Федеральное государственное бюджетное образовательное учреждение высшего образования
«ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ ИМЕНИ ДВАЖДЫ ГЕРОЯ СОВЕТСКОГО СОЮЗА, ЛЕТЧИКА-КОСМОНАВТА А.А. ЛЕОНОВА»

Троицкий Александр Витальевич
Подписано цифровой подписью: Троицкий Александр Витальевич

УТВЕРЖДАЮ
И.о. проректора
А.В. Троицкий
«___»_____2023 г.

ИНСТИТУТ ИНФОКОММУНИКАЦИОННЫХ СИСТЕМ И ТЕХНОЛОГИЙ
КАФЕДРА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

РАБОЧАЯ ПРОГРАММА

ДИСЦИПЛИНЫ
«ЗАЩИЩЕННЫЕ ИС»

Направление подготовки: 09.04.03 Прикладная информатика

Профиль: Моделирование и проектирование информационных систем

Уровень высшего образования: магистратура

Форма обучения: очная

Королев 2023

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

Автор: Воронов А. Н. Рабочая программа дисциплины: Защищенные ИС – Королёв МО: «Технологический Университет», 2023

Рецензент: к.в.н. доцент Сухотерин А.И.

Рабочая программа составлена в соответствии с требованиями федерального государственного образовательного стандарта высшего профессионального образования по направлению подготовки магистров 09.04.03 «Прикладная информатика» и Учебного плана, утвержденного Ученым советом Университета. Протокол № 9 от 11.04.2023 г.

Рабочая программа рассмотрена и одобрена на заседании кафедры:

Заведующий кафедрой (ФИО, ученая степень, звание, подпись)	Сазонов С.Ю. к.т.н. доцент			
Год утверждения (переутверждения)	2023			
Номер и дата протокола заседания кафедры	№8 от 29.03.2023			

Рабочая программа согласована:

Руководитель ОПОП _____ к.т.н., доцент Раев О.Н.

Рабочая программа рекомендована на заседании УМС:

Год утверждения (переутверждения)	2023			
Номер и дата протокола заседания УМС	№5 от 11.04.2023			

1. Перечень планируемых результатов обучения по дисциплине, соотнесенных с планируемыми результатами освоения ОПОП ВО

Целью изучения дисциплины является: освоение дисциплинарных компетенций, связанных с созданием и изучением современной защищенных информационных систем различного применения и степени сложности.

В процессе обучения обучающийся приобретает и совершенствует следующие компетенции:

профессиональные компетенции (ПК):

- Способность использовать передовые методы оценки качества, надежности и информационной безопасности ИС в процессе эксплуатации прикладных ИС (ПК-5);
- Способность управлять информационными ресурсами и ИС (ПК-9).

Основными **задачами** дисциплины являются:

1. изучение современной классификации средств защиты информации в корпоративных вычислительных сетях и системах;
2. изучение современных технологий построения безопасных информационных систем
3. изучение этапов и технологий проектирования и создания безопасных информационных систем
4. изучение современных программных и аппаратных средств защиты информации;
5. изучение основных угроз информации в современных информационных системах и сетях
6. изучение инструментальных программных и аппаратных средств анализа защищенности информационных систем и сетей
7. формирование умений в разработке проектов комплексных защищенных инфраструктур для типовых современных применений, отвечающую предъявляемым требованиям к уровню защищенности, выполняемых с использованием современных программных, программно-аппаратных и аппаратных средств защиты информации
8. формирование навыков разработки и внедрения комплексной защищенной инфраструктуры на предприятиях, включающих навыки базовой и расширенной настройки и использования современных программных и аппаратных средств защиты информации: файрволлов, интерактивных детекторов атак, защищенных доменных сервисов.

Показатель освоения компетенции отражают следующие индикаторы**:**

Необходимые знания:

- Понимает передовые методы оценки качества, надежности и информационной безопасности ИС в процессе эксплуатации прикладных ИС
- Имеет понятие об информационных ресурсах и ИСС;

Необходимые умения:

- Использует передовые методы оценки качества, надежности и информационной безопасности ИС в процессе эксплуатации прикладных ИС
- Обладает возможностью управлять информационными ресурсами и ИС;

Трудовые действия:

- Применяет передовые методы оценки качества, надежности и информационной безопасности ИС в процессе эксплуатации прикладных ИС
- Применяет методики управления информационными ресурсами и ИС.

2. Место дисциплины в структуре ОПОП ВО

Дисциплина относится к дисциплинам части, формируемой участниками образовательных отношений основной профессиональной образовательной программы подготовки магистров по направлению подготовки 09.04.03 «Прикладная информатика».

