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 КИБЕРБЕЗОПАСНОСТИ

ОДОБРЕНО УМС ИИКС

Протокол № 8/1/2025

от 25.08.2025 г.

РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ

БЕЗОПАСНОСТЬ ОПЕРАЦИОННЫХ СИСТЕМ (АДМИНИСТРИРОВАНИЕ)

Направление подготовки (специальность) [1] 10.03.01 Информационная безопасность

Семестр	Трудоемкость, кред.	Общий объем курса, час.	Лекции, час.	Практич. занятия, час.	Лаборат. работы, час.	В форме практической подготовки, час.	СРС, час.	КСР, час.	Форма(ы) контроля, экз./зач./КР/КП
6	2-3	72-108	15	0	15		24-42	0	Э , 3
Итого	2-3	72-108	15	0	15	0	24-42	0	

АННОТАЦИЯ

Цель - подготовить специалиста, который умеет не только глубоко понимать, как устроены современные операционные системы, но и грамотно настраивать их подсистемы безопасности, а также эффективно администрировать эти механизмы на практике

1. ЦЕЛИ И ЗАДАЧИ ОСВОЕНИЯ УЧЕБНОЙ ДИСЦИПЛИНЫ

Цель - подготовить специалиста, который умеет не только глубоко понимать, как устроены современные операционные системы, но и грамотно настраивать их подсистемы безопасности, а также эффективно администрировать эти механизмы на практике

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**
ОПК-1.2 [1] – Способен администрировать средства защиты информации в компьютерных системах и сетях	З-ОПК-1.2 [1] – знать принципы администрирования средств защиты информации в компьютерных системах и сетях У-ОПК-1.2 [1] – уметь администрировать средства защиты информации в компьютерных системах и сетях В-ОПК-1.2 [1] – владеть приемами администрирования средств защиты информации в компьютерных системах и сетях
ОПК-1.1 [1] – Способен разрабатывать и реализовывать политики управления доступом в компьютерных системах	З-ОПК-1.1 [1] – знать способы разработки политик управления доступом и информационными потоками в компьютерных системах У-ОПК-1.1 [1] – разрабатывать политики управления доступом и информационными потоками в компьютерных системах В-ОПК-1.1 [1] – владеть принципами формирования политики управления доступом и информационными потоками в компьютерных системах

Профессиональные компетенции в соответствии 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**

		Основание (профессиональный стандарт-ПС, анализ опыта)	**профессиональной компетенции**
проектно-технологический			
проектирование и разработка систем информационной безопасности	технологии обеспечения информационной безопасности компьютерных систем	ПК-1.4 [1] - способен проектировать, внедрять и поддерживать интегрированные процессы обеспечения информационной безопасности в средах разработки, тестирования и эксплуатации программного обеспечения *Основание:* Профессиональный стандарт: 06.032	З-ПК-1.4[1] - знать принципы автоматизации процессов жизненного цикла программного обеспечения от сборки до реагирования на инциденты; У-ПК-1.4[1] - уметь обосновывать выбор используемых программно-аппаратных средств защиты информации в компьютерных сетях; В-ПК-1.4[1] - владеть навыками управления жизненным циклом безопасной разработки
проектирование и разработка систем информационной безопасности	технологии обеспечения информационной безопасности компьютерных систем	ПК-2 [1] - способен проектировать подсистемы безопасности информации с учетом действующих нормативных и методических документов *Основание:* Профессиональный стандарт: 06.032	З-ПК-2[1] - знать действующие нормативные и методические документы по проектированию подсистемы безопасности информации ; У-ПК-2[1] - уметь проектировать подсистемы безопасности информации с учетом действующих нормативных и методических документов; В-ПК-2[1] - владеть принципами проектирования подсистемы безопасности информации
эксплуатационный			
эксплуатация	программно-	ПК-1.3 [1] - способен	З-ПК-1.3[1] - знать

технических и программно-аппаратных средств защиты информации	аппаратные средства защиты информации	настраивать и поддерживать различные семейства операционных систем, систем управления базами данных, диагностировать сетевые проблемы *Основание:* Профессиональный стандарт: 06.032	основы администрирования различных семейств операционных систем, основы администрирования систем управления базами данных, принципы сетевого взаимодействия, принципы построения корпоративных сетей, криптографические протоколы; У-ПК-1.3[1] - уметь управлять учетными записями и привилегиями в операционных системах и системах управления базами данных, анализировать журналы событий развертывать и администрировать средства анализа защищенности, диагностировать сетевые проблемы, автоматизировать задачи с помощью скриптовых языков; В-ПК-1.3[1] - владеть навыками настройки различных типов операционных систем, систем управления базами данных

