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 № 4/1/2023

от 25.04.2023 г.

РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ

УПРАВЛЕНИЕ ИНЦИДЕНТАМИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

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/ В**	**СРС, час.**	**КСР, час.**	**Форма(ы) контроля, экз./зач./КР/КП**
7	3	108	32	0	32		44	0	З
Итого	3	108	32	0	32	16	44	0	

АННОТАЦИЯ

К основным целям освоения дисциплины следует отнести:
 приобретение студентами знаний о процессах, процедурах, методах управления инцидентами информационной безопасности систем и умений по идентификации инцидентов информационной безопасности, формированию правил и процедур реагирования на инциденты информационной безопасности информационных систем.
К основным задачам освоения дисциплины следует отнести:
 знание регламента устранения и учёта выявленных инцидентов и регламента информирования персонала о выявленных инцидентах
 умение оценивать последствия выявленных инцидентов; определять источники и причины возникновения инцидентов;
 владение навыками обнаружения, идентификации, устранения инцидентов в процессе эксплуатации системы; навыками определения правил и процедур выявления инцидентов, реагирования на инциденты в процессе эксплуатации системы; навыками резервирования программного обеспечения, технических средств, каналов передачи данных системы

1. ЦЕЛИ И ЗАДАЧИ ОСВОЕНИЯ УЧЕБНОЙ ДИСЦИПЛИНЫ

К основным целям освоения дисциплины следует отнести:
 приобретение студентами знаний о процессах, процедурах, методах управления инцидентами информационной безопасности систем и умений по идентификации инцидентов информационной безопасности, формированию правил и процедур реагирования на инциденты информационной безопасности информационных систем.
К основным задачам освоения дисциплины следует отнести:
 знание регламента устранения и учёта выявленных инцидентов и регламента информирования персонала о выявленных инцидентах
 умение оценивать последствия выявленных инцидентов; определять источники и причины возникновения инцидентов;
 владение навыками обнаружения, идентификации, устранения инцидентов в процессе эксплуатации системы; навыками определения правил и процедур выявления инцидентов, реагирования на инциденты в процессе эксплуатации системы; навыками резервирования программного обеспечения, технических средств, каналов передачи данных системы

2. МЕСТО УЧЕБНОЙ ДИСЦИПЛИНЫ В СТРУКТУРЕ ООП ВО

Дисциплина является профессиональной, ее изучение необходимо для формирования практических навыков выпускников в области информационной 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**
проектно-технологический			
проектирование и разработка защищенных программно-аппаратных комплексов и распределённых информационных систем	программно-аппаратные комплексы и распределённые информационные системы	ПК-4.2 [1] - способен проектировать и разрабатывать защищенные программно-аппаратные комплексы и распределенные информационные системы *Основание:* Профессиональный стандарт: 06.032	З-ПК-4.2[1] - знать принципы проектирования и разработки защищенных программно-аппаратных комплексов и распределенных информационных систем; У-ПК-4.2[1] - уметь проектировать и разрабатывать защищенные программно-аппаратные комплексы и распределенные информационные системы; В-ПК-4.2[1] - владеть навыками проектирования и разработки защищенных программно-аппаратных комплексов и распределенных информационных систем
эксплуатационный			
эксплуатация технических и программно-	программно-аппаратные средства защиты	ПК-4.3 [1] - способен проводить экспериментальное	З-ПК-4.3[1] - знать способы проведения экспериментального

аппаратных средств защиты информации	информации	исследование компьютерных систем с целью выявления уязвимостей *Основание:* Профессиональный стандарт: 06.032	исследования компьютерных систем с целью выявления уязвимостей; У-ПК-4.3[1] - уметь проводить экспериментальное исследование компьютерных систем с целью выявления уязвимостей; В-ПК-4.3[1] - владеть принципами проведения экспериментального исследования компьютерных систем с целью выявления уязвимостей

4. ВОСПИТАТЕЛЬНЫЙ ПОТЕНЦИАЛ ДИСЦИПЛИНЫ

Направления/цели воспитания	Задачи воспитания (код)	Воспитательный потенциал дисциплин
Профессиональное воспитание	Создание условий, обеспечивающих, формирование ответственности за профессиональный выбор, профессиональное развитие и профессиональные решения (В18)	Использование воспитательного потенциала дисциплин профессионального модуля для формирования у студентов ответственности за свое профессиональное развитие посредством выбора студентами индивидуальных образовательных траекторий, организации системы общения между всеми участниками образовательного процесса, в том числе с использованием новых информационных технологий.
Профессиональное воспитание	Создание условий, обеспечивающих, формирование научного мировоззрения, культуры поиска нестандартных научно-технических/практических решений, критического отношения к исследованиям лженаучного толка (В19)	1.Использование воспитательного потенциала дисциплин/практик «Научно-исследовательская работа», «Проектная практика», «Научный семинар» для: - формирования понимания основных принципов и способов научного познания мира, развития исследовательских качеств студентов посредством их вовлечения в исследовательские проекты по областям научных исследований. 2.Использование воспитательного потенциала

