Министерство науки и высшего образования Российской Федерации
Федеральное государственное бюджетное образовательное учреждение
высшего образования
**«Владимирский государственный университет
имени Александра Григорьевича и Николая Григорьевича Столетовых»
(ВлГУ)**

Институт информационных технологий и радиоэлектроники

УТВЕРЖДАЮ:
Директор института
_____ Галкин А. А.
«_06_» _07_____2022 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

ЗАЩИЩЕННЫЕ ИНФОРМАЦИОННЫЕ СИСТЕМЫ
(наименование дисциплины)

направление подготовки / специальность
10.04.01. «Информационная безопасность»

направленность (профиль) подготовки
Автоматизация информационно-аналитической деятельности

г. Владимир

2022 Год

1. ЦЕЛИ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Целью освоения дисциплины «Защищенные информационные системы» являются обеспечение подготовки студентов в соответствии с требованиями ФГОС ВО и учебного плана по направлению 10.04.01 «Информационная безопасность». Целью освоения дисциплины является ознакомление магистрантов с современным теоретическим аппаратом информационной безопасности, представление сведений о базовых моделях и алгоритмах, используемых в управлении информационной безопасностью в информационных системах, а также о процессе теоретико-методологического анализа различных механизмов и сервисов защиты информации.

Задачей освоения курса является изучение аппарата управления информационной безопасностью в информационных системах, освоение методов анализа программно-технических сервисов информационной безопасности.

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОПОП

Дисциплина «Защищенные информационные системы» относится к обязательной части образовательной программы, код Б1.О.02 магистратуры направления подготовки 10.04.01 «Информационная безопасность». В учебном плане предусмотрены виды учебной деятельности, обеспечивающие синтез теоретических лекций, практически занятий и самостоятельной работы студентов. Курс тесно взаимосвязан с другими дисциплинами данного цикла.

3. ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОБУЧЕНИЯ ПО ДИСЦИПЛИНЕ

Планируемые результаты обучения по дисциплине, соотнесенные с планируемыми результатами освоения ОПОП (компетенциями и индикаторами достижения компетенций)

Формируемые компетенции (код, содержание компетенции)	Планируемые результаты обучения по дисциплине, в соответствии с индикатором достижения компетенции		Наименование оценочного средства
	Индикатор достижения компетенции	Результаты обучения по дисциплине	
ОПК-1 Способен обосновывать требования к системе информационной безопасности и разрабатывать проект технического задания на ее создание	ОПК-1.1.1	Знать принципы организации информационных систем в соответствии с требованиями по защите информации	Тестовые вопросы
	ОПК-1.1.2	Знать основные этапы процесса проектирования и общие требования к содержанию проекта	
	ОПК-1.1.3	Знать основные меры по защите информации в автоматизированных системах	
	ОПК-1.2.1	Уметь определять информационную инфраструктуру и информационные ресурсы организации, подлежащие защите	
	ОПК-1.2.2	Уметь анализировать показатели качества и критерии оценки систем и отдельных методов и средств защиты информации	
	ОПК-1.2.3	Уметь формировать требования и разрабатывать внешние спецификации для разрабатываемого программного обеспечения	
	ОПК-1.2.4	Уметь определять информационную инфраструктуру и информационные ресурсы организации, подлежащие защите	
	ОПК-1.3.1	Владеть навыками обнаружения инцидентов в процессе эксплуатации автоматизированной системы	

	ОПК-1.3.2	Владеть навыками идентификации инцидентов в процессе эксплуатации автоматизированной системы	
	ОПК-1.3.3	Владеть навыками оценки защищенности автоматизированных систем с помощью типовых программных средств	
	ОПК-1.3.4	Владеть навыками оценки последствий от реализации угроз безопасности информации в автоматизированной системе	
ОПК-2 Способен разрабатывать технический проект системы (подсистемы либо компонента системы) обеспечения информационной безопасности	ОПК-2.1.1	Знать содержание и порядок деятельности персонала по эксплуатации защищенных автоматизированных систем и систем безопасности автоматизированных систем	Тестовые вопросы
	ОПК-2.1.2	Знать критерии оценки защищенности автоматизированной системы	
	ОПК-2.1.3	Знать основные угрозы безопасности информации и модели нарушителя в автоматизированных системах	
	ОПК-2.2.1	Уметь осуществлять планирование и организацию работы персонала автоматизированной системы с учетом требований по защите информации	
	ОПК-2.2.2	Уметь выявлять и анализировать уязвимости автоматизированной системы, приводящие к возникновению угроз безопасности информации	
	ОПК-2.2.3	Уметь регистрировать и анализировать события, связанные с защитой информации в автоматизированных системах	
	ОПК-2.2.4	Уметь классифицировать и оценивать угрозы безопасности информации автоматизированной системы	
	ОПК-2.2.5	Уметь проводить анализ доступных информационных источников с целью выявления известных уязвимостей используемых в системе защиты информации программных и программно-аппаратных средств	
	ОПК-2.3.1	Владеть навыками анализа воздействия изменений конфигурации автоматизированной системы на ее защищенность	
	ОПК-2.3.2	Владеть навыками составления комплекса правил, процедур, практических приемов, принципов и методов, средств обеспечения защиты информации в автоматизированной системе	

