Министерство науки и высшего образования Российской Федерации
Федеральное государственное автономное образовательное учреждение
высшего образования
«Национальный исследовательский ядерный университет «МИФИ»

ИНСТИТУТ ИНТЕЛЛЕКТУАЛЬНЫХ КИБЕРНЕТИЧЕСКИХ СИСТЕМ

КАФЕДРА СТРАТЕГИЧЕСКИХ ИНФОРМАЦИОННЫХ ИССЛЕДОВАНИЙ

ОДОБРЕНО УМС ИИКС

Протокол № УМС-575/01-1

от 30.08.2021 г.

РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ

ОСНОВЫ БЕЗОПАСНОЙ РАЗРАБОТКИ ПРИЛОЖЕНИЙ

Направление подготовки (специальность) [1] 10.04.01 Информационная безопасность

Семестр	**Трудоемкость, кред.**	**Общий объем курса, час.**	**Лекции, час.**	**Практич. занятия, час.**	**Лаборат. работы, час.**	**В форме практической подготовки/ В**	**СРС, час.**	**КСР, час.**	**Форма(ы) контроля, экз./зач./КР/КП**
3	2	72	8	24	0		40	0	З
Итого	2	72	8	24	0	2	40	0	

АННОТАЦИЯ

Цель дисциплины - обеспечение требуемого уровня знаний, умений и навыков студентов по разработке приложений; организации и обеспечению (проведению работ) их безопасности.

Задачи дисциплины - дать основы правовых, организационно-распорядительных, нормативных и информационных документов в области разработки приложений, тестирования и обеспечения их безопасности.

Для этого поставлены основные задачи, которые включают в себя: основы разработки приложений и тестов; выделить основные понятия, объяснить цели и задачи разработки приложений и тестирования, фазы тестирования, роли участников группы разработки приложений и тестирования; оценки рисков требований, изменение требований в процессе разработки приложений; методы оценки несоответствия приложений, анализ требований к ПО с точки зрения пригодности к разработке и эксплуатации приложений; разработка приложений на основе требований; способность принимать участие на всех этапах жизненного цикла, сопровождать информационные, автоматизированные, телекоммуникационные системы и сервисы; организация и обеспечивание необходимой защиты.

1. ЦЕЛИ И ЗАДАЧИ ОСВОЕНИЯ УЧЕБНОЙ ДИСЦИПЛИНЫ

Целями освоения учебной дисциплины «Основы безопасности разработки приложений» является получение студентами требуемого уровня знаний, умений и навыков в способности принимать участие в создании и управлении информационными системами (ИС) на всех этапах жизненного цикла; в организации безопасной эксплуатации и сопровождении ИС и сервисов, получении навыков аналитической деятельности.

Основными задачами изучения дисциплины являются:

основы правовых, организационно-распорядительных, нормативных и информационных документов в области разработки приложений, тестирования и обеспечения их безопасности;

основы разработки приложений и тестов;

выделение основных понятий (объяснить цели и задачи разработки приложений и тестирования, фазы тестирования, роли участников группы разработки приложений);

оценка рисков требований, изменение требований в процессе разработки приложений;

методы оценки несоответствия приложений, анализ требований к ПО с точки зрения пригодности к разработке и эксплуатации приложений;

разработка приложений на основе требований;

способность принимать участие на всех этапах жизненного цикла, сопровождать информационные, автоматизированные, телекоммуникационные системы и сервисы;

организация и обеспечивание необходимой защиты приложений.

2. МЕСТО УЧЕБНОЙ ДИСЦИПЛИНЫ В СТРУКТУРЕ ООП ВО

Данная учебная дисциплина входит в базовую часть профессионального модуля ООП «Обеспечение безопасности значимых объектов критической информационной инфраструктуры» ОС НИЯУ МИФИ 10.04.01 «Информационная безопасность».

Требования к «входным» знаниям, умениям и готовностям студента, необходимым при освоении данной дисциплины:

знать технологии систем безопасности и подходы безопасности; основы разработки и обеспечения безопасности приложений; потенциальные угрозы безопасности информации разрабатываемых программых приложений;

уметь оценивать знания по безопасности разработчиков; выполнять проверку кода на соответствие рекомендациям по безопасности; обеспечивать защиту разрабатываемых приложений: обнаружение, управление, противодействие и восстановление;

владеть основами детального описания архитектуры аппаратных средств; навыками тесстирования на уязвимость; обеспечения защиты разрабатываемых приложений; проверки систем безопасности.