Дисциплина реализуется кафедрой информационной безопасности.

Дисциплина базируется на компетенциях, освоенных в курсе «Управление рисками в технологических системах» (ПК-4, 9), и служит основой написания ВКР.

3. Объем дисциплины и виды учебной работы

Общая трудоемкость дисциплины составляет 2 зачетные единицы, 72 часа. Практическая подготовка обучающихся составляет 8 часов.

Таблица 1

Виды занятий	Всего часов	Семестр …	Семестр 4	Семестр …	Семестр …
Общая трудоемкость	**72**		**72**		
Аудиторные занятия	**16**		**16**		
Лекции (Л)	8		8		
Практические занятия (ПЗ)	8		8		
Лабораторные работы (ЛР)	-		-		
Практическая подготовка	8		8		
Самостоятельная работа	**56**		**56**		
Курсовые работы (проекты)	-		-		
Расчетно-графические работы					
Контрольная работа	+		+		
Текущий контроль знаний					
Вид итогового контроля	Экзамен		Экзамен		

4. Содержание дисциплины
4.1. Темы дисциплины и виды занятий

Таблица 2

Наименование тем	Лекции, час.	Практические занятия, час	Лабораторные занятия, час	Занятия в интерактивной форме, час	Практическая подготовка	Код компетенций
Тема 1. Основные понятия защищенных ИС. Общие принципы построения защищенных ИС.	1	-	-	-	-	ПК – 5,9
Тема 2. Разграничения доступа к ресурсам ИС	1	-	-	-	-	ПК – 5,9
Тема 3. Способы хранения конфиденциальной информации.	1	-	-	-	-	ПК – 5,9
Тема 4. Основные направления защиты информации. Организационные меры защиты информации в организации.	1	-	-	1	-	ПК – 5,9
Тема 5. Системы обнаружения атак.	1	2	-	2	2	ПК – 5,9
Тема 6. Безопасное использование службы доменных имен (DNS).	1	2	-	2	2	ПК – 5,9
Тема 7. Обеспечение Безопасности WEB-серверов. Безопасность WEB-ориентированного контента.	1	2	-	1	2	ПК – 5,9
Тема 8. Технологии аутентификации и шифрования.	1	2	-	2	2	ПК – 5,9
Итого:	**8**	**8**	**-**	**8**	**8**	

4.2. Содержание тем дисциплины

Тема 1. Основные понятия защищенных ИС. Общие принципы построения защищенных ИС.

Понятие «Информационная система». Концепция безопасности информационной системы. Цели обеспечения информационной безопасности. Санкционированный и несанкционированный доступ. Угрозы безопасности и каналы реализации угроз. Уровни защиты информации. Стандарты безопасности. Классы защищенности информационных систем. Нормативная база Российской Федерации. Современная доктрина информационной безопасности Российской Федерации.

Тема 2. Разграничения доступа к ресурсам ИС.

Основные понятия систем разграничения доступа. Сущность и определение политики безопасности. Основные типы политик безопасности: мандатные, ролевые, контроля целостности информационных ресурсов, избирательного разграничения доступа. Субъектно-объектная модель информационной системы.

Тема 3. Способы хранения конфиденциальной информации.

Положение о конфиденциальной информации в электронном виде. Контентная категоризация. Классификация информации по уровню конфиденциальности. Метки документов. Способы хранение конфиденциальной информации. Сводная информация. Интеллектуальная собственность. Неструктурированная информация.

Тема 4. Основные направления защиты информации. Организационные меры защиты информации в организации.

Защита документов. Защита каналов утечки конфиденциальной информации. Мониторинг действий пользователей. Классификация внутренних нарушителей: неосторожные, манипулируемые, саботажники, нелояльные, мотивированные извне. Другие градации. Кадровая политика. Определение прав локальных пользователей. Стандартизация программного обеспечения. Организация процедуры хранения физических носителей информации. Определение уровней контроля информационных потоков. Режимы архива, сигнализации, активной защиты.

Тема 5. Системы обнаружения атак.

Понятие системы обнаружения атак (IDS). Типы и базовая структура IDS. Совместное расположение Host и Target. Разделение Host и управления. Полностью распределенное управление. Network-based IDS, Host-based IDS, Application-based IDS. Анализ, выполняемый IDS. Определение злоупотреблений. Активные и пассивные ответные действия. Использование SNMP TRAPS. Системы анализа и оценки уязвимостей. Host-based и Network-based анализ уязвимостей. Способы взаимодействия сканера уязвимостей и IDS.