4. ВОСПИТАТЕЛЬНЫЙ ПОТЕНЦИАЛ ДИСЦИПЛИНЫ

Направления/цели воспитания	**Задачи воспитания (код)**
Профессиональное воспитание	Создание условий, обеспечивающих, формирование культуры информационной безопасности (В23)
Профессиональное воспитание	Создание условий, обеспечивающих, формирование профессионально значимых установок: не производить, не копировать и не использовать программные и технические средства, не приобретённые на законных основаниях; не нарушать признанные нормы

	авторского права; не нарушать тайны передачи сообщений, не практиковать вскрытие информационных систем и сетей передачи данных; соблюдать конфиденциальность доверенной информации (В40)

5. 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
	6 Семестр						
1	Первый раздел	1-8	8/0/8		25	КИ-8	З-ОПК-1.2, У-ОПК-1.2, В-ОПК-1.2, З-ОПК-1.1, У-ОПК-1.1, В-ОПК-1.1, З-ПК-1.4, У-ПК-1.4, В-ПК-1.4, З-ПК-1.3, У-ПК-1.3, В-ПК-1.3, З-ПК-2, У-ПК-2, В-ПК-2
2	Второй раздел	9-15	7/0/7		25	КИ-15	З-ОПК-1.2, У-ОПК-1.2, В-ОПК-1.2, З-ОПК-1.1, У-ОПК-1.1, В-ОПК-1.1, З-ПК-1.4, У-ПК-1.4, В-ПК-1.4, З-ПК-1.3, У-ПК-1.3, В-ПК-1.3, З-ПК-2, У-ПК-2, В-ПК-2

	Итого за 6 Семестр		15/0/15		50		
	Контрольные мероприятия за 6 Семестр				50	З, Э	З-ОПК-1.2, У-ОПК-1.2, В-ОПК-1.2, З-ОПК-1.1, У-ОПК-1.1, В-ОПК-1.1, З-ПК-1.4, У-ПК-1.4, В-ПК-1.4, З-ПК-1.3, У-ПК-1.3, В-ПК-1.3, З-ПК-2, У-ПК-2, В-ПК-2, З-ОПК-1.2, У-ОПК-1.2, В-ОПК-1.2, З-ОПК-1.1, У-ОПК-1.1, В-ОПК-1.1, З-ПК-1.4, У-ПК-1.4, В-ПК-1.4, З-ПК-1.3, У-ПК-1.3, В-ПК-1.3, З-ПК-2, У-ПК-2, В-ПК-2

* – 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.**
	6 Семестр	15	0	15
1-8	**Первый раздел**	8	0	8
1	**Стандарты безопасной настройки ОС. Профили защиты ФСТЭК** Настройка ОС в соответствии с требованиями профиля	Всего аудиторных часов		
		1	0	1
		Онлайн		

	защиты	0	0	0
2	**Доверенная загрузка (Trusted Boot)** Настройка пароля на GRUB, внедрение UEFI Secure Boot с собственными ключами. Контроль параметров загрузки ядра.	Всего аудиторных часов		
		1	0	1
		Онлайн		
		0	0	0
3	**Квоты и шифрование файловых систем** Создание зашифрованных разделов LUKS (с разблокировкой по TPM/флешке). Настройка дисковых квот	Всего аудиторных часов		
		1	0	1
		Онлайн		
		0	0	0
4	**Мандатное управление доступом (MAC). Система SELinux** Работа с контекстами, типами и булевыми переключателями. Устранение блокировок через анализ audit.log (без отключения SELinux).	Всего аудиторных часов		
		1	0	1
		Онлайн		
		0	0	0
5	**LSM: Разработка политик SELinux** Создание собственного модуля политики (.te, .fc) для кастомного приложения, работающего в нестандартном порту или директории.	Всего аудиторных часов		
		1	0	1
		Онлайн		
		0	0	0
6	**Администрирование SELinux** Диагностика отказов доступа через логи аудита, управление контекстами файлов и сетевых портов. Тонкая настройка прав сервисов с помощью булевых переключателей (Booleans) без отключения защиты.	Всего аудиторных часов		
		1	0	1
		Онлайн		
		0	0	0
7 - 8	**Система аутентификации PAM** Настройка двухфакторной аутентификации для SSH/Sudo. Ограничение доступа через pam_access и pam_limits	Всего аудиторных часов		
		2	0	2
		Онлайн		
		0	0	0
9-15	**Второй раздел**	7	0	7
9 - 10	**Безопасность сети в системе Linux** Тюнинг параметров ядра для защиты от сетевых атак: предотвращение IP Spoofing, защита от SYN-флуда (Syncookies), отключение ICMP-редиректов.	Всего аудиторных часов		
		2	0	2
		Онлайн		
		0	0	0
11	**Сетевой фильтр ядра (nftables)** Переход от iptables к nftables: создание stateful-правил, защита от сканирования портов, использование «наборов» (sets) для черных списков.	Всего аудиторных часов		
		1	0	1
		Онлайн		
		0	0	0
12 - 15	**Система резервного копирования** Установка Кибербэкап Начальная настройка Резервное копирование Восстановление	Всего аудиторных часов		
		4	0	4
		Онлайн		
		0	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**
	6 Семестр
1 - 4	**Л/р 1** Настройка пароля на GRUB, внедрение UEFI Secure Boot с собственными ключами. Контроль параметров загрузки ядра.
5 - 8	**Л/р 2** Создание зашифрованных разделов LUKS (с разблокировкой по TPM/флешке). Настройка дисковых квот
9 - 11	**Л/р 3** Тюнинг параметров ядра для защиты от сетевых атак: предотвращение IP Spoofing, защита от SYN-флуда (Syncookies), отключение ICMP-редиректов.
12 - 15	**Л/р 4** Установка Кибербэкап