4. ОБЪЕМ И СТРУКТУРА ДИСЦИПЛИНЫ

Трудоемкость дисциплины составляет 11 зачетных единиц, 396 часов

Тематический план
форма обучения – очная

№ п/п	Наименование тем и/или разделов/тем дисциплины	Семестр	Неделя семестра	Контактная работа обучающихся с педагогическим работником				Самостоятельная работа	Формы текущего контроля успеваемости, форма промежуточной аттестации *(по семестрам)*
				Лекции	Практические занятия	Лабораторные работы	*в форме практической подготовки*		
1	Понятие профиля защиты.	1	1-2	4		4		4	
2	Классы в системе общих критериев.	1	3-4	4		4		4	
3	Классы защищенности в системе общих критериев.	1	5-6	4		4	2	4	Рейтинг-контроль №1
4	Понятие аудита политики безопасности.	1	7-8	4		4		4	
5	Гарантии безопасности компьютерных систем в системе общих критериев..	1	9-10	4		4	2	4	
6	Понятие гарантии безопасности	1	11-12	4		4		4	Рейтинг-контроль №2
7	Уровни гарантий	1	13-14	4		4	2	4	
8	Каналы утечки и их анализ в системе общих критериев.	1	15-16	4		4	2	4	
9	Виды каналов утечки информации	1	17-18	4		4		4	Рейтинг-контроль №3
Всего за 1 семестр:		**108**		**36**		**36**		**36**	**Зачет**
1	Безопасное функционирование в системе общих критериев..	2	1-2	4		4	2	8	
2	Управление конфигурацией	2	3-4	4		4	2	8	
3	Основные угрозы безопасности информации в компьютерных системах.	2	5-6	4		4		8	Рейтинг-контроль №1
4	Модель угроз. Анализ критичных технологий.	2	7-8	4		4		8	
5	Требования, предъявляемые к разработке модели угроз.	2	9-10	4		4	2	8	
6	Государственная политика в области безопасности компьютерных систем.	2	11-12	4		4		8	Рейтинг-контроль №2
7	Система лицензирования и сертификации средств защиты.	2	13-14	4		4	2	8	
8	Разработка политик безопасности для защищенных компьютерных систем.	2	15-16	4		4	2	8	
9	Требования, предъявляемые к разработке политик безопасности. Дискреционная и многоуровневая политика безопасности.	2	17-18	4		4	2	8	Рейтинг-контроль №3
Всего за 2 семестр:		**180**		**36**		**36**		**72**	**Экзамен (36)**

1	Порядок аттестации защищенных компьютерных систем.	3	1-2	4		4	2	5	
2	Понятие аттестации защищенных компьютерных систем.	3	3-4	4		4		5	
3	Концепция управления ИТ-подразделением (IT Service Management. ITIL) — основа концепции управления ИТ-службами.	3	5-6	4		4	2	5	Рейтинг-контроль №1
4	Порядок внедрения SLM-системы. Service Desk — цели, возможности, реализации. Microsoft Operations Framework (MOF).	3	7-8	4		4	2	5	
5	Стадии создания ЗИС: формирование требований к ЗИС,	3	9-10	4		4	2	5	
6	Разработка концепции ЗИС, техническое задание, эскизный проект, технический проект, рабочая документация	3	11-12	4		4	2	5	Рейтинг-контроль №2
7	Методы и методики оценки качества ЗИС.	3	13-14	4		4		5	
8	Требования к эксплуатационной документации ЗИС.	3	15-16	4		4	2	5	
9	Порядок приемки защищенных ЗИС	3	17-18	4		4	2	5	Рейтинг-контроль №3
Всего за 3 семестр:		**108**		**36**		**36**		**9**	**Экзамен (27)**
Наличие в дисциплине КП/КР		**Нет**							
Итого по дисциплине		**396**		**108**		**108**		**117**	**Зачет** **Экзамен (36)** **Экзамен(27)**

Содержание лекционных занятий по дисциплине

1 семестр.

Раздел 1. Подсистемы, классы.

Тема 1. Гарантии безопасности. Требования по безопасности информационных технологий. Классы защищенности. Компоненты подсистем поддержки политики безопасности. Содержание политики безопасности.

Тема 2. Классы в системе общих критериев. Классы защищенности в системе общих критериев. Понятие аудита политики безопасности. Требования к подсистемам аудита. Подсистемы подтверждения подлинности отправки и получения сообщения.

Тема 3. Подсистемы разграничения доступа. Подсистемы идентификации и аутентификации. Подсистемы защиты функций защиты. Подсистемы защиты ресурсов системы. Подсистемы защиты связи. Требования к подсистемам, предъявляемые в каждом классе защищенности.

Тема 4. Гарантии безопасности компьютерных систем в системе общих критериев. Понятие гарантии безопасности. Уровни гарантий.

Тема 5. Гарантии проектирования защищенных информационных систем. Принципы обеспечения гарантий безопасности. Методология анализа гарантий безопасности.

Раздел 2. Каналы утечки информации.

Тема 1. Каналы утечки и их анализ в системе общих критериев. Виды каналов утечки информации.

Тема 2. Место каналов утечки информации в системе общих критериев безопасности. Методология анализа каналов утечки информации.

Тема 3. Безопасное функционирование в системе общих критериев. Управление конфигурацией.

Тема 4. Безопасная установка систем защиты информационных технологий. Безопасная модернизация информационных технологий.

2 семестр

Раздел 1. Модели угроз.

Тема 1. Основные угрозы безопасности информации в компьютерных системах. Ценности, опасности, потери, риски, угрозы в компьютерных системах. Основные угрозы информации в компьютерных системах. Специфика возникновения угроз в открытых сетях. Особенности защиты информации на узлах компьютерной сети.

Тема 2. Системные вопросы защиты программ и данных. Анализ рисков. Модель противника, возможности противника. Параллельный анализ целей и возможностей злоумышленника в компьютерной сети и в ситуации при наличии изолированного компьютера. Основные категории требований к программной и программно-аппаратной реализации средств защиты информации. Требования к защите автоматизированных систем от НСД.

