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

ИНСТИТУТ ИНТЕЛЛЕКТУАЛЬНЫХ КИБЕРНЕТИЧЕСКИХ СИСТЕМ

КАФЕДРА КРИПТОЛОГИИ И ДИСКРЕТНОЙ МАТЕМАТИКИ

ОДОБРЕНО УМС ИИКС

Протокол № 8/1/2024

от 28.08.2024 г.

РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ

ВЫЯВЛЕНИЕ УЯЗВИМОСТЕЙ (СКАНЕРЫ, MBSA)

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**
2	3	108	30	15	15		12	0	Э
Итого	3	108	30	15	15	0	12	0	

АННОТАЦИЯ

Цель дисциплины – ознакомление студентов с теоретическими и практическими аспектами анализа уязвимостей и общими принципами защиты программного обеспечения (ПО) для повышения безопасности разработки и эксплуатации информационных систем различного назначения.

Основные задачи дисциплины: ознакомление студентов с причинами возникновения и принципами эксплуатации уязвимостей в программном коде, изучение практических примеров уязвимостей в программном коде; изучение принципов анализа кода, внутреннего представления программы для анализа, ознакомление с принципами работы статистических и динамических анализаторов кода;

Изучение принципов создания безопасного ПО и современных методов защиты исходных и байт кодов программ; овладение практическими навыками формирования комплекса мер для повышения качества разработки ПО.

1. ЦЕЛИ И ЗАДАЧИ ОСВОЕНИЯ УЧЕБНОЙ ДИСЦИПЛИНЫ

Цель дисциплины – ознакомление студентов с теоретическими и практическими аспектами анализа уязвимостей и общими принципами защиты программного обеспечения (ПО) для повышения безопасности разработки и эксплуатации информационных систем различного назначения.

Основные задачи дисциплины: ознакомление студентов с причинами возникновения и принципами эксплуатации уязвимостей в программном коде, изучение практических примеров уязвимостей в программном коде; изучение принципов анализа кода, внутреннего представления программы для анализа, ознакомление с принципами работы статистических и динамических анализаторов кода;

Изучение принципов создания безопасного ПО и современных методов защиты исходных и байт кодов программ; овладение практическими навыками формирования комплекса мер для повышения качества разработки ПО.

2. МЕСТО УЧЕБНОЙ ДИСЦИПЛИНЫ В СТРУКТУРЕ ООП ВО

дисциплина специализации

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;**	**Код и наименование индикатора достижения профессиональной**

		Основание (профессиональный стандарт-ПС, анализ опыта)	**компетенции**
научно-исследовательский			
выполнение научно-исследовательских работ по развитию методов обеспечения информационной безопасности	методы обеспечения информационной безопасности	ПК-8.1 [1] - Способен проводить мониторинг и проверку эффективности системы управления информационной безопасностью, а также непрерывное улучшение системы управления информационной безопасностью, основанное на результатах объективных измерений *Основание:* Профессиональный стандарт: 06.032	З-ПК-8.1[1] - Знать: основные методы мониторинга и повышения защищенности информации ; У-ПК-8.1[1] - Уметь: применять методики мониторинга и повышения защищенности информации; В-ПК-8.1[1] - Владеть: практическими навыками мониторинга и повышения защищенности информации конкретных организаций, в том числе объектов критической инфраструктуры
проектный			
разработка проектных решений по обеспечению информационной безопасности	информационные ресурсы	ПК-8.3 [1] - Способен реализовывать требования информационной безопасности организации, устанавливать политики и цели информационной безопасности *Основание:* Профессиональный стандарт: 06.032	З-ПК-8.3[1] - Знать: нормативную и правовую базу обеспечения информационной безопасности; У-ПК-8.3[1] - Уметь: применять положения нормативной и правовой базы, осуществлять выбор мер по обеспечению безопасности; В-ПК-8.3[1] - Владеть: практическими навыками применения нормативной и правовой базы обеспечения информационной безопасности и осуществлять реализацию мер по обеспечению информационной безопасности
организационно-управленческий			
организовать эффективную работу	информационные ресурсы	ПК-8 [1] - Способен использовать навыки	З-ПК-8[1] - Знать: профессиональная и

по защите информационных ресурсов организации		составления и оформления организационно-нормативных документов, научных отчетов, обзоров, докладов и статей в области ИБ или в области информационно-аналитических систем безопасности *Основание:* Профессиональный стандарт: 06.032	криптографическая терминология в области безопасности информации; эталонная модель взаимодействия открытых систем, основные протоколы, последовательность и содержание этапов построения и функционирования современных локальных и глобальных компьютерных сетей; принципы работы элементов и функциональных узлов электронной аппаратуры, типовые схемотехнические решения основных узлов и блоков электронной аппаратуры; принципы организации документирования разработки и процесса сопровождения программного и аппаратного обеспечения. организационно-распорядительная документация по защите информации на объекте информатизации; современные информационные технологии (операционные системы, базы данных, вычислительные сети); технические каналы утечки акустической речевой информации; методы защиты информации от утечки по техническим каналам; способы защиты акустической речевой информации от утечки по техническим каналам. ; У-ПК-8[1] - Уметь: анализировать