Тема 6. Безопасное использование службы доменных имен (DNS).

Безопасность DNS. Сервисы DNS. Инфраструктура DNS. Компоненты DNS и понятие безопасности. Основные механизмы безопасности для сервисов DNS. Данные DNS и ПО DNS. Name-серверы, Авторитетные и кэширующие Name-серверы. Resolver′ы. Транзакции DNS. Запрос/ответ DNS. Зонная пересылка. Динамические обновления. Безопасность окружения DNS. Угрозы для ПО и данных DNS.

Тема 7. Обеспечение безопасности WEB-серверов. Безопасность WEB-ориентированного контента.

Причины уязвимости WEB-сервера. Планирование развертывания WEB-сервера. Безопасное инсталлирование и конфигурирование используемой ОС.

Удаление или запрещение ненужных сервисов и приложений. Управление ресурсами на у ровне ОС. Альтернативные платформы для web-сервера. Использование Appliances для web-сервера. Специально усиленные ОС и web-серверы. Тестирование безопасности ОС. Безопасное инсталлирование и конфигурирование web-сервера. Соответствующий список действий. Разграничение доступа для ПО web-сервера. Управление доступом к директории содержимого web-сервера. Публикации информации на web-сайтах. Обеспечение безопасности технологий создания активного содержимого. URLs и cookies. Уязвимости технологий активного содержимого на стороне клиента. Уязвимости технологий создания содержимого на стороне сервера. Необходимые действия для обеспечения безопасности web-содержимого.

Тема 8. Технологии аутентификации и шифрования.

Требования к аутентификации и шифрованию. Аутентификация, основанная на IP-адресе. Basic и Digest аутентификации. SSL/TLS. Возможности и слабые места SSL/TLS. Пример SSL/TLS сессии. Схемы шифрования SSL/TLS. Список действий при использовании технологий аутентификации и шифрования. Wirewall прикладного уровня для Web: ModSecurity.

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

«Методические указания для обучающихся по освоению дисциплины».

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

Структура фонда оценочных средств для проведения промежуточной аттестации обучающихся по дисциплине «Защищенные ИС» приведена в Приложении 1 к настоящей рабочей программе.

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

Основная литература:

1. Гришина Н. В. Информационная безопасность предприятия: Учебное пособие / Гришина Наталия Васильевна. - 2; доп. - Москва; Москва: Издательство "ФОРУМ": ООО "Научно-издательский центр ИНФРА-М", 2015. - 240 с. - ДЛЯ СТУДЕНТОВ ВЫСШИХ УЧЕБНЫХ ЗАВЕДЕНИЙ. - ISBN 978-5-00091-007-8.
   URL: http://znanium.com/go.php?id=491597
2. Малюк А. А., Горбатов В. С. и др**.** Введение в информационную безопасность: Учебное пособие / Малюк А. А.,Горбатов В.С. и др. ; под. ред. В.С. Горбатого. - М.: Телеком, 2011. - 288 с.: ил. - ISBN 978-5-9912-0160-5.
3. Малюк А. А. Теория защиты информации [Текст] / А. А. Малюк. - М.: Горячая линия - Телеком, 2013. - 184 с.: ил. - (Научное издание). - ISBN 978-5-9912-0246-6.

Дополнительная литература:

1. Бирюков А. Информационная безопасность: защита и нападение [Текст] / А. Бирюков. - М.: ДМК Пресс, 2012. - 474 с.: ил.; 60х90 /16. - ISBN 978-5-94074-647-8.
2. Шаньгин В. Ф. Информационная безопасность компьютерных систем и сетей: Учебное пособие / Шаньгин Владимир Федорович. - Москва; Москва: Издательский Дом "ФОРУМ": ООО "Научно-издательский центр ИНФРА-М", 2014. - 416 с. - ДЛЯ УЧАЩИХСЯ ПТУ И СТУДЕНТОВ СРЕДНИХ СПЕЦИАЛЬНЫХ УЧЕБНЫХ ЗАВЕДЕНИЙ. - ISBN 978-5-8199-0331-5. URL: http://znanium.com/go.php?id=423927
3. Цирлов В. Л. Основы информационной безопасности [Текст]: краткий курс / В. Л. Цирлов. - Ростов н/Д.: Феникс, 2008. - 253 с. - (Профессиональное образование). - ISBN 978-5-222-13164-0.