Тема 3. Модель угроз. Анализ критичных технологий. Требования, предъявляемые к разработке модели угроз.

Тема 4. Структура модели угроз безопасности информации. Анализ критичных технологий обработки информации.

Раздел 2. Политика безопасности.

Тема 1. Государственная политика в области безопасности компьютерных систем. Система лицензирования и сертификации средств защиты. Структуры в РФ, обеспечивающие лицензирование и сертификацию средств защиты.

Тема 2. Нормативная база и ответственность за защиту информации в компьютерных системах. Руководящие документы ФСТЭК России по оценке защищенности автоматизированных систем от несанкционированного доступа

Тема 3. Разработка политик безопасности для защищенных компьютерных систем. Требования, предъявляемые к разработке политик безопасности.

Тема 4. Дискреционная и многоуровневая политика безопасности. Политика мандатного доступа. Политика защиты целостности информационных ресурсов.

Тема 5. Порядок аттестации защищенных компьютерных систем. Понятие аттестации защищенных компьютерных систем. Руководящие документы ФСТЭК России по аттестации. Порядок аттестации.

3 семестр

Раздел 1. Современная структура ITIL.

Тема 1. Принципы и методы аттестационных испытаний защищенных компьютерных систем по требованиям безопасности. Содержание этапов аттестационных испытаний. Контроль эффективности защитных мероприятий в системе аттестации.

Тема 2. Концепция управления ИТ-подразделением (IT Service Management. ITIL) — основа концепции управления ИТ-службами. Современная структура ITIL.

Тема 3. Преимущества внедрения ITSM. Бизнес-ориентированное управление ИТ на современном предприятии.

Тема 4. Порядок внедрения SLM-системы. Service Desk — цели, возможности, реализации. Microsoft Operations Framework (MOF).

Раздел 2. Защищенные информационные системы.

Тема 1. Стадии создания ЗИС: Формирование требований к ЗИС, разработка концепции ЗИС, техническое задание, эскизный проект, технический проект, рабочая документация, ввод в действие, аттестация ЗИС по требованиям безопасности, сопровождение ЗИС.

Тема 2. Методы и методики оценки качества ЗИС. Требования к эксплуатационной документации ЗИС.

Тема 3. Порядок приемки защищенных ЗИС, в том числе программных и технических (в частности, криптографических) средств и систем защиты информации от НСД. Особенности эксплуатации ЗИС на объекте защиты.

Содержание лабораторных занятий по дисциплине
1 семестр

Тема№ 1. Порядок лицензирования в области создания средств защиты информации и защищенных информационных систем для руководителя предприятия (организации) – соискателя лицензии

Содержание лабораторной работы. Перечислите нормативные правовые акты, регламентирующие процесс лицензирования деятельности организаций по оказанию услуг в области информационной безопасности. Что представляет собой лицензия? Назовите органы государственного лицензирования и их полномочия. Дайте общую характеристику системы лицензирования по обеспечению защиты сведений, составляющих государственную тайну. Назовите функции органов, уполномоченных на ведение лицензионной деятельности. Приведите перечень видов деятельности предприятий, подлежащих лицензированию ФСБ.

Тема № 2. Разработка профиля защиты и построение политик безопасности для компьютерной системы предприятия (организации)

Содержание лабораторной работы.

Что подразумеваю под понятием «профиль защиты»?

Как производят разработку профиля защиты для компьютерной системы предприятия?

Дайте определение понятию «политика безопасности» для компьютерной системы предприятия?

Назначение «политики безопасности» для компьютерной системы предприятия?

Основные разделы «политики безопасности» для компьютерной системы предприятия?

Тема № 3. Проведение аттестационных испытаний компьютерных систем в защищенном исполнении и выдача «Аттестата соответствия»

Содержание лабораторной работы.

Основные принципы системы аттестации.

Организационная структура системы аттестации

Порядок проведения аттестации

Порядок контроля и надзора за аттестацией и эксплуатацией аттестованных объектов

Что такое аттестация?

Что представляет собой аттестат соответствия?

Тема № 4. Обнаружение узлов корпоративной СЕТИ. ICMP ECHO REQUEST (Утилиты FPING и NMAP)

Содержание лабораторной работы.

Проверьте наличие всех рассмотренных утилит в системе:

linux:~# whereis nmap

nmap: /usr/bin/nmap /usr/lib/nmap /usr/share/nmap /usr/share/man/man1/nmap.1.gz

Исследуйте подсеть лаборатории (компьютерного класса, экспериментальной установки), выявите все активные узлы средствами утилит fping, nmap, hping3 (ознакомиться с назначением и основными опциями утилиты hping3 необходимо самостоятельно: http://www.hping.org);

Сравните время сканирования всего диапазона адресов исследуемой подсети различными утилитами: ping, fping, hping3, nmap (для nmap провести сканирование тремя различными режимами управления временем), результаты оформите в виде таблицы;

Напишите программу (bash, perl, ruby), производящую периодическую проверку доступности некоторого множества узлов сети (с использованием любой из рассмотренных утилит) и выводящую сообщение на стандартное устройство (отправляющую сообщение на почту, адрес почты уточнить у преподавателя) в случае недоступности какого-либо из

наблюдаемых узлов (перечень контролируемых узлов сети необходимо выбирать из полученного ранее файла).

2 семестр

Тема № 1. Обнаружение узлов корпоративной сети. Информационные ICMP сообщения. **Содержание лабораторной работы.** Исследуйте подсеть лаборатории (компьютерного класса, экспериментальной установки), выявите все активные узлы средством запросов TimeStamp Request, Information Request, Netmask Request. Выявите узлы сети, на которых запросы ICMP Echo Request фильтруются; Повторите исследование, используя все рассмотренные в работе утилиты, сравните результаты; Сравните реакцию различных ОС на информационные ICMP-запросы.