3. ФОРМИРУЕМЫЕ КОМПЕТЕНЦИИ И ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОБУЧЕНИЯ

Универсальные и(или) общепрофессиональные компетенции:

Код и наименование компетенции	Код и наименование индикатора достижения компетенции

Профессиональные компетенции в соотвествии с задачами и объектами (областями знаний) профессиональной деятельности:

Задача профессиональной деятельности (ЗПД)	**Объект или область знания**	**Код и наименование профессиональной компетенции; Основание (профессиональный стандарт-ПС, анализ опыта)**	**Код и наименование индикатора достижения профессиональной компетенции**
проектный			
Проектирование систем обеспечения информационной безопасности (СОИБ) конкретных объектов на стадиях разработки, эксплуатации и модернизации	Средства и технологии обеспечения безопасности значимых объектов критической информационной инфраструктуры	ПК-2 [1] - Способен разрабатывать технические задания на проектирование систем обеспечения ИБ иди информационно-аналитических систем безопасности *Основание:* Профессиональный стандарт: 06.032, 06.033, 06.034	З-ПК-2[1] - Знать: формальные модели безопасности компьютерных систем и сетей; способы обнаружения и нейтрализации последствий вторжений в компьютерные системы; основные угрозы безопасности информации и модели нарушителя; в автоматизированных системах основные меры по защите информации; в автоматизированных системах; основные криптографические методы, алгоритмы, протоколы, используемые для

			защиты информации; в автоматизированных системах; технические средства контроля эффективности мер защиты информации; современные информационные технологии (операционные системы, базы данных, вычислительные сети); методы контроля защищенности информации от несанкционированного доступа и специальных программных воздействий; средства контроля защищенности информации от несанкционированного доступа. ; У-ПК-2[1] - Уметь: применять инструментальные средства проведения мониторинга защищенности компьютерных систем; анализировать основные характеристики и возможности телекоммуникационных систем по передаче информации, основные узлы и устройства современных автоматизированных систем; разрабатывать программы и методики испытаний программно-технического средства защиты информации от несанкционированного доступа и специальных воздействий на нее; проводить испытания программно-технического средства защиты информации от несанкционированного

			доступа и специальных воздействий на нее. ; В-ПК-2[1] - Владеть: основами выполнения анализа защищенности компьютерных систем с использованием сканеров безопасности; основами составлением методик тестирования систем защиты информации автоматизированных систем; основами подбора инструментальных средств тестирования систем защиты информации автоматизированных систем; основами разработки технического задания на создание программно-технического средства защиты информации от несанкционированного доступа и специальных воздействий на нее; основами разработки программ и методик испытаний программно-технического средства защиты информации от несанкционированного доступа и специальных воздействий на нее; основами испытаний программно-технического средств защиты информации от несанкционированного доступа и специальных воздействий на нее.
научно- исследовательский			
Анализ фундаментальных и прикладных проблем ИБ в условиях становления современного информационного	Фундаментальные и прикладные проблемы информационной безопасности; методы и средства проектирования,	ПК-3 [1] - Способен самостоятельно ставить конкретные задачи научных исследований в области ИБ или информационно-	З-ПК-3[1] - Знать: руководящие и методические документы уполномоченных федеральных органов исполнительной власти,

общества; выполнение научных исследований в области ИБ; подготовка по результатам научных исследований отчетов, статей, докладов на научных конференциях	моделирования и экспериментальной отработки систем, средств и технологий обеспечения информационной безопасности значимых объектов критической информационной инфраструктуры	аналитических систем безопасности и решать их с использованием новейшего отечественного и зарубежного опыта *Основание:* Профессиональный стандарт: 06.030	устанавливающие требования к организации и проведению аттестации и сертификационных испытаний средств и систем защиты сссэ от нсд, зткс; основные средства и способы обеспечения информационной безопасности, принципы построения средств и систем защиты сссэ от нсд, зткс; национальные, межгосударственные и международные стандарты, устанавливающие требования по защите информации, анализу защищенности сетей электросвязи и оценки рисков нарушения их информационной безопасности. ; У-ПК-3[1] - Уметь: организовывать сбор, обработку, анализ и систематизацию научно-технической информации, отечественного и зарубежного опыта по проблемам информационной безопасности сетей электросвязи.; В-ПК-3[1] - Владеть: организацией подготовки научно-технических отчетов, обзоров, публикаций по результатам выполненных исследований.