Рекомендуемая литература:

1. Ворона В. А., Тихонов В. А. Инженерно-техническая и пожарная защита объектов / Ворона В.А., Тихонов В.А. - М.: Горячая линия-Телеком, 2012. - 512 с.: ил. - ISBN 978-5-9912-0179-7.
2. Ворона В. А., Тихонов В. А. Технические средства наблюдения в охране объектов / Ворона В.А., Тихонов В.А. - М.: Горячая линия-Телеком, 2011. - 184 с.: ил. - ISBN 978-5-9912-0143-8.
3. Зайцев А. П. и др. Технические средства и методы защиты информации [Текст]: учебное пособие для вуза / Зайцев А.П. и др.; под. ред. А. П. Зайцева, А. А. Шелупанова. - 4-е изд., испр. и доп. - М.: Горячая линия-Телеком, 2012. - 616 с.: ил. - ISBN 978-5-9912-0084-4.
4. Ярочкин В. И. Информационная безопасность / В. И. Ярочкин; В.И. Ярочкин. - 5-е изд. - Москва: Академический проект, 2008. - 544 с. - (Gaudeamus). - ISBN 978-5-8291-0987-5.
URL: http://biblioclub.ru/index.php?page=book&id=211164

8. Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины

Интернет-ресурсы:

http://www.znanium.com/ - электронно-библиотечная система
http://www.e.lanbook.com/ - ЭБС Издательства "ЛАНЬ"
http://www.rucont.ru/- электронно-библиотечная система
http://www.biblioclub.ru/ -университетская библиотека онлайн

9. Методические указания для обучающихся по освоению дисциплины

Методические указания для обучающихся, по освоению дисциплины, приведены в Приложении 2 к настоящей рабочей программе.

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

Перечень программного обеспечения: MS Office.

Информационные справочные системы:

1. Ресурсы информационно-образовательной среды Университета.

2. Информационно – справочные (правовые) системы: «Консультант +».

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 лекций в форме слайд-презентаций, оборудованный современными лицензионными программно-техническими средствами: операционная система не ниже WindowsXP; офисные программы MSOffice;
- рабочее место преподавателя, оснащенное компьютером с доступом в Интернет;
- рабочие места студентов, оснащенные компьютерами с доступом в Интернет.

Приложение 1

ИНСТИТУТ ИНФОКОММУНИКАЦИОННЫХ СИСТЕМ И ТЕХНОЛОГИЙ
КАФЕДРА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ДЛЯ ПРОВЕДЕНИЯ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ОБУЧАЮЩИХСЯ ПО ДИСЦИПЛИНЕ «ЗАЩИЩЕННЫЕ ИС»

Направление подготовки: 09.04.03 Прикладная информатика

Профиль: Моделирование и проектирование информационных систем

Уровень высшего образования: магистратура

Форма обучения: очная

Королёв 2023

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

№ п/п	Индекс компетенции	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:		
				Необходимые знания	Необходимые умения	Трудовые действия
1.	ПК-5	Способность использовать передовые методы оценки качества, надежности и информационной безопасности ИС в процессе эксплуатации прикладных ИС	Тема1-8.	Понимает передовые методы оценки качества, надежности и информационной безопасно-сти ИС в процессе эксплуата-ции прикладных ИС	Использует передовые методы оценки качества, надежности и информационной безопасности ИС в процессе эксплуатации прикладных ИС	Применяет передовые методы оценки качества, надежности и информационной безопасно-сти ИС в процессе эксплуата-ции прикладных ИС
2.	ПК-9	Способность управлять информационными ресурсами и ИС	Тема 1 - 8	Имеет понятие об информаци-онных ресурсах и ИС	Обладает возможностью управлять информационными ресурсами и ИС	Применяет методики управле-ния информационными ресурсами и ИС

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

Код компетенции	**Инструменты, оценивающие сформированность компетенции**	**Этапы и показатель оценивания компетенции**	**Критерии оценивания компетенции на различных этапах формирования и шкалы оценивания**
ПК -5,9	Доклад в форме презентации	А) полностью сформирована **5 баллов** В) частично сформирована **3-4 балла** С) не сформирована **2 балла**	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 в срок не позднее 1 недели после проведения процедуры – для текущего контроля. Оценка проставляется в электронный журнал.
ПК -5,9	Выполнение контрольной работы	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	При определении сформированности компетенций критериями оценивания выступают методические рекомендации, разработанные по дисциплине для данного вида.