Тема № 2. Обнаружение узлов корпоративной сети средствами протокола TCP (TCP-PING. **Содержание лабораторной работы.** Исследуйте подсеть лаборатории (компьютерного класса, экспериментальной установки), выявите все активные узлы методом TCP Ping, с использованием TCP-пакетов с различным сочетанием флагов (с техникой сканирования методом TCP Ping средствами nmap ознакомьтесь самостоятельно: http://nmap.org/man/ru/); Выявите узлы сети, на которых запросы ICMP Echo Request фильтруются; Сравните реакцию различных ОС на информационные ICMP запросы. Необходимо использовать одну из рассмотренных утилит (на выбор). Результаты занесите в таблицу; Исследуйте реакцию узла сети на SYN-запросы, сравните ответы от открытого и закрытого TCP-порта. Все исследования необходимо провести средствами hping3 и nmap.

Тема № 3. Обнаружение узлов корпоративной сети средствами протоколов UDP (UDP-PING), IP. **Содержание лабораторной работы.** Идентифицируйте узлы сети, фильтрующие сообщения ICMP Echo Request (диапазон адресов узлов сети уточнить у преподавателя). Сканирование произведите методом UPD Discovery средствами рассмотренных утилит; Исследуйте реакцию узла сети на UDP-запросы, сравните ответы открытого и закрытого UDP-порта. Исследования проведите для различных ОС; Идентифицируйте узлы сети, фильтрующие сообщения ICMP Echo Request, используйте рассмотренные методы протокола IP; Сравните реакцию различных ОС на IP-пакеты с рассмотренными типами ошибок в заголовке.

Тема № 4. Обнаружение узлов корпоративной сети средствами протокола ARP (ARP-PING). **Содержание лабораторной работы.** Идентифицируйте узлы сети, фильтрующие сообщения ICMP Echo Request (диапазон адресов узлов сети уточнить у преподавателя). Произведите сканирование методом ARPing с помощью рассмотренных утилит; Напишите программу (bash, perl, ruby), производящую периодическую проверку на предмет появления нового устройства в сети (с неизвестным ранее аппаратным адресом). Результаты проверки должны выводиться на стандартное устройство и сохраняться в файле.

3 семестр

Тема № 1. Основные средства определения маршрутов IP-пакетов - PING, TRACEROUTE. **Содержание лабораторной работы.** Произвести трассировку методом Record Route до следующих узлов сети: серверов DNS университета, пограничного маршрутизатора университета, yandex.ru, mail.ru, vkontakte.ru, elibrary.ru, google.com. Составить перечень промежуточных узлов на каждом из путей прохождения IP-трафика с указанием IP-адресов их интерфейсов. Результаты занести в таблицу.

Тема № 2. Дополнительные средства определения маршрутов IP-ПАКЕТОВ - NMAP, TRACEMAP, MRT. **Содержание лабораторной работы.** Постройте карту маршрутов IP-пакетов от одного из АРМ локальной сети до наиболее востребованных (в организации) ресурсов Интернет (не менее десяти ресурсов). Средствами программы mtr исследуйте качество канала от компьютеров лаборатории (домашнего компьютера) до популярных ресурсов Интернет (ресурсов сети университета). Отследите изменения маршрутов за период времени 60-180 минут (если таковые будут происходить). Выпишите все альтернативные маршруты.

Тема № 3. Идентификация статуса TCP-портов (TCP-CONNECT. SYN-SCAN). **Содержание лабораторной работы.** 1. Необходимо обнаружить все открытые порты TCP (22, 23, 80) сети лаборатории (компьютерного класса, экспериментальной установки), с использованием функции connect(). 2. Повторите исследование, применяя метод Half-open SYN flag scanning. 3. Сравните время сканирования в первом и втором случае. 4. Повторите исследования с помощью утилиты hping3. Сравните результаты.

Тема № 4. Методы скрытого сканирования (STEALTH TCP SCANNING METHODS). **Содержание лабораторной работы.** Исследуйте ответ различных ОС на сканирование методами Stealth scanning. Занесите в таблицу (табл. 6) результаты для различных методов сканирования и состояний TCP-порта (порт открыт, порт закрыт, порт открыт и фильтруется, порт закрыт и фильтруется).

Тема № 5. Идентификация прикладных сетевых служб методом анализа особенностей реализации (SMTP). **Содержание лабораторной работы.** 1. Установите наиболее популярные свободно распространяемые сервера электронной почты: postfix, sendmail, qmail, exim4 (перечень и версии уточнить у преподавателя). 2. Экспериментально исследуйте особенности их работы:

- исследуйте ответы на синтаксически верные стандартные команды;
- исследуйте ответы на команды с ошибками;
- исследуйте ответы на команды VRFY и EXPN;
- исследуйте поддержку малоиспользуемых команд.

3. Варианты ответов оформите в виде таблицы. 4. Подготовьте профили каждого исследуемого сервера. 5. Проведите исследование почтовых серверов Интернет / университета (адреса уточнить у преподавателя) рассмотренным методом.6. Сравните полученные данные с подготовленными профилями. Сделайте предположения в версиях ПО исследуемых серверов.