4. СТРУКТУРА И СОДЕРЖАНИЕ УЧЕБНОЙ ДИСЦИПЛИНЫ

Разделы учебной дисциплины, их объем, сроки изучения и формы контроля:

№ п.п	Наименование раздела учебной дисциплины	Недели	Лекции/ Практ. (семинары)/ Лабораторные работы, час.	Обязат. текущий контроль (форма*, неделя)	Максимальный балл за раздел**	Аттестация раздела (форма*, неделя)	Индикаторы освоения компетенции
	3 Семестр						
1	Основы разработки и безопасности приложений	1-8	4/12/0		25	КИ-8	З-ПК-2, У-ПК-2, В-ПК-2, З-ПК-3, У-ПК-3, В-ПК-3
2	Основы сетевой безопасности	9-16	4/12/0		25	КИ-16	З-ПК-2, У-ПК-2, В-ПК-2, З-ПК-3, У-ПК-3, В-ПК-3
	Итого за 3 Семестр		8/24/0		50		
	Контрольные мероприятия за 3 Семестр				50	З	З-ПК-2, У-ПК-2, В-ПК-2, З-ПК-3, У-ПК-3, В-ПК-3

* – сокращенное наименование формы контроля

** – сумма максимальных баллов должна быть равна 100 за семестр, включая зачет и (или) экзамен

Сокращение наименований форм текущего контроля и аттестации разделов:

Обозначение	Полное наименование
КИ	Контроль по итогам
З	Зачет

КАЛЕНДАРНЫЙ ПЛАН

Недели	Темы занятий / Содержание	Лек., час.	Пр./сем., час.	Лаб., час.
	3 Семестр	8	24	0
1-8	**Основы разработки и безопасности приложений**	4	12	0
1	**Тема 1. Выбор стратегии тестирования и разработки тестов; Тема 2. Компонентная разработка приложений** Т1. Стратегии тестирования и разработки тестов. Уровни тестирования. Технологии тестирования. Программные ошибки. Виды тестирования. Основные правила создания тестов. Общие требования. Т2. Основные концепции компонентной разработки приложений. Стандарты компонентов. Интерфейсы компонентов. Контейнеры. Метаданные. Распределенные серверные компоненты. Интегрированные среды разработки приложений.	Всего аудиторных часов		
		1	1	0
		Онлайн		
		0	0	0
2	**Тема 2. Компонентная разработка приложений; Тема 3. Основы безопасности приложений** Т 2. Модель DCOM. Спецификация Java Beans. Компонентная разработка WEB-приложений. Спецификации компонентов в архитектуре CORBA. Перспективы развития методов и средств компонентной разработки приложений. Т 3. Типичные атаки. Последствия слабой системы безопасности. Проблемы при реализации системы безопасности приложений. Роль разработчика в построении безопасных приложений. Перспективы развития методов и средств разработки приложений и обеспечения их безопасности.	Всего аудиторных часов		
		1	1	0
		Онлайн		
		0	0	0
3	**Тема 3. Основы безопасности приложений; Тема 4. Разведка.** Т 3. Целостный подход к вопросам безопасности. Подходы к вопросам безопасности приложений. Вопросы безопасности на стадиях цикла разработки. Моделирование и процесс моделирования угроз. Идентификация угроз. Пути и процесс снижения рисков. Обзор технологий безопасности. Безопасные коммуникации. Т 4. Основные термины ИБ. «Специальные» термины. Что делает настоящий хакер. Что можно взять для аудита. Модель злоумышленника. Возможности. Цели. Инструментарий. Методологии. Подходы к оценке защищенности. Классический тест на проникновение. Сканирование.	Всего аудиторных часов		
		1	1	0
		Онлайн		
		0	0	0
4	**Тема 4. Разведка** Анализ конфигурации системы. Комплексное	Всего аудиторных часов		
		1	1	0