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

3.1 Примерная тематика докладов в презентационной форме:

1. Состав и основные характеристики современных средств охранной сигнализации.
2. Особенности применения современных средств охранной сигнализации в России и за рубежом.
3. Состав и основные характеристики современных систем и средств контроля и управления доступом.
4. Особенности применения современных систем и средств контроля и управления доступом в России и за рубежом.
5. Состав и основные характеристики современных радиоволновых однопозиционных средств охраны.
6. Особенности применения современных радиоволновых однопозиционных средств охраны в России и за рубежом.
7. Состав и основные характеристики современных радиоволновых двухпозиционных средств охраны.
8. Особенности применения современных радиоволновых двухпозиционных средств охраны в России и за рубежом.
9. Состав и основные характеристики современных проводноволновых средств охраны.
10. Особенности применения современных проводноволновых средств охраны в России и за рубежом.
11. Состав и основные характеристики современных вибрационных средств охраны.

12. Особенности применения современных вибрационных средств охраны в России и за рубежом.
13. Доктрина информационной безопасности РФ: современные информационные угрозы.
14. Доктрина информационной безопасности РФ: сущность и задачи.
15. Доктрина ИБ РФ: критически важные информационные объекты.
16. Доктрина ИБ РФ: направления обеспечения информационной безопасности.
17. Классификация защищаемого информационного ресурса.
18. Конфиденциальная информация и ее характеристика.
19. Секретная информация как объект информационной безопасности.
20. Организационное обеспечение информационной безопасности.
21. Техническое обеспечение информационной безопасности.
22. Правовое обеспечение информационной безопасности.
23. Организационная система обеспечения ИБ РФ.
24. Персональные данные как объект ИБ.
25. Понятие о теории защиты информации.

3.2 Примерная тематика контрольных работ:

1. Имеется ИС, состоящая из двух групп пользователей и администратора. У каждой группы пользователей свой каталог и пользователи должны иметь доступ к сетевому принтеру и модему. Администратор имеет полный доступ ко всем сетевым ресурсам (каталогам групп, системному каталогу, сканеру, принтеру, модему). В системе предусмотрены следующие права доступа – чтение, запись, выполнение. Определите список объектов и субъектов данной вычислительной системы. Составьте матрицу доступа.
2. Имеется некоторая ИС, построенная в соответствии с мандатной моделью безопасности Бела- Лапалулла. Пользователь, работающий в данной системе и имеющий уровень доступа «С» (Секретно), пытается прочитать файл, имеющий уровень секретности «К» (Конфиденциально). Возможна ли данная операция? И если не возможна, то какое правило модели Бела- Лапалулла она нарушает. Если возможно, то, в соответствии с каким правилом.
3. Имеется некоторая ИС, построенная в соответствии с мандатной моделью безопасности Бела- Лапалулла. Пользователь, работающий в данной системе, пытается удалить в корзину какой-либо файл, имеющий уровень доступа «СС». Возможна ли данная операция? И если не возможна, то какое правило модели Бела- Лапалулла она нарушает. Если возможно, то, в соответствии с каким правилом.

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

Формой контроля знаний по дисциплине «Защищенные ИС» является экзамен.

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
Проводится в сроки, установленные графиком учебного процесса	Экзамен	ПК -5,9	3 вопроса	Экзамен проводится в устной форме, путем ответа на вопросы. Время, отведенное на процедуру – 30 минут.	Результаты предоставляются в день проведения экзамена	Критерии оценки: «**Отлично**»: знание основных понятий предмета; умение использовать и применять полученные знания на практике; работа на практических занятиях; знание основных научных теорий, изучаемых предметов; ответ на вопросы билета. «**Хорошо**»: знание основных понятий предмета; умение использовать и применять полученные знания на практике; работа на практических занятиях; знание основных научных теорий, изучаемых предметов; ответы на большинство вопросов билета «**Удовлетворительно**»: демонстрирует частичные знания по темам дисциплин; незнание неумение использовать и применять полученные знания на практике; не работал на практических занятиях; ответил не на все вопросы билета «**Неудовлетворительно**»: демонстрирует частичные знания по темам дисциплин; незнание основ-

						ных понятий предмета; неумение использовать и применять полученные знания на практике; не работал на практических занятиях; не отвечает на вопросы.