5. ОЦЕНОЧНЫЕ СРЕДСТВА ДЛЯ ТЕКУЩЕГО КОНТРОЛЯ УСПЕВАЕМОСТИ, ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ПО ИТОГАМ ОСВОЕНИЯ ДИСЦИПЛИНЫ И УЧЕБНО-МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ САМОСТОЯТЕЛЬНОЙ РАБОТЫ СТУДЕНТОВ

5.1. Текущий контроль успеваемости

1 семестр

Вопросы рейтинг-контроля №1

- Ценности, опасности, потери, риски, угрозы в компьютерных системах.
- Основные угрозы информации в компьютерных системах.
- Специфика возникновения угроз в открытых сетях.
- Особенности защиты информации на узлах компьютерной сети.
- Системные вопросы защиты программ и данных.
- Анализ рисков. Модель противника, возможности противника.
- Параллельный анализ целей и возможностей злоумышленника в компьютерной сети и в ситуации при наличии изолированного компьютера.

Вопросы рейтинг-контроля №2

- Система лицензирования и сертификации средств защиты.
- Структуры в РФ, обеспечивающие лицензирование и сертификацию средств защиты.
- Нормативная база и ответственность за защиту информации в компьютерных системах.
- Основные руководящие документы ФСТЭК России, по оценке защищенности автоматизированных систем от несанкционированного доступа.
- Разработка политик безопасности для защищенных компьютерных систем.
- Требования, предъявляемые к разработке политик безопасности.

- Дискреционная и многоуровневая политика безопасности.
- Политика мандатного доступа.
- Политика защиты целостности информационных ресурсов.

Вопросы рейтинг-контроля №3

- Руководящие документы ФСТЭК России по аттестации.
- Порядок аттестации. Принципы и методы аттестационных испытаний защищенных компьютерных систем по требованиям безопасности.
- Содержание этапов аттестационных испытаний.
- Контроль эффективности защитных мероприятий в системе аттестации.
- Концепция управления ИТ-подразделением (IT Service Management. ITIL) — основа концепции управления ИТ-службами.
- Современная структура ITIL.
- Преимущества внедрения ITSM.
- Бизнес-ориентированное управление ИТ на современном предприятии.
- Порядок внедрения SLM-системы.
- Service Desk — цели, возможности, реализации.

2 семестр

Вопросы рейтинг-контроля №1

- Государственные стандарты на разработку и создание информационных систем в защищенном исполнении.
- CASE-технологии создания информационных систем.
- Стандарт ITIL.
- Построение гарантированно защищенных баз данных и их оценка по стандарту «Оранжевая книга».
- Американский стандарт по защите информации «Оранжевая книга».
- Понятие гарантии защиты.
- Критерии оценки защищенности баз данных.
- Содержание классов защищенности.

Вопросы рейтинг-контроля №2

- Подход к безопасности компьютерных систем в СС и базовые концепции. Понятие профиля защиты.
- Функции поддержки политики безопасности. Гарантии безопасности.
- Требования по безопасности информационных технологий. Классы защищенности.
- Компоненты подсистем поддержки политики безопасности.
- Содержание типовой политики безопасности.
- Классы защищенности в системе общих критериев. Понятие аудита политики безопасности.
- Требования к подсистемам аудита.
- Подсистемы подтверждения подлинности отправки и получения сообщения.

Вопросы рейтинг-контроля №3

- Каналы утечки и их анализ в системе общих критериев.
- Виды каналов утечки информации. Место каналов утечки информации в системе общих критериев безопасности.
- Методология анализа каналов утечки информации.
- Безопасное функционирование в системе общих критериев.

- Управление конфигурацией. Безопасная установка систем защиты информационных технологий.

Безопасная модернизация информационных технологий

3 семестр

Вопросы рейтинг-контроля №1

- Основные категории требований к программной и программно-аппаратной реализации средств защиты информации.
- Требования к защите автоматизированных систем от НСД.
- Модель угроз. Анализ критичных технологий.
- Требования, предъявляемые к разработке модели угроз.
- Структура модели угроз безопасности информации.
- Анализ критичных технологий обработки информации.
- Система лицензирования и сертификации средств защиты.

Вопросы рейтинг-контроля №2

- Понятие аттестации защищенных компьютерных систем.
- Руководящие документы ФСТЭК России по аттестации.
- Порядок аттестации. Принципы и методы аттестационных испытаний защищенных компьютерных систем по требованиям безопасности.
- Содержание этапов аттестационных испытаний.
- Контроль эффективности защитных мероприятий в системе аттестации.
- Концепция управления ИТ-подразделением (IT Service Management. ITIL) — основа концепции управления ИТ-службами.

Вопросы рейтинг-контроля №3

- Microsoft Operations Framework (MOF).
- Стадии создания ЗИС: формирование требований к ЗИС, разработка концепции ЗИС. Техническое задание, эскизный проект, технический проект, рабочая документация, ввод в действие.
- Сопровождение ЗИС.
- Методы и методики оценки качества ЗИС.
- Требования к эксплуатационной документации ЗИС.
- Порядок приемки защищенных ЗИС, в том числе программных и технических (в частности, криптографических) средств и систем защиты информации от НСД.
- Особенности эксплуатации ЗИС на объекте защиты.

5.2. Промежуточная аттестация по итогам освоения дисциплины

Примерный перечень вопросов к зачету 1 семестр

- Подсистемы подтверждения подлинности отправки и получения сообщения.
- Подсистемы разграничения доступа.
- Подсистемы идентификации и аутентификации.
- Подсистемы защиты функций защиты. Подсистемы защиты ресурсов системы.
- Подсистемы защиты связи.
- Требования к подсистемам, предъявляемые в каждом классе защищенности.
- Гарантии безопасности компьютерных систем в системе общих критериев.
- Понятие гарантии безопасности. Уровни гарантий.
- Гарантии проектирования защищенных информационных систем.