		дисциплин "История науки и инженерии", "Критическое мышление и основы научной коммуникации", "Введение в специальность", "Научно-исследовательская работа", "Научный семинар" для: - формирования способности отделять настоящие научные исследования от лженаучных посредством проведения со студентами занятий и регулярных бесед; - формирования критического мышления, умения рассматривать различные исследования с экспертной позиции посредством обсуждения со студентами современных исследований, исторических предпосылок появления тех или иных открытий и теорий.
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)	1. Использование воспитательного потенциала дисциплин "Информатика (Основы программирования)", Программирование (Объектно-ориентированное программирование)", "Программирование (Алгоритмы и структуры данных)" для формирования культуры написания и оформления программ, а также привития навыков командной работы за счет использования систем управления проектами и контроля версий. 2.Использование воспитательного потенциала дисциплины "Проектная практика" для формирования культуры решения изобретательских задач, развития логического мышления, путем погружения студентов в научную и инновационную деятельность института и вовлечения в проектную работу. 3.Использование воспитательного потенциала профильных дисциплин для формирования навыков цифровой гигиены, а также системности и гибкости

		мышления, посредством изучения методологических и технологических основ обеспечения информационной безопасности и кибербезопасности при выполнении и защите результатов учебных заданий и лабораторных работ по криптографическим методам защиты информации в компьютерных системах и сетях. 4.Использование воспитательного потенциала дисциплин " "Информатика (Основы программирования)", Программирование (Объектно-ориентированное программирование)", "Программирование (Алгоритмы и структуры данных)" для формирования культуры безопасного программирования посредством тематического акцентирования в содержании дисциплин и учебных заданий. 5.Использование воспитательного потенциала дисциплины "Проектная практика" для формирования системного подхода по обеспечению информационной безопасности и кибербезопасности в различных сферах деятельности посредством исследования и перенятия опыта постановки и решения научно-практических задач организациями-партнерами.

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
	7 Семестр						
1	Первый раздел	1-8	16/0/16		25	КИ-8	З-ПК-4.2, У-ПК-4.2, В-ПК-4.2, З-ПК-4.3, У-ПК-4.3, В-ПК-4.3
2	Второй раздел	9-16	16/0/16		25	КИ-16	З-ПК-4.2, У-ПК-4.2, В-ПК-4.2, З-ПК-4.3, У-ПК-4.3, В-ПК-4.3
	Итого за 7 Семестр		32/0/32		50		
	Контрольные мероприятия за 7 Семестр				50	З	З-ПК-4.2, У-ПК-4.2, В-ПК-4.2, З-ПК-4.3,

							У-ПК-4.3, В-ПК-4.3

* – 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.**
	7 Семестр	32	0	32
1-8	**Первый раздел**	16	0	16
1 - 2	**Общие положения** Термины и определения: событие информационной безопасности (ИБ); инцидент ИБ; менеджмент инцидентов ИБ; группа реагирования на инциденты ИБ. Виды инцидентов ИБ защищенных информационных систем: неавторизованный доступ; отказ в обслуживании; вредоносный код; несоответствующее использование; сбор информации. Причины возникновения инцидентов ИБ защищенных информационных систем: остаточные риски, изменения внутренней и внешней среды (появление новых угроз), появление новых уязвимостей. Последствия инцидентов ИБ. Цели менеджмента инцидентов ИБ. Система менеджмента инцидентов ИБ защищенных информационных систем. Процессы менеджмента инцидентов ИБ защищенных информационных систем	Всего аудиторных часов 2 Онлайн 0	0 0	2 0
3 - 5	**Планирование системы менеджмента инцидентов ИБ защищенных ИС** Политика менеджмента инцидентов ИБ. Содержание политики менеджмента инцидентов ИБ. Документационное обеспечение системы менеджмента инцидентов ИБ. Процедуры менеджмента инцидентов ИБ защищенных	Всего аудиторных часов 7 Онлайн 0	0 0	7 0