	тестирование. Управление проектом. Своя лаборатория для хакинга. Один из главных принципов аудита. Виды результирующих отчетов. Документация в ходе тестирования. Промежуточные результаты. Основная проблема документирования. Разведывательный цикл. Цикл: коротко о главном. Что можно найти с помощью Google. Основные операторы Google. Расширенный поиск Google. Поиск уязвимых систем. Поиск паролей. (Важно!) Сайты, где можно найти информацию о компании. Whois. Traceroute. Subdomains. robots.txt.	Онлайн		
		0	0	0
5	**ПЗ 1. Протокол HTTP** Протокол HTTP	Всего аудиторных часов		
		0	2	0
		Онлайн		
		0	0	0
6	**ПЗ 2. Инъекции** Инъекции	Всего аудиторных часов		
		0	2	0
		Онлайн		
		0	0	0
7	**ПЗ 3. Атаки Cross-Site Scripting (XSS)** Атаки Cross-Site Scripting (XSS)	Всего аудиторных часов		
		0	2	0
		Онлайн		
		0	0	0
8	**ПЗ 4. Атаки на преобразование / парсинг данных** Атаки на преобразование / парсинг данных	Всего аудиторных часов		
		0	2	0
		Онлайн		
		0	0	0
9-16	**Основы сетевой безопасности**	4	12	0
9	**Тема 5. Безопасность приложений** Разработка программного обеспечения (ПО). Каскадная модель разработки ПО (waterfall). Гибкая модель разработки ПО (Agile). Application Security. Waterfall Secure SDL. Agile Secure SDL. Стандарты и методологии. Yandex SDL. Guides. Trainings. CTF. Threat Model. Security Design Review. Consulting. SAST. DAST. Fuzzing. Pentest. Bug bounty. Примеры уязвимостей. Методологии тестирования безопасности. OWASP TOP 10. A1 – injection. A1 - Injection (LDAP injection). A2 - Broken Authentication. A2 - Session Fixation. A3 - Sensitive Data Exposure. A3 - Sensitive Data Exposure. A3 - Unhandled Exeption. A4 - XML eXternal Entities (XXE). A4 – XXE. A5 - Broken Access Control. A2 - Insecure Direct Object Reference (IDOR). A6 - Security Misconfiguration. A7 - Cross Site Scripting (XSS). A8 - Insecure Deserialization. A9 - Using Components With Known Vulnerabilities. A10 - Insufficient Logging And Monitoring. За пределами OWASP TOP 10. Cross Site Request Forgery (CSRF). Server Side Request Forgery (SSRF). Open Redirect.	Всего аудиторных часов		
		1	1	0
		Онлайн		
		0	0	0
10	**Тема 6. Сетевая безопасность** Теория. Модель OSI. TCP/IP. Уязвимости канального уровня. ARP-Spoofing. STP (Spanning Tree Protocol). Атаки на STP. VLAN. VLAN Hopping. DDoS-атаки. Классификация. SYN-Flood. Атаки на ICMP. Атаки с	Всего аудиторных часов		
		1	1	0
		Онлайн		
		0	0	0