4.1. Типовые вопросы, выносимые на экзамен

1. Общие определения и характеристики систем. Понятие сложности, критерии и свойства.
2. Критерии и свойства для системы. Вероятностная модель системы и пример пограничных состояний.
3. Информационные системы. Автоматизированные системы. Определения. Структура и классификация систем.
4. Базовые информационные процессы в системах.
5. Закон необходимого разнообразия Эшби. Энтропийная форма закона. Следствия из закона Эшби.
6. Основные принципы обеспечения информационной безопасности для информационных систем.
7. Методическая и нормативная база для построения защищенных систем.
8. Виды защищенных автоматизированных систем в соответствии с требованиями ГОСТ.
9. Принципы защиты информации в автоматизированных системах в соответствии с требованиями ГОСТ.
10. Принципы защиты информации в ИСПДН.
11. Аспекты построения доверенной вычислительной среды (ТСВ).
12. Способы реализации механизмов парольной защиты. Хранение и передача паролей.
13. Принципы распределения и реализации системы полномочий и доступов.
14. Пример построения защищенной системы на основе микроядерной ОС.
15. Программные аспекты построения защищенных систем. Работа с памятью.
16. Общие принципы обеспечения резервирования и защиты от сбоев.
17. Протоколы резервирования сетевой инфраструктуры.
18. Аспекты резервирования и надежности виртуальных систем.
19. Иерархическая модель данных.
20. Сетевая модель данных.
21. Модель системы защиты. Комплексный подход.
22. Международные стандарты оценки защищённости.
23. Руководящие документы Гостехкомиссии России. и.

Итоговое начисление баллов по дисциплине осуществляется в соответствии с разработанной и внедренной балльно-рейтинговой системой контроля и оценивания уровня знаний и внеучебной созидательной активности обучающихся.

Приложение 2

ИНСТИТУТ ИНФОКОММУНИКАЦИОННЫХ СИСТЕМ И ТЕХНОЛОГИЙ
КАФЕДРА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ «ЗАЩИЩЕННЫЕ ИС»

Направление подготовки: 09.04.03 Прикладная информатика

Профиль: Моделирование и проектирование информационных систем

Уровень высшего образования: магистратура

Форма обучения: очная

Королев 2023

1. Общие положения

Целью изучения дисциплины является: освоение дисциплинарных компетенций, связанных с созданием и изучением современной защищенных информационных систем различного применения и степени сложности.

Задачи дисциплины:

1. изучение современной классификации средств защиты информации в корпоративных вычислительных сетях и системах;
2. изучение современных технологий построения безопасных информационных систем
3. изучение этапов и технологий проектирования и создания безопасных информационных систем
4. изучение современных программных и аппаратных средств защиты информации;
5. изучение основных угроз информации в современных информационных системах и сетях
6. изучение инструментальных программных и аппаратных средств анализа защищенности информационных систем и сетей
7. формирование умений в разработке проектов комплексных защищенных инфраструктур для типовых современных применений, отвечающую предъявляемым требованиям к уровню защищенности, выполняемых с использованием современных программных, программно-аппаратных и аппаратных средств защиты информации
8. формирование навыков разработки и внедрения комплексной защищенной инфраструктуры на предприятиях, включающих навыки базовой и расширенной настройки и использования современных программных и аппаратных средств защиты информации: файрволлов, интерактивных детекторов атак, защищенных доменных сервисов.

2. Указания по проведению практических занятий

Практическое занятие 1.

Вид практического занятия**:** *смешанная форма практического занятия.*

Образовательные технологии: *групповая дискуссия*

Тема и содержание практического занятия: *Тема 5. Системы обнаружения атак.*

Основные положения темы занятия:

1. Типы и базовая структура IDS.
2. Совместное расположение Host и Target.
3. Активные и пассивные ответные действия.
4. Использование SNMP TRAPS.
5. Системы анализа и оценки уязвимостей. Host-based и Network-based анализ уязвимостей.
6. Способы взаимодействия сканера уязвимостей и IDS.

Продолжительность занятия – 2 ч.

Практическое занятие 2.

Вид практического занятия**:** *смешанная форма практического занятия.*

Образовательные технологии: *групповая дискуссия*

Тема и содержание практического занятия: *Тема 6. Безопасное использование службы доменных имен (DNS).*

Основные положения темы занятия:

1. Безопасность DNS. Сервисы DNS. Инфраструктура DNS.
2. Основные механизмы безопасности для сервисов DNS.
3. Авторитетные и кэширующие Name-серверы. Resolver'ы.
4. Динамические обновления.
5. Угрозы для ПО и данных DNS.

Продолжительность занятия – 2 ч.

Практическое занятие 3.