- Принципы обеспечения гарантий безопасности. Методология анализа гарантий безопасности.
- Каналы утечки и их анализ в системе общих критериев.
- Виды каналов утечки информации. Место каналов утечки информации в системе общих критериев безопасности.
- Методология анализа каналов утечки информации.
- Безопасное функционирование в системе общих критериев.
- Управление конфигурацией. Безопасная установка систем защиты информационных технологий.
- Безопасная модернизация информационных технологий

Примерный перечень вопросов к экзамену 2 семестр

- Ценности, опасности, потери, риски, угрозы в компьютерных системах.
- Основные угрозы информации в компьютерных системах.
- Специфика возникновения угроз в открытых сетях.
- Особенности защиты информации на узлах компьютерной сети.
- Системные вопросы защиты программ и данных.
- Анализ рисков. Модель противника, возможности противника.
- Параллельный анализ целей и возможностей злоумышленника в компьютерной сети и в ситуации при наличии изолированного компьютера.
- Основные категории требований к программной и программно-аппаратной реализации средств защиты информации.
- Требования к защите автоматизированных систем от НСД.
- Модель угроз. Анализ критичных технологий.
- Требования, предъявляемые к разработке модели угроз.
- Структура модели угроз безопасности информации.
- Анализ критичных технологий обработки информации.
- Система лицензирования и сертификации средств защиты.
- Структуры в РФ, обеспечивающие лицензирование и сертификацию средств защиты.
- Нормативная база и ответственность за защиту информации в компьютерных системах.
- Основные руководящие документы ФСТЭК России, по оценке защищенности автоматизированных систем от несанкционированного доступа.

Примерный перечень вопросов к экзамену 3 семестр

- Разработка политик безопасности для защищенных компьютерных систем.
- Требования, предъявляемые к разработке политик безопасности.
- Дискреционная и многоуровневая политика безопасности.
- Политика мандатного доступа.
- Политика защиты целостности информационных ресурсов.
- Понятие аттестации защищенных компьютерных систем.
- Руководящие документы ФСТЭК России по аттестации.
- Порядок аттестации. Принципы и методы аттестационных испытаний защищенных компьютерных систем по требованиям безопасности.
- Содержание этапов аттестационных испытаний.
- Контроль эффективности защитных мероприятий в системе аттестации.
- Концепция управления ИТ-подразделением (IT Service Management. ITIL) — основа концепции управления ИТ-службами.
- Современная структура ITIL.
- Преимущества внедрения ITSM.
- Бизнес-ориентированное управление ИТ на современном предприятии.
- Порядок внедрения SLM-системы.

- Service Desk — цели, возможности, реализации.
- Microsoft Operations Framework (MOF).
- Стадии создания ЗИС: формирование требований к ЗИС, разработка концепции ЗИС. Техническое задание, эскизный проект, технический проект, рабочая документация, ввод в действие.
- Методы и методики оценки качества ЗИС.
- Требования к эксплуатационной документации ЗИС.
- Порядок приемки защищенных ЗИС, в том числе программных и технических (в частности, криптографических) средств и систем защиты информации от НСД.
- Особенности эксплуатации ЗИС на объекте защиты.

5.3. Самостоятельная работа обучающегося.

Примерные вопросы и задания для самостоятельной работы студентов

1 семестр

- Методология Penetration Testing. Open Source Security Testing Methodology Manual (OSSTMM).
- Методология Penetration Testing. Information Systems Security Assessment Framework (ISSAF).
- Методология Penetration Testing. Open Web Application Security Project (OWASP).
- Методология Penetration Testing. Web Application Security Consortium Threat Classification (WASC-TC).
- Стандарт Penetration Testing. Penetration Testing Execution Standard (PTES).
- Footprinting. Цели, задачи Footprinting. Этапы Footprinting и Reconnaissance.
- Footprinting. Открытые источники и пассивный сбор информации.
- Footprinting. Активный сбор информации.
- Footprinting. Программные инструменты Footprinting и Reconnaissance.
- Сканирование сети. Обнаружение узлов сети. Методы и программные средства.
- Сканирование сети. Обнаружение открытых портов узла сети. Методы и программные средства.
- Сканирование сети. Типы сканирования (Full Open Scan, Half-open Scan, Xmas Tree Scan). Особенности использования рассматриваемых типов сканирования.
- Сканирование сети. Типы сканирования (FIN Scan, NULL Scan, ACK Scanning). Особенности использования рассматриваемых типов сканирования.
- Сканирование сети. Типы сканирования (UDP Scanning, ARP Scan). Особенности использования рассматриваемых типов сканирования.

2 семестр

- Services fingerprinting. Методы Services fingerprinting.
- Services fingerprinting. Программные инструменты Services fingerprinting.
- OS Fingerprinting. Методы OS Fingerprinting. Banner Grabbing.
- OS Fingerprinting. Методы OS Fingerprinting. Пассивное исследование стека в задаче идентификации ОС.
- OS Fingerprinting. Методы OS Fingerprinting. Активное исследование стека в задаче идентификации ОС.
- Enumeration. Понятие, цели и задачи Enumeration. Инвентаризация ресурсов OS Windows. Методы и средства.
- Enumeration. Понятие, цели и задачи Enumeration. Инвентаризация ресурсов OS Linux/Unix. Методы и средства.
- Enumeration. Понятие, цели и задачи Enumeration. Инвентаризация посредством SNMP.
- Enumeration. Понятие, цели и задачи Enumeration. Инвентаризация LDAP.