	информационных систем. Группа реагирования на инциденты ИБ (ГРИИБ). Назначение. Члены группы реагирования и её структура. Взаимодействие с другими подразделениями организации. Отношения со сторонними лицами и организациями. Техническая поддержка обработки инцидентов ИБ и восстановления после них. Обеспечение осведомленности сотрудников об обнаружении и оповещении об инцидентах ИБ защищенных информационных систем. Обучение персонала ГРИИБ менеджменту инцидентов ИБ защищенных информационных систем. Контрольный перечень действий по обработке инцидентов ИБ защищенных информационных систем. Приоритетный порядок обработки инцидентов ИБ на основе классификации инцидентов защищенных информационных систем			
6 - 8	**Использование системы менеджмента инцидентов ИБ защищенных ИС** Обнаружение и оповещение об инциденте ИБ защищенных информационных систем. Средства обнаружения инцидентов ИБ. Предвестники и указатели инцидентов ИБ защищенных информационных систем. Анализ инцидентов ИБ защищенных информационных систем. Порядок анализа событий ИБ и инцидентов ИБ. Первичная оценка. Отчётность о событии ИБ. Вторичная оценка. Отчётность об инциденте ИБ. Сдерживание инцидента ИБ защищенных информационных систем. Принятие решения о сдерживании. Стратегии сдерживания инцидента ИБ. Устранение инцидента ИБ защищенных информационных систем и восстановление после него. Действия по устранению инцидента и восстановлению после него. Резервное копирование данных. Резервный фонд оборудования. Сбор и обработка данных об инцидентах ИБ защищенных информационных систем. Цель сбора данных. Статистические данные об инцидентах ИБ. Итоговая отчётность об инцидентах ИБ. Срок хранения данных об инцидентах ИБ.	Всего аудиторных часов 7 Онлайн 0	0 0	7 0
9-16	**Второй раздел**	16	0	16
9 - 12	**Анализ и улучшение системы менеджмента инцидентов ИБ защищенных ИС** Изучение полученного опыта. Определение и осуществление улучшений оценки	Всего аудиторных часов 8 Онлайн 0	0 0	8 0

	риска и управления информационной безопасностью. Определение и осуществление улучшений системы менеджмента инцидентов ИБ защищенных информационных систем.			
13 - 16	**Менеджмент конкретных видов инцидентов ИБ защищенных ИС** Определение инцидента неавторизованного доступом. Примеры инцидентов неавторизованного доступа. Менеджмент инцидентов неавторизованного доступа. Определение инцидента отказа в обслуживании. Примеры инцидентов отказа в обслуживании: рефлекторные атаки, усилительные атаки, атаки распределенного отказа в обслуживании. Менеджмент инцидентов отказа в обслуживании. Определение инцидента, связанного с применением вредоносного кода. Примеры инцидентов, связанных с применением вредоносного кода. Менеджмент инцидентов, связанных с применением вредоносного кода. Определение инцидента, связанного с несоответствующим использованием. Примеры инцидентов, связанных с несоответствующим использованием. Менеджмент инцидентов, связанных с несоответствующим использованием. Определение инцидента сбора информации. Примеры инцидентов сбора информации. Менеджмент инцидентов сбора информации.	Всего аудиторных часов		
		8	0	8
		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**
	7 Семестр
	Л/Р 1 Порядок анализа событий ИБ и инцидентов ИБ
	Л/Р 2

	Устранение инцидента ИБ защищенных информационных систем и восстановление после него
	Л/Р 3 Определение инцидента отказа в обслуживании
	Л/Р 4 Определение инцидента, связанного с применением вредоносного кода

6. ОБРАЗОВАТЕЛЬНЫЕ ТЕХНОЛОГИИ

Образовательные технологии сочетают в себе совокупность методов и средств для реализации определенного содержания обучения и воспитания в рамках дисциплины, влючают решение дидактических и воспитательных задач, формируя основные понятия дисциплины, технологии проведения занятиий, 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)**
ПК-4.2	З-ПК-4.2	З, КИ-8, КИ-16
	У-ПК-4.2	З, КИ-8, КИ-16
	В-ПК-4.2	З, КИ-8, КИ-16
ПК-4.3	З-ПК-4.3	З, КИ-8, КИ-16
	У-ПК-4.3	З, КИ-8, КИ-16
	В-ПК-4.3	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 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, 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.

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):

Белозубова Анна Игоревна