	усилением. Сканирование. Цели сканирования. NMAP. NMAP - поиск живых систем. NMAP: полное сканирование. NMAP: скрытое сканирование. Экзотические виды сканирования. NMAP: UDP-сканирование. Примеры использования NMAP.			
11	**Тема 7. Управление безопасностью; Тема 8. Технологии Security Operation Centre** Т 7. Основы управления безопасностью приложений. Проактивный подход к вопросам безопасности в процессе разработки приложений. Запуск с наименьшими привилегиями. Уменьшения периметра в местах возможных атак. Основы эшелонированной защиты. Основы работы в linux-системах. /etc/passwd (/etc/shadow). Т 8. Файлы. Определение SOC (Security Operation Centre). Технологии SOC. Поведенческий анализ. SOC: процессы. SOC: основные функции. Процессы SOC. SOC: Персонал. Роли в SOC. Соответствие. Расследование инцидентов. Реагирование на инциденты. Жизненный цикл реагирования на инциденты.	Всего аудиторных часов		
		1	1	0
		Онлайн		
		0	0	0
12	**Тема 8. Технологии Security Operation Centre** Т 8. Технологии Security Operation Centre Подготовка. Повышение защищенности. Журналирование. Что, зачем и как собирать. Автоматизация. Kill-chain. Примеры инцидентов. Кража/потеря и восстановление оборудования. Несанкционированные сервисы снаружи. Фишинговая рассылка. Реагирование. Анализ вложений. Поиск скомпрометированных хостов. Анализ хоста. Дампы памяти. Анализ дампов памяти. Анализ диска. Использование Data Protection API (DPAPI) для защиты данных. Тестирование систем безопасности приложений.	Всего аудиторных часов		
		1	1	0
		Онлайн		
		0	0	0
13	**ПЗ 5. Атаки на механизмы контроля доступа** Атаки на механизмы контроля доступа	Всего аудиторных часов		
		0	2	0
		Онлайн		
		0	0	0
14	**ПЗ 6. Server-side безопасность (SSRF, Insecure Deserialization и т.д.)** Server-side безопасность (SSRF, Insecure Deserialization и т.д.)	Всего аудиторных часов		
		0	2	0
		Онлайн		
		0	0	0
15	**ПЗ 7. Client-side безопасность (CORS, Clickjacking, DOM-based XSS, WebSockets)** Client-side безопасность (CORS, Clickjacking, DOM-based XSS, WebSockets)	Всего аудиторных часов		
		0	2	0
		Онлайн		
		0	0	0
16	**ПЗ 8. Атаки на протокол HTTP (Header Injection, Request Smuggling и т.д.)** Атаки на протокол HTTP (Header Injection, Request Smuggling и т.д.)	Всего аудиторных часов		
		0	2	0
		Онлайн		
		0	0	0

Сокращенные наименования онлайн опций:

Обозна	Полное наименование

чение	
ЭК	Электронный курс
ПМ	Полнотекстовый материал
ПЛ	Полнотекстовые лекции
ВМ	Видео-материалы
АМ	Аудио-материалы
Прз	Презентации
Т	Тесты
ЭСМ	Электронные справочные материалы
ИС	Интерактивный сайт

ТЕМЫ ПРАКТИЧЕСКИХ ЗАНЯТИЙ

Недели	**Темы занятий / Содержание**
	3 Семестр
1	**ПЗ 1. Протокол HTTP** Протокол HTTP
2	**ПЗ 2. Инъекции** Инъекции
3	**ПЗ 3. Атаки Cross-Site Scripting (XSS)** Атаки Cross-Site Scripting (XSS)
4	**ПЗ 4. Атаки на преобразование / парсинг данных** Атаки на преобразование / парсинг данных
5	**ПЗ 1. Протокол HTTP** Протокол HTTP
6	**ПЗ 2. Инъекции** Инъекции
7	**ПЗ 3. Атаки Cross-Site Scripting (XSS)** Атаки Cross-Site Scripting (XSS)
8	**ПЗ 4. Атаки на преобразование / парсинг данных** Атаки на преобразование / парсинг данных
9	**ПЗ 5. Атаки на механизмы контроля доступа** Атаки на механизмы контроля доступа
10	**ПЗ 6. Server-side безопасность (SSRF, Insecure Deserialization и т.д.)** Server-side безопасность (SSRF, Insecure Deserialization и т.д.)
11	**ПЗ 7. Client-side безопасность (CORS, Clickjacking, DOM-based XSS, WebSockets)** Client-side безопасность (CORS, Clickjacking, DOM-based XSS, WebSockets)
12	**ПЗ 8. Атаки на протокол HTTP (Header Injection, Request Smuggling и т.д.)** Атаки на протокол HTTP (Header Injection, Request Smuggling и т.д.)
13	**ПЗ 5. Атаки на механизмы контроля доступа** Атаки на механизмы контроля доступа
14	**ПЗ 6. Server-side безопасность (SSRF, Insecure Deserialization и т.д.)** Server-side безопасность (SSRF, Insecure Deserialization и т.д.)