Вид практического занятия**:** *смешанная форма практического занятия.*

Образовательные технологии: *групповая дискуссия*

Тема и содержание практического занятия: *Тема 7. Обеспечение безопасности WEB-серверов. Безопасность WEB-ориентированного контента.*

Основные положения темы занятия:

1. Безопасное инсталлирование и конфигурирование используемой ОС.
2. Тестирование безопасности ОС.
3. Безопасное инсталлирование и конфигурирование web-сервера. Соответствующий список действий.
4. Обеспечение безопасности технологий создания активного содержимого. URLs и cookies.
5. Уязвимости технологий активного содержимого на стороне клиента. Уязвимости технологий создания содержимого на стороне сервера.
6. Необходимые действия для обеспечения безопасности web-содержимого.

Продолжительность занятия – 2 ч.

Практическое занятие 4.

Вид практического занятия**:** *смешанная форма практического занятия.*

Образовательные технологии: *групповая дискуссия*

Тема и содержание практического занятия: *Тема 8. Технологии аутентификации и шифрования.*

Основные положения темы занятия:

1. Требования к аутентификации и шифрованию.
2. Схемы шифрования SSL/TLS.
3. Список действий при использовании технологий аутентификации и шифрования.
4. Wirewall прикладного уровня для Web: ModSecurity.

Продолжительность занятия – 2 ч.

3. Указания по проведению лабораторного практикума

Не предусмотрено учебным планом.

4. Указания по проведению самостоятельной работы обучающихся

Цель самостоятельной работы: подготовить студентов к самостоятельному научному творчеству.

Задачи самостоятельной работы:

1) расширить представление в области информационной безопасности и существующих средств защиты информации;

2) привить навыки самостоятельного решения нестандартных задач в области применения защитных средств и технологий.

Тематическое содержание самостоятельной работы представлено в таблице:

№ п/п	Виды самостоятельной работы	Количество часов	Перечень заданий
1.	Вопросы, выносимые на самостоятельное изучение	20	1. Особенности шифрования данных псевдослучайными числами. 2. Основные методы шифрования информации и их характеристика. 3. Порядок применения поточных и блочных шифров, понятие криптографического протокола. 4. Криптографические системы с открытым ключом и их особенности применения. 5. Методы использования специальных свойств компьютерных форматов. 6. Философия использования электронной цифровой подписи и методы хеширования сообщений. 7. Методы использования избыточности аудио- и видеоинформации в компьютерной стеганографии. 8. Характеристика современных распространённых методов биометрической идентификации личности и особенности их применения. 9. Реализация технологии речевой подписи (аудиомаркирования) сообщений с применением компьютерных технологий. 10. Практическое применение защитной технологии «речевая подпись» в современном мире.
2.	Тематика докладов	20	• Понятие информационной войны. Проблемы информационной войны. • Информационное оружие и его классификация. • Цели информационной войны, её составные части и средства её ведения. Объекты воздействия в информационной войне. • Уровни ведения информационной войны. Информационные операции. Психологические операции. Оперативная маскировка. Радиоэлектронная борьба. Воздействие на сети. • Основные положения государственной информационной политики Российской Федерации. Первоочередные мероприятия по реализации государственной политики обеспечения информационной безопасности. • Виды защищаемой информации в сфере государственного

			и муниципального управления. • Обеспечение информационной безопасности организации. • Управление и защита информации в информационно-телекоммуникационных сетях. • Характеристика эффективных стандартов по безопасности. Требования к полноте эффективных стандартов по безопасности. • Риск работы на персональном компьютере. Планирование безопасной работы на персональном компьютере. • Стандарты предприятия по использованию персональных компьютеров. Практические меры безопасности для персональных компьютеров
3.	Выполнение практических заданий	20	1. Основные криптографические методы защиты электронной документации и данных. 2. Современные технологии обеспечения безопасности на основе индивидуальных особенностей человека.
4	Подготовка к экзамену	32	Проработка лекций, практик, изучение рекомендованной литературы. Консультации у преподавателя.

5. Указания по проведению контрольных работ для обучающихся очной формы обучения

5.1. Требования к структуре

Структура контрольной работы должна способствовать раскрытию темы: иметь титульный лист, содержание, введение, основную часть, заключение, список литературы.

5.2. Требования к содержанию (основной части)

1. Во введении обосновывается актуальность темы, определяется цель работы, задачи и методы исследования.

2. При определении целей и задач исследования необходимо правильно их формулировать. Так, в качестве цели не следует употреблять глагол «сделать». Правильно будет использовать глаголы: «раскрыть», «определить», «установить», «показать», «выявить» и т.д.

3. Основная часть работы включает 2 - 4 вопроса, каждый из которых посвящается решению задач, сформулированных во введении, и заканчивается констатацией итогов.

4. Приветствуется иллюстрация содержания работы таблицами, графическим материалом (рисунками, схемами и т.п.).

