной учебной литературы, необходимой для освоения дисциплины (модуля)

Основная литература:

1. Бирюков А. Информационная безопасность / А. Бирюков . - Москва : ДМК Пресс, 2017. - с. URL: https://e.lanbook.com/book/93278
2. Рябко Б.Я., Фионов А.Н. Основы современной криптографии и стеганографии – 2-е издание- М.: Горячая линия – Телеком, 2013. – 232с.

Дополнительная литература:

1. Гришина Н.В.Информационная безопасность предприятия : учебное пособие / Н.В. Гришина. - 2-е изд., доп. - М. ; М. : ФОРУМ : НИЦ ИНФРА-М, 2015. - 240 с. - (Высшее образование - бакалавриат)
2. Кияев, В. Безопасность информационных систем / В. Кияев; О. Граничин. - Москва : Национальный Открытый Университет

«ИНТУИТ», 2016. - 192 с. URL: http://biblioclub.ru/index.php?page=book&id=429032

Рекомендуемая литература

1. В.А.Северин. Комплексная защита информации на предприятии. М.: Издательский дом «Городец»,2008.- 368с.
2. Мельников В.П. идр Информационная безопасность.М.: Издателский центр «Академия» , 2008.-336с.
3. А.И. Баранчиков, П.А. Баранчиков, А.Н. Пылькин Алгоритмы и модели ограничения доступа к записям баз данных. - М. Горячая линия – Телеком, 2011 – 182с.
4. А.Ф. Чепига Информационная безопасность автоматизированных систем. М.: «Гелиос АРВ», 2010. -336с.
5. В.Ф. Шаньгин Комплексная защита информации в корпоративных системах. М.: ИД «Форум»: ИНФРА-М., 2010.-592с.
6. О.А.Романов, С.А. Бабин, С.Г. Жданов Организационное обеспечение информационной безопасности М.: Издательский центр «Академия», 2008,-192.
7. Васильков А.В., Васильков А.А., Васильков И.А. Информационные системы и их безопасность М.: ФОРУМ, 2011,-528с.

7. Перечень ресурсов информационно-телекоммуникационной сети интернет

Интернет-ресурсы:

1. http://eup.ru/catalog/all-all.asp – научно-образовательный портал.
2. http://informika.ru/ – образовательный портал.
3. www.wikIsec.ru - Энциклопедия информационной безопасности. – Публикации, статьи.
4. www.biblioclub.ru - Универсальная библиотека онлайн.
5. www.rucont.ru - ЭБС «Руконт».
6. http://www.academy.it.ru/ – академия АЙТИ.
7. http://www.minfin.ru - Официальный сайт Министерства финансов Российской Федерации
8. http://www.gov.ru/ - Официальный сервер органов государственной власти Российской Федерации.
9. http://www.fsb.ru/ - Официальный сайт Федеральной Службы Безопасности

http://www.fstec.ru/ - Официальный сайт Федеральной Службы по Техническому Экспортному контролю

8. Перечень информационных технологий

Перечень программного обеспечения: *MSOffice, ПО комплекса «Основы компьютерно-информационной безопасности».*

Информационные справочные системы:

1. Ресурсы информационно-образовательной среды МГОТУ

2. Рабочая программа и методическое обеспечение по дисциплине «Безопасность информационных систем».