15	**ПЗ 7. Client-side безопасность (CORS, Clickjacking, DOM-based XSS, WebSockets)** Client-side безопасность (CORS, Clickjacking, DOM-based XSS, WebSockets)
16	**ПЗ 8. Атаки на протокол HTTP (Header Injection, Request Smuggling и т.д.)** Атаки на протокол HTTP (Header Injection, Request Smuggling и т.д.)

5. ОБРАЗОВАТЕЛЬНЫЕ ТЕХНОЛОГИИ

В соответствии с целью формирования и развития профессиональных навыков студентов и требованиями ОС НИЯУ МИФИ по направлению подготовки реализация компетентностного подхода предусматривает в учебном процессе широкое использование активных и интерактивных форм проведения занятий в сочетании с внеаудиторной работой.

Цель обучения достигается сочетанием применения традиционных и инновационных педагогических технологий, направленных на развитие познавательной активности, творческой самостоятельности студентов. Последовательное и целенаправленное выдвижение перед студентом познавательных задач, решая которые студенты активно усваивают знания; поисковые методы; постановка познавательных задач.

6. ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

Фонд оценочных средств по дисциплине обеспечивает проверку освоения планируемых результатов обучения (компетенций и их индикаторов) посредством мероприятий текущего, рубежного и промежуточного контроля по дисциплине.

Связь между формируемыми компетенциями и формами контроля их освоения представлена в следующей таблице:

Компетенция	**Индикаторы освоения**	**Аттестационное мероприятие (КП 1)**
ПК-2	З-ПК-2	З, КИ-8, КИ-16
	У-ПК-2	З, КИ-8, КИ-16
	В-ПК-2	З, КИ-8, КИ-16
ПК-3	З-ПК-3	З, КИ-8, КИ-16
	У-ПК-3	З, КИ-8, КИ-16
	В-ПК-3	З, КИ-8, КИ-16

Шкалы оценки образовательных достижений

Шкала каждого контрольного мероприятия лежит в пределах от 0 до установленного максимального балла включительно. Итоговая аттестация по дисциплине оценивается по 100-балльной шкале и представляет собой сумму баллов, заработанных студентом при выполнении заданий в рамках текущего и промежуточного контроля.

Итоговая оценка выставляется в соответствии со следующей шкалой:

Сумма	Оценка по 4-ех	Оценка	Требования к уровню освоению

баллов	балльной шкале	ECTS	учебной дисциплины
90-100	5 – *«отлично»*	A	Оценка «отлично» выставляется студенту, если он глубоко и прочно усвоил программный материал, исчерпывающе, последовательно, четко и логически стройно его излагает, умеет тесно увязывать теорию с практикой, использует в ответе материал монографической литературы.
85-89	4 – «*хорошо*»	B	Оценка «хорошо» выставляется студенту, если он твёрдо знает материал, грамотно и по существу излагает его, не допуская существенных неточностей в ответе на вопрос.
75-84		C	
70-74		D	
65-69	3 – «*удовлетворительно*»		Оценка «удовлетворительно» выставляется студенту, если он имеет знания только основного материала, но не усвоил его деталей, допускает неточности, недостаточно правильные формулировки, нарушения логической последовательности в изложении программного материала.
60-64		E	
Ниже 60	2 – «*неудовлетворительно*»	F	Оценка «неудовлетворительно» выставляется студенту, который не знает значительной части программного материала, допускает существенные ошибки. Как правило, оценка «неудовлетворительно» ставится студентам, которые не могут продолжить обучение без дополнительных занятий по соответствующей дисциплине.

7. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ УЧЕБНОЙ ДИСЦИПЛИНЫ

ОСНОВНАЯ ЛИТЕРАТУРА:

1. ЭИ Р 15 Базы данных: основы, проектирование, разработка информационных систем, проекты. Курс лекций : учеб. пособие, Москва: НИЯУ МИФИ, 2020

2. 004 А27 AJAX и PHP. Разработка динамических веб-приложений : , К. Дари [и др.], Санкт-Петербург - Москва: Символ, 2009

3. ЭИ З-17 Применение методов Data Mining для поддержки процессов управления IT-услугами : учебное пособие, К. С. Зайцев, Москва: НИЯУ МИФИ, 2009