5. Необходимо давать ссылки на используемую Вами литературу.

6. Заключение должно содержать сделанные автором работы выводы, итоги исследования.

7. Вслед за заключением идет список литературы, который должен быть составлен в соответствии с установленными требованиями. Если в работе имеются приложения, они оформляются на отдельных листах, и должны быть соответственно пронумерованы.

5.3. Требования к оформлению

Объём контрольной работы – 10 страниц формата А 4, напечатанного с одной стороны текста (1,5 интервал, шрифт Times New Roman).

6. Перечень основной и дополнительной учебной литературы

Основная литература:

1. Гришина Н. В. Информационная безопасность предприятия: Учебное пособие / Гришина Наталия Васильевна. - 2; доп. - Москва; Москва: Издательство "ФОРУМ": ООО "Научно-издательский центр ИНФРА-М", 2015. - 240 с. - ДЛЯ СТУДЕНТОВ ВЫСШИХ УЧЕБНЫХ ЗАВЕДЕНИЙ. - ISBN 978-5-00091-007-8.
   URL: http://znanium.com/go.php?id=491597
2. Малюк А. А., Горбатов В. С. и др**.** Введение в информационную безопасность: Учебное пособие / Малюк А. А.,Горбатов В.С. и др. ; под. ред. В.С. Горбатого. - М.: Телеком, 2011. - 288 с.: ил. - ISBN 978-5-9912-0160-5.
3. Малюк А. А. Теория защиты информации [Текст] / А. А. Малюк. - М.: Горячая линия - Телеком, 2013. - 184 с.: ил. - (Научное издание). - ISBN 978-5-9912-0246-6.

Дополнительная литература:

1. Бирюков А. Информационная безопасность: защита и нападение [Текст] / А. Бирюков. - М.: ДМК Пресс, 2012. - 474 с.: ил.; 60х90 /16. - ISBN 978-5-94074-647-8.
2. Шаньгин В. Ф. Информационная безопасность компьютерных систем и сетей: Учебное пособие / Шаньгин Владимир Федорович. - Москва; Москва: Издательский Дом "ФОРУМ": ООО "Научно-издательский центр ИНФРА-М", 2014. - 416 с. - ДЛЯ УЧАЩИХСЯ ПТУ И СТУДЕНТОВ СРЕДНИХ СПЕЦИАЛЬНЫХ УЧЕБНЫХ ЗАВЕДЕНИЙ. - ISBN 978-5-8199-0331-5. URL: http://znanium.com/go.php?id=423927
3. Цирлов В. Л. Основы информационной безопасности [Текст]: краткий курс / В. Л. Цирлов. - Ростов н/Д.: Феникс, 2008. - 253 с. - (Профессиональное образование). - ISBN 978-5-222-13164-0.

Рекомендуемая литература:

1. Ворона В. А., Тихонов В. А. Инженерно-техническая и пожарная защита объектов / Ворона В.А., Тихонов В.А. - М.: Горячая линия-Телеком, 2012. - 512 с.: ил. - ISBN 978-5-9912-0179-7.
2. Ворона В. А., Тихонов В. А. Технические средства наблюдения в охране объектов / Ворона В.А., Тихонов В.А. - М.: Горячая линия-Телеком, 2011. - 184 с.: ил. - ISBN 978-5-9912-0143-8.
3. Зайцев А. П. и др**.** Технические средства и методы защиты информации [Текст]: учебное пособие для вуза / Зайцев А.П. и др.; под. ред. А. П. Зайцева, А. А. Шелупанова. - 4-е изд., испр. и доп. - М.: Горячая линия-Телеком, 2012. - 616 с.: ил. - ISBN 978-5-9912-0084-4.

4. Ярочкин В. И. Информационная безопасность / В. И. Ярочкин; В.И. Ярочкин. - 5-е изд. - Москва: Академический проект, 2008. - 544 с. - (Gaudeamus). - ISBN 978-5-8291-0987-5. URL: http://biblioclub.ru/index.php?page=book&id=211164

7. Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины

Интернет-ресурсы:
http://www.znanium.com/ - электронно-библиотечная система
http://www.e.lanbook.com/ - ЭБС Издательства "ЛАНЬ"
http://www.rucont.ru/- электронно-библиотечная система
http://www.biblioclub.ru/ -университетская библиотека онлайн

8. Перечень информационных технологий

Перечень программного обеспечения: *MSOffice.*
Информационные справочные системы:
1. Ресурсы информационно-образовательной среды Университета
2. Информационно – справочные (правовые) системы: «Консультант +».