6. ОБРАЗОВАТЕЛЬНЫЕ ТЕХНОЛОГИИ

Образовательные технологии 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 занятий, усвоения новых знаний, технологии повторения и контроля материала, самостоятельной работы.

7. 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)**
ОПК-1.1	З-ОПК-1.1	З, Э, КИ-8, КИ-15
	У-ОПК-1.1	З, Э, КИ-8, КИ-15
	В-ОПК-1.1	З, Э, КИ-8, КИ-15
ОПК-1.2	З-ОПК-1.2	З, Э, КИ-8, КИ-15
	У-ОПК-1.2	З, Э, КИ-8, КИ-15
	В-ОПК-1.2	З, Э, КИ-8, КИ-15
ПК-1.3	З-ПК-1.3	З, Э, КИ-8, КИ-15
	У-ПК-1.3	З, Э, КИ-8, КИ-15
	В-ПК-1.3	З, Э, КИ-8, КИ-15
ПК-1.4	З-ПК-1.4	З, Э, КИ-8, КИ-15
	У-ПК-1.4	З, Э, КИ-8, КИ-15

	В-ПК-1.4	З, Э, КИ-8, КИ-15
ПК-2	З-ПК-2	З, Э, КИ-8, КИ-15
	У-ПК-2	З, Э, КИ-8, КИ-15
	В-ПК-2	З, 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:

<table>
<tr><th>Сумма баллов</th><th>Оценка по 4-х балльной шкале</th><th>Отметка о зачете</th><th>Оценка ECTS</th></tr>
<tr><td>90-100</td><td>5 – «отлично»</td><td rowspan="7">«зачтено»</td><td>A</td></tr>
<tr><td>85-89</td><td rowspan="3">4 – «хорошо»</td><td>B</td></tr>
<tr><td>75-84</td><td>C</td></tr>
<tr><td>70-74</td><td rowspan="2">D</td></tr>
<tr><td>65-69</td><td rowspan="2">3 – «удовлетворительно»</td></tr>
<tr><td>60-64</td><td>E</td></tr>
<tr><td>ниже 60</td><td>2 – «неудовлетворительно»</td><td>«не зачтено»</td><td>F</td></tr>
</table>

Оценка «отлично» соответствует глубокому и прочному освоению материала программы обучающимся, который последовательно, четко и логически стройно излагает свои ответы, умеет тесно увязывать теорию с практикой, использует в ответах материалы монографической литературы.

Оценка «хорошо» соответствует твердым знаниям материала обучающимся, который грамотно и, по существу, излагает свои ответы, не допуская существенных неточностей.

Оценка «удовлетворительно» соответствует базовому уровню освоения материала обучающимся, при котором освоен основной материал, но не усвоены его детали, в ответах присутствуют неточности, недостаточно правильные формулировки, нарушения логической последовательности.

Отметка «зачтено» соответствует, как минимум, базовому уровню освоения материала программы, при котором обучающийся владеет необходимыми знаниями, умениями и навыками, умеет применять теоретические положения для решения типовых практических задач.

Оценку «неудовлетворительно» / отметку «не зачтено» получает обучающийся, который не знает значительной части материала программы, допускает в ответах существенные ошибки, не выполнил все обязательные задания, предусмотренные программой. Как правило, такие обучающиеся не могут продолжить обучение без дополнительных занятий.

8. 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/

9. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ УЧЕБНОЙ ДИСЦИПЛИНЫ

Специальное материально-техническое обеспечение не требуется

10. 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.

11. УЧЕБНО-МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ ДЛЯ ПРЕПОДАВАТЕЛЕЙ

Учебный курс строится на интегративной основе и включает в себя как теоретические знания, так и практические 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):

Карапетьянц Николай