4. 004 Х79 Методы и средства защиты информации в компьютерных системах : учебное пособие для вузов, П. Б. Хорев, Москва: Академия, 2008

ДОПОЛНИТЕЛЬНАЯ ЛИТЕРАТУРА:

1. ЭИ Г 12 Разработка и эксплуатация автоматизированных информационных систем : , Москва: Форум, 2019

2. ЭИ Ч-49 Управление качеством программного обеспечения : , Москва: Форум, 2020

3. 65 К72 Автоматизированные системы управления безопасной ресурососберегающей эксплуатацией оборудования нефтеперерабатывающих и нефтехимических производств(АСУ БЭР-Компакс) : , Костюков В.Н.,Бойченко С.Н.,Костюков А.В., М.: Машиностроение, 1999

4. 004 В27 Разработка веб-приложений с помощью PHP и MySQL : , ЛюкВеллинг, ЛораТомсон, Москва [и др.]: Вильямс, 2010

ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ:

Специальное программное обеспечение не требуется

LMS И ИНТЕРНЕТ-РЕСУРСЫ:

https://online.mephi.ru/

http://library.mephi.ru/

8. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ УЧЕБНОЙ ДИСЦИПЛИНЫ

Специальное материально-техническое обеспечение не требуется

9. УЧЕБНО-МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ ДЛЯ СТУДЕНТОВ

Настоящие методические указания раскрывают рекомендуемый режим и характер учебной работы по изучению теоретических разделов курса, практическому применению изученного материала, по выполнению самостоятельной работы путем использования лекционного материала. Методические указания служат основой мотивации студента к самостоятельной работе и не подменяют рекомендуемую учебную литературу.

Данные указания определяют взаимосвязь курса с другими учебными дисциплинами образовательной программы – «Обеспечение безопасности значимых объектов критической информационной инфраструктуры», место курса в различных областях науки и техники. В том числе в области защиты программых приложений; в профессиональной деятельности выпускника; требования образовательного стандарта к уровню его подготовки; содержание дисциплины, сущность и краткая характеристика входящих в нее разделов, их взаимосвязь, особенности организации образовательного процесса по данной дисциплине специальности.

Особенности изучения разделов дисциплины

В процессе изучения данной дисциплины необходимо использовать действующие правовые акты в области защиты информации и разработки приложений, организационно-распорядительные, нормативные и информационные документы ФСТЭК России, других уполномоченных органов государственной власти, а также соответствующие учебно-методические пособия, иллюстративный материал (презентации).

На лекционных занятиях излагаются наиболее важные и сложные вопросы, являющиеся теоретической основой построения измерительных комплексов по анализу защищенности объектов информатизации и проведению инструментальных специальных исследований при аттестации объектов информатизации по требованиям безопасности информации. Часть лекций может излагаться проблемным методом с привлечением студентов для решения сформулированной преподавателем проблемы. С целью текущего контроля знаний в ходе лекций могут использоваться различные приёмы тестирования.

Проведение лабораторных работ - не предусмотренно.

На практических занятиях выносятся вопросы уровня навыков и умений. Задания выполняются студентами с использованием сети Интернет. На каждом рабочем месте должен быть развернут персональный компьютер (АРМ) с выходом в интернет. Результаты, полученные в ходе практических занятий, используются студентами в качестве исходных данных при отработке итоговых пакетов документов.

В качестве форм промежуточного контроля полученных знаний (раздел 1 и 2) используются: контрольная работа и тестирование. Для повышения результатов контроля студентами (по их желанию) могут быть выполнены и использованы письменные работы (рефераты).

В процессе итогового контроля также могут использоваться результаты, полученные студентами на практических занятиях.

10. УЧЕБНО-МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ ДЛЯ ПРЕПОДАВАТЕЛЕЙ

Настоящие методические указания раскрывают рекомендуемый режим и характер учебной работы по изучению теоретических разделов курса, практическому применению изученного материала, по выполнению самостоятельной работы путем использования лекционного материала. Методические указания служат основой мотивации студента к самостоятельной работе и не подменяют рекомендуемую учебную литературу.