- Enumeration. Понятие, цели и задачи Enumeration. Инвентаризация SMTP.
- Sniffing. Цели и задачи анализа трафика. Программные инструменты анализа трафика.
- Sniffing атаки в коммутируемой сетевой среде. MAC Flooding. ARP Poisoning.
- Sniffing атаки в коммутируемой сетевой среде. MAC Spoofing.

3 семестр

- Sniffing атаки в коммутируемой сетевой среде. Методы и средства защиты от Sniffing атак.
- Атаки DOS. Цели и задачи атак DOS. Типы атак DOS.
- Атаки DOS. Service Request Floods. SYN Attack/Flood. ICMP Flood Attack. Программные средства проведения атак.
- Атаки DOS. Ping of Death. Teardrop. Smurf. Fraggle. Программные средства проведения атак.
- Атаки Buffer Overflow. Принципы.
- Атаки DDOS. Особенности реализации.
- Беспроводные сети. Угрозы и уязвимости Wireless Networks.
- Беспроводные сети. Аутентификация Wi-fi.
- Беспроводные сети. Атаки деаутентификации (Deauthentication Attack).
- Сканеры уязвимостей. Идентификация уязвимостей в сетях.
- Сканеры уязвимостей. Уязвимости БД.
- Средства анализа защищенности БД.
- Сканеры уязвимостей. Уязвимости WEB приложений.
- Средства анализа защищенности WEB приложений.

Фонд оценочных материалов (ФОМ) для проведения аттестации уровня сформированности компетенций обучающихся по дисциплине оформляется отдельным документом.

6. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

6.1. Книгообеспеченность

Наименование литературы: автор, название, вид издания, издательство	Год издания	КНИГООБЕСПЕЧЕННОСТЬ
		Наличие в электронном каталоге ЭБС
Основная литература		
Технологии обеспечения безопасности информационных систем: учебное пособие: [16+] / А. Л. Марухленко, Л. О. Марухленко, М. А. Ефремов и др. – Москва; Берлин: Директ-Медиа, 2021. – 210 с.– ISBN 978-5-4499-1671-6. – DOI 10.23681/598988	2021	https://biblioclub.ru/index.php?page=book&id=598988 (дата обращения: 18.09.2021)
Голиков, А. М. Основы проектирования защищенных телекоммуникационных систем: курс лекций, компьютерный практикум, компьютерные лабораторные работы и задание на самостоятельную работу / А. М. Голиков. – Томск: ТУСУР, 2016. – 396 с.	2016	https://biblioclub.ru/index.php?page=book&id=480796 (дата обращения: 18.09.2021)
Мэйволд, Э. Безопасность сетей: учебное пособие: [16+] / Э. Мэйволд. – 2-е изд., испр. – Москва: «ИНТУИТ», 2016. – 572 с.	2016	https://biblioclub.ru/index.php?page=book&id=429035 (дата обращения: 18.09.2021)
Бова, В. В. Основы проектирования информационных систем и технологий: учебное пособие: [16+] / В. В. Бова, Ю. А. Кравченко. – Ростов-на-Дону; Таганрог: Южный федеральный университет, 2018. – 106 с.– ISBN 978-5-9275-2717-5	2018	https://biblioclub.ru/index.php?page=book&id=499515 (дата обращения: 18.09.2021)

Пелешенко, В. С. Менеджмент инцидентов информационной безопасности защищенных автоматизированных систем управления: учебное пособие: [16+] / В. С. Пелешенко, С. В. Говорова, М. А. Лапина. – Ставрополь: Северо-Кавказский Федеральный университет (СКФУ), 2017. – 86 с.	2017	https://biblioclub.ru/index.php?page=book&id=467139 (дата обращения: 18.09.2021)
Дополнительная литература		
Методологические основы построения защищенных автоматизированных систем: учебное пособие / А. В. Душкин, О. В. Ланкин, С. В. Потехецкий и др.; Воронежский государственный университет инженерных технологий. – Воронеж: Воронежский государственный университет инженерных технологий, 2013. – 258 с. – ISBN 978-5-89448-981-0	2013	https://biblioclub.ru/index.php?page=book&id=255851 (дата обращения: 18.09.2021)
Голиков, А. М. Защита информации в инфокоммуникационных системах и сетях: учебное пособие: [16+] / А. М. Голиков; Томский Государственный университет систем управления и радиоэлектроники (ТУСУР). – Томск, 2015. – 284 с.	2015	https://biblioclub.ru/index.php?page=book&id=480637 (дата обращения: 18.09.2021)
Организация безопасной работы информационных систем: учебное пособие / Ю. Ю. Громов, Ю. Ф. Мартемьянов, Ю. К. Букурако и др.; Тамбовский государственный технический университет. – Тамбов, 2014. – 132 с..	2014	https://biblioclub.ru/index.php?page=book&id=277794 (дата обращения: 18.09.2021)

6.2. Периодические издания

- Журнал «Вопросы защиты информации». Режим доступа: http://i-vimi.ru/editions/detail.php?SECTION_ID=155/;
- Журнал "Information Security/Информационная безопасность". Режим доступа: http://www.itsec.ru/insec-about.php.
- Ежемесячный теоретический и прикладной научно-технический журнал «Информационные технологии». Режим доступа http://novtex.ru/IT/.
- «Журнал сетевых решений/LAN» -Режим доступа: http://www.osp.ru/lan/current;
- Электронный журнал «Корпоративные сети передачи данных» -Режим доступа: http://www.delpress.ru/

6.3. Интернет-ресурсы

- Образовательный сервер кафедры ИЗИ.– Режим доступа: http://edu.izi.vlsu.ru
- Информационная образовательная сеть.- Режим доступа: http://ien.izi.vlsu.ru
- Внутривузовские издания ВлГУ.– Режим доступа: http://e.lib.vlsu.ru/

7. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Занятия проводятся в следующих аудиториях ВлГУ (корпус №2) по адресу г. Владимир, ул. Белоконской, д. 3.