			программные, архитектурно-технические и схемотехнические решения компонентов автоматизированных систем с целью выявления потенциальных уязвимостей безопасности информации в автоматизированных системах; проводить комплексное тестирование аппаратных и программных средств; определять перечень информации (сведений)ограниченного доступа, подлежащих защите в организации; определять условия расположения объектов информатизации относительно границ контролируемой зоны; разрабатывать аналитическое обоснование необходимости создания системы защиты информации в организации; разрабатывать разрешительную систему доступа к информационным ресурсам, программным и техническим средствам автоматизированных (информационных) систем организации. ; В-ПК-8[1] - Владеть: основами применения средств схемотехнического проектирования и современной измерительной аппаратуры; основами оптимизации работ электронных схем с учетом требований по

			защите информации; основами организации проведения научных исследований по вопросам технической защиты информации, выполняемых в организации.

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
	2 Семестр						
1	Первый раздел	1-8	15/8/8		25	КИ-8	З-ПК-8.1, У-ПК-8.1, В-ПК-8.1, З-ПК-8.3, У-ПК-8.3, В-ПК-8.3, З-ПК-8, У-ПК-8, В-ПК-8
2	Второй раздел	9-15	15/7/7		25	КИ-15	З-ПК-8.1, У-ПК-8.1, В-ПК-8.1, З-ПК-8.3, У-ПК-8.3, В-ПК-8.3, З-ПК-8, У-ПК-8, В-ПК-8
	Итого за 2 Семестр		30/15/15		50		
	Контрольные мероприятия за 2 Семестр				50	Э	З-ПК-8, У-ПК-8, В-ПК-8, З-ПК-8.1, У-ПК-8.1, В-ПК-8.1, З-ПК-8.3, У-ПК-8.3, В-ПК-8.3

* – 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
Э	Экзамен

КАЛЕНДАРНЫЙ ПЛАН

Недели	**Темы занятий / Содержание**	**Лек., час.**	**Пр./сем., час.**	**Лаб., час.**
	2 Семестр	30	15	15
1-8	**Первый раздел**	15	8	8
	Теоретические	Всего аудиторных часов		
		15	8	8
	1. Понятие и классификация уязвимостей. 2. Причины возникновения уязвимостей в программном коде и принципы их эксплуатации. 3. Уязвимости переполнения буфера в стеке. 4. Уязвимости переполнения буфера в куче. 5. Методы обнаружения и предотвращения переполнения буфера. 6. Уязвимость форматной строки. 7. Уязвимость переполнения целых чисел. 8. Эксплойты.	Онлайн		
		15	0	0
9-15	**Второй раздел**	15	7	7
	Практические	Всего аудиторных часов		
		7	4	4
	9. Практические примеры уязвимостей в программном коде. 10. Типовые сценарии выявления уязвимостей в программном коде. 11. Статические и динамические анализаторы кода. 12. Тестирование по принципу «белого ящика». 13. Файззингтестирование.	Онлайн		
		7	0	0

	14. Повышение качества разработки ПО при использовании специализированных программных средств.			
	Методы защиты программного 15. Принципы создания безопасного ПО. 16. Современные методы защиты ПО от взлома. 17. Технические меры защиты ПО. 18. Защита кода от анализа. 19. Принципы работы обфускаторов исходных и байткодов.	Всего аудиторных часов		
		8	3	3
		Онлайн		
		8	0	0

Сокращенные наименования онлайн опций:

Обозначение	**Полное наименование**
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 ЛАБОРАТОРНЫХ РАБОТ

Недели	**Темы занятий / Содержание**
	2 Семестр
	Л/Р 3 Типовые сценарии выявления уязвимостей в программном коде
	Л/Р 4 Современные методы защиты ПО от взлома
	Л/Р 1 Уязвимости переполнения буфера в куче
	Л/Р 2 Методы обнаружения и предотвращения переполнения буфера

5. ОБРАЗОВАТЕЛЬНЫЕ ТЕХНОЛОГИИ

Образовательные технологии (лекции, практические работы с компьютерными программами, лабораторные работы) сочетают в себе совокупность методов и средств для реализации определенного содержания обучения и воспитания в рамках дисциплины, включают решение дидактических и воспитательных задач, формируя основные понятия дисциплины,

технологии проведения занятиий, усвоения новых знаний, технологии повторения и контроля материала, самостоятельной работы.