Данные указания определяют взаимосвязь курса с другими учебными дисциплинами образовательной программы – «Обеспечение безопасности значимых объектов критической информационной инфраструктуры», место курса в различных областях науки и техники. В том числе в области защиты программых приложений; в профессиональной деятельности выпускника; требования образовательного стандарта к уровню его подготовки; содержание дисциплины, сущность и краткая характеристика входящих в нее разделов, их взаимосвязь, особенности организации образовательного процесса по данной дисциплине специальности.

Особенности изучения разделов дисциплины

В процессе изучения данной дисциплины необходимо использовать действующие правовые акты в области защиты информации и разработки приложений, организационно-распорядительные, нормативные и информационные документы ФСТЭК России, других уполномоченных органов государственной власти, а также соответствующие учебно-методические пособия, иллюстративный материал (презентации).

На лекционных занятиях излагаются наиболее важные и сложные вопросы, являющиеся теоретической основой построения измерительных комплексов по анализу защищенности объектов информатизации и проведению инструментальных специальных исследований при аттестации объектов информатизации по требованиям безопасности информации. Часть лекций может излагаться проблемным методом с привлечением студентов для решения

сформулированной преподавателем проблемы. С целью текущего контроля знаний в ходе лекций могут использоваться различные приёмы тестирования.

Проведение лабораторных работ - не предусмотренно.

На практических занятиях выносятся вопросы уровня навыков и умений. Задания выполняются студентами с использованием сети Интернет. На каждом рабочем месте должен быть развернут персональный компьютер (АРМ) с выходом в интернет. Результаты, полученные в ходе практических занятий, используются студентами в качестве исходных данных при отработке итоговых пакетов документов.

В качестве форм промежуточного контроля полученных знаний (раздел 1 и 2) используются: контрольная работа и тестирование. Для повышения результатов контроля студентами (по их желанию) могут быть выполнены и использованы письменные работы (рефераты).

В процессе итогового контроля также могут использоваться результаты, полученные студентами на практических занятиях.

1. Чтение лекций.

Первая лекция должна быть введением к дисциплине (разделу дисциплины, читаемому в начинающемся семестре). Она должна содержать общий обзор содержания дисциплины. В ней следует отметить методические инновации в решении задач, рассматриваемых в дисциплине, дать перечень рекомендованной литературы и вновь появившихся литературных источников, обратив внимание студентов на обязательную и дополнительную литературу.

Изложению текущего лекционного материала должна предшествовать вводная часть, содержащая краткий перечень вопросов, рассмотренных на предыдущих лекциях. На этом этапе полезно задать несколько вопросов аудитории, осуществить выборочный контроль знания студентов.

При изложении лекционного материала следует поощрять вопросы непосредственно в процессе изложения, внимательно относясь к вопросам студентов и при необходимости давая дополнительные, более подробные пояснения.

При чтении лекций преимущественное внимания следует уделять качественным вопросам, опуская простые математические выкладки, либо рекомендуя выполнить их самим студентам, либо отсылая студентов к литературным источникам и методическим пособиям.

В процессе лекционного курса необходимо возможно чаще возвращаться к основным вопросам дисциплины, проводя выборочный экспресс-контроль знаний студентов.

Принятая преподавателем система обозначений должна чётко разъясняться в процессе её введения и использоваться в конспектах лекций.

В лекциях, предшествующих практическим занятиям, следует кратко излагать содержание и основные задачи практического занятия, дать рекомендации студентам для подготовки к нему.

На последней лекции важно найти время для обзора основных положений, рассмотренных в дисциплине, перечню и формулировке вопросов, выносимых на экзамен или зачёт.

2. Указания по контролю самостоятельной работы студентов.

По усмотрению преподавателя задание на самостоятельную работу может быть индивидуальным или фронтальным.

При использовании индивидуальных заданий требовать от студента письменный отчет о проделанной работе, проводить его обсуждение.

При применении фронтальных заданий вести коллективные обсуждения со студентами основных теоретических положений.

С целью контроля качества выполнения самостоятельной работы требовать индивидуальные отчеты (допустимо вместо письменного отчета применять индивидуальные контрольные вопросы).

Автор(ы):

Гавдан Григорий Петрович

Рецензент(ы):

Горбатов В.С.