ауд. 408-2, Лекционная аудитория, количество студенческих мест – 50, площадь 60 м2, оснащение: мультимедийное оборудование (интерактивная доска Hitachi FX-77WD, проектор BenQ MX 503 DLP 2700ANSI XGA), ноутбук Lenovo Idea Pad B5045

ауд. 427а-2, лаборатория сетевых технологий, количество студенческих мест – 14, площадь 36 м2, оснащение: компьютерный класс с 8 рабочими станциями Core 2 Duo E8400 с выходом в Internet, 3 маршрутизатора Cisco 2800 Series, 6 маршрутизаторов Cisco 2621, 6 коммутаторов Cisco Catalyst 2960 Series, 3 коммутатора Cisco Catalyst 2950 Series, коммутатор Cisco Catalyst Express 500 Series, проектор BenQ MP 620 P, экран настенный рулонный. Лицензионное программное обеспечение: операционная система Windows 7

Профессиональная, офисный пакет приложений Microsoft Office Профессиональный плюс 2007, бесплатно распространяемое программное обеспечение: линейка интегрированных сред разработки Visual Studio Express 2012, программный продукт виртуализации Oracle VM VirtualBox 5.0.4, симулятор сети передачи данных Cisco Packet Tracer 7.0, интегрированная среда разработки программного обеспечения IntelliJ IDEA Community Edition 15.0.3.

ауд. 427б-2, УНЦ «Комплексная защита объектов информатизации», количество студенческих мест – 15, площадь 52 м2, оснащение: компьютерный класс с 7 рабочими станциями Alliance Optima P4 с выходом в Internet, коммутатор D-Link DGS-1100-16 мультимедийный комплект (проектор Toshiba TLP X200, экран настенный рулонный), прибор ST-031P «Пиранья-Р» многофункциональный поисковый, прибор «Улан-2» поисковый, виброакустический генератор шума «Соната АВ 1М», имитатор работы средств нелегального съема информации, работающих по радиоканалу «Шиповник», анализатор спектра «GoodWill GSP-827», индикатор поля «SEL SP-75 Black Hunter», устройство блокирования работы систем мобильной связи «Мозайка-3», устройство защиты телефонных переговоров от прослушивания «Прокруст 2000», диктофон Edic MINI Hunter, локатор «Родник-2К» нелинейный, комплекс проведения акустических и виброакустических измерений «Спрут мини-А», видеорегистратор цифровой Best DVR-405, генератор Шума «Гном-3»,учебно-исследовательский комплекс «Сверхширокополосные беспроводные сенсорные сети» (Nano Xaos), сканирующий приемник «Icom IC-R1500», анализатор сетей Wi-Fi Fluke AirCheck с активной антенной. Лицензионное программное обеспечение: Windows 8 Профессиональная, офисный пакет приложений Microsoft Office Профессиональный плюс 2010, бесплатно распространяемое программное обеспечение: линейка интегрированных сред разработки Visual Studio Express 2012, инструмент имитационного моделирования AnyLogic 7.2.0 Personal Learning Edition, интегрированная среда разработки программного обеспечения IntelliJ IDEA Community Edition 14.1.4.

Рабочую программу составил: заведующий кафедрой ИЗИ
д.т.н. Монахов М.Ю.____

Рецензент: Заместитель руководителя РАЦ ООО
«ИнфоЦентр» к.т.н. Вертилевский Н.В____

Программа рассмотрена и одобрена на заседании кафедры ИЗИ

Протокол № 14 от 28.06.22 года
Заведующий кафедрой д.т.н., профессор____________________________/М.Ю. Монахов/

Рабочая программа рассмотрена и одобрена на заседании учебно-методической комиссии направления 10.04.01 «Информационная безопасность»
Протокол № 14 от 28.06.22 года
Председатель комиссии д.т.н., профессор____________________________/М.Ю. Монахов/

ЛИСТ ПЕРЕУТВЕРЖДЕНИЯ
РАБОЧЕЙ ПРОГРАММЫ ДИСЦИПЛИНЫ

Рабочая программа одобрена на 20____ / 20____ учебный год

Протокол заседания кафедры № ______ от _________ года

Заведующий кафедрой _д.т.н., профессор__________________________/М.Ю. Монахов/__

(ФИО, подпись)

Рабочая программа одобрена на 20____ / 20____ учебный год

Протокол заседания кафедры № ______ от _________ года

Заведующий кафедрой _д.т.н., профессор__________________________/М.Ю. Монахов/__

(ФИО, подпись)

Рабочая программа одобрена на 20____ / 20____ учебный год

Протокол заседания кафедры № ______ от _________ года

Заведующий кафедрой _д.т.н., профессор__________________________/М.Ю. Монахов/__

(ФИО, подпись)

Рабочая программа одобрена на 20____ / 20____ учебный год

Протокол заседания кафедры № ______ от _________ года

Заведующий кафедрой _д.т.н., профессор__________________________/М.Ю. Монахов/__

(ФИО, подпись)

ЛИСТ РЕГИСТРАЦИИ ИЗМЕНЕНИЙ

в рабочую программу дисциплины

Защищенные информационные системы

образовательной программы направления подготовки *10.04.01 Информационная безопасность*

Номер изменения	Внесены изменения в части/разделы рабочей программы	Исполнитель ФИО	Основание (номер и дата протокола заседания кафедры)
1			
2			

Заведующий кафедрой _____/М.Ю. Монахов/_____

Подпись *ФИО*