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-8	З-ПК-8	Э, КИ-8, КИ-15
	У-ПК-8	Э, КИ-8, КИ-15
	В-ПК-8	Э, КИ-8, КИ-15
ПК-8.1	З-ПК-8.1	Э, КИ-8, КИ-15
	У-ПК-8.1	Э, КИ-8, КИ-15
	В-ПК-8.1	Э, КИ-8, КИ-15
ПК-8.3	З-ПК-8.3	Э, КИ-8, КИ-15
	У-ПК-8.3	Э, КИ-8, КИ-15
	В-ПК-8.3	Э, КИ-8, КИ-15

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 баллов	Оценка по 4-ех балльной шкале	Оценка ECTS	Требования к уровню освоению 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,
60-64		E	

			нарушения логической последовательности в изложении программного материала.
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:

ДОПОЛНИТЕЛЬНАЯ ЛИТЕРАТУРА:

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

Студенты должны своевременно спланировать учебное время для поэтапного и системного изучения данной учебной дисциплины в соответствии с планом лекций и семинарских занятий, графиком контроля знаний.

Успешное освоение дисциплины требует от студентов посещения лекций, активной работы во время семинарских занятий, выполнения всех домашних заданий, ознакомления с базовыми учебниками, основной и дополнительной литературой, а также предполагает творческое участие студента путем планомерной, повседневной работы.

Изучение дисциплины следует начинать с проработки учебной программы, особое внимание, уделяя целям и задачам, структуре и содержанию курса.

Во время лекций рекомендуется писать конспект. Запись лекции – одна из форм активной самостоятельной работы студентов, требующая навыков и умения кратко,

схематично, последовательно и логично фиксировать основные положения, выводы, обобщения, формулировки.

При необходимости в конце лекции преподаватель оставляет время для того, чтобы студенты имели возможность задать вопросы по изучаемому материалу.

Лекции нацелены на освещение основополагающих положений теории алгоритмов и теории функций алгебры логики, наиболее трудных вопросов, как правило, связанных с доказательством необходимых утверждений и теорем, призваны способствовать формированию навыков работы с научной литературой. Предполагается также, что студенты приходят на лекции, предварительно проработав соответствующий учебный материал по источникам, рекомендуемым программой.

Конспект лекций для закрепления полученных знаний необходимо просмотреть сразу после занятий. Хорошо отметить материал конспекта лекций, который вызывает затруднения для понимания. Можно попытаться найти ответы на затруднительные вопросы, используя рекомендуемую литературу. Если самостоятельно не удалось разобраться в материале, рекомендуется сформулировать вопросы и обратиться за помощью к преподавателю на консультации или ближайшей лекции.

В процессе изучения учебной дисциплины необходимо обратить внимание на самоконтроль. Требуется регулярно отводить время для повторения пройденного материала, проверяя свои знания, умения и навыки по контрольным вопросам, а также для выполнения домашних заданий, которые выдаются после каждого семинара.

Систематическая индивидуальная работа, постоянная активность на занятиях, готовность ставить и обсуждать актуальные проблемы курса – залог успешной работы и положительной оценки.

10. УЧЕБНО-МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ ДЛЯ ПРЕПОДАВАТЕЛЕЙ

навыки, получаемые студентами в ходе лекций, аудиторных практических занятий, лабораторных и самостоятельных занятий.

Данная дисциплина выполняет функции теоретической и практической подготовки студентов. Содержание дисциплины распределяется между лекционной и практической частями на основе принципа дополняемости: практические занятия, как правило, не дублируют лекции и посвящены рассмотрению практических примеров и конкретизации материала, введенного на лекции. В лекционном курсе главное место отводится общетеоретическим проблемам.

Содержание учебного курса, его объем и характер обусловливают необходимость оптимизации учебного процесса в плане отбора материала обучения и методики его организации, а также контроля текущей учебной работы. В связи с этим возрастает значимость и изменяется статус внеаудиторной (самостоятельной) работы, которая становится полноценным и обязательным видом учебно-познавательной деятельности студентов. При изучении курса самостоятельная работа включает:

самостоятельное ознакомление студентов с теоретическим материалом, представленным в отечественных и зарубежных научно-практических публикациях;

самостоятельное изучение тем учебной программы, достаточно хорошо обеспеченных литературой и сравнительно несложных для понимания;

подготовку к практическим занятиям по тем разделам, которые не дублируют темы лекционной части, а потому предполагают самостоятельную проработку материала учебных пособий.

Со стороны преподавателя должен быть установлен контакт со студентами, и они должны быть информированы о порядке прохождения курса, его особенностях, учебно-методическом обеспечении по данной дисциплине. Преподаватель дает методические рекомендации обучаемым по самостоятельному изучению проблем, характеризуя пути и средства достижения поставленных перед ними задач, высказывает советы и рекомендации по изучению учебной литературы, самостоятельной работе и работе на семинарских занятиях.

Автор(ы):

Епишкина Анна Васильевна, к.т.н.