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

РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ

ИНФОРМАЦИОННО-АНАЛИТИЧЕСКИЕ СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ

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	24	16	16		16	0	З
Итого	2	72	24	16	16	0	16	0	

АННОТАЦИЯ

Цель дисциплины – получить навыки комплексного выстраивания системы защиты информации.

В курсе рассматриваются следующие темы:

- информационно-аналитическая деятельность в системе безопасности;
- конкурентная разведка;
- информационные технологии в системе информационно-аналитического обеспечения безопасности.

В рамках практикума студенты получают навыки активного и пассивного методов сбора информации.

1. ЦЕЛИ И ЗАДАЧИ ОСВОЕНИЯ УЧЕБНОЙ ДИСЦИПЛИНЫ

Цель дисциплины – получить навыки комплексного выстраивания системы защиты информации.

В курсе рассматриваются следующие темы:

- информационно-аналитическая деятельность в системе безопасности;
- конкурентная разведка;
- информационные технологии в системе информационно-аналитического обеспечения безопасности.

В рамках практикума студенты получают навыки активного и пассивного методов сбора информации.

2. МЕСТО УЧЕБНОЙ ДИСЦИПЛИНЫ В СТРУКТУРЕ ООП ВО

дисциплина профессионального цикла

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			
разработка проектных решений по обеспечению информационной безопасности	информационные ресурсы	ПК-1 [1] - Способен принимать участие в разработке систем обеспечения ИБ или информационно-аналитических систем безопасности *Основание:* Профессиональный стандарт: 06.032	З-ПК-1[1] - Знать: модели угроз нсд к сетям электросвязи; методики оценки уязвимостей сетей электросвязи с точки зрения возможности нсд к ним; нормативные правовые акты в области связи, информатизации и защиты информации; виды политик безопасности компьютерных систем и сетей; возможности используемых и планируемых к использованию средств защиты информации; особенности защиты информации в автоматизированных системах управления технологическими процессами; критерии оценки эффективности и надежности средств защиты информации программного обеспечения автоматизированных систем; основные характеристики технических средств защиты информации от утечек по техническим каналам; нормативные правовые акты, методические документы, национальные стандарты в области защиты информации ограниченного доступа и аттестации объектов информатизации на соответствие требованиям по защите информации; технические каналы

			утечки информации. ; У-ПК-1[1] - Уметь: выявлять и оценивать угрозы нсд к сетям электросвязи; анализировать компьютерную систему с целью определения необходимого уровня защищенности и доверия; классифицировать защищаемую информацию по видам тайны и степеням конфиденциальности; выбирать меры защиты информации, подлежащие реализации в системе защиты информации автоматизированной системы; проводить анализ угроз безопасности информации на объекте информатизации; проводить предпроектное обследование объекта информатизации. ; В-ПК-1[1] - Владеть: основами проведения технических работ при аттестации сссэ с учетом требований по защите информации; определением угроз безопасности информации, реализация которых может привести к нарушению безопасности информации в компьютерной системе и сети; основами разработки модели угроз безопасности информации и модели нарушителя в автоматизированных

			системах; основами предпроектного обследования объекта информатизации; основами разработки аналитического обоснования необходимости создания системы защиты информации на объекте информатизации (модели угроз безопасности информации).
организационно-управленческий			
организовать эффективную работу по защите информационных ресурсов организации	информационные ресурсы	ПК-8.2 [1] - Способен осуществить разработку, внедрение, обеспечение функционирования системы управления информационной безопасностью организации *Основание:* Профессиональный стандарт: 06.032	З-ПК-8.2[1] - Знать: методологию разработки, внедрения и обеспечения функционирования системы управления информационной безопасностью; У-ПК-8.2[1] - Уметь: выбирать меры обеспечения системы управления информационной безопасностью, реализующие процесс разработки, внедрения и обеспечения функционирования; В-ПК-8.2[1] - Владеть: практическими навыками участия в проектировании системы управления информационной безопасностью конкретного объекта

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	Первый раздел	1-8	12/8/8		25	КИ-8	З-ПК-1, У-ПК-1, В-ПК-1, З-ПК-8.2, У-ПК-8.2, В-ПК-8.2
2	Второй раздел	9-16	12/8/8		25	КИ-16	З-ПК-1, У-ПК-1, В-ПК-1, З-ПК-8.2, У-ПК-8.2, В-ПК-8.2
	Итого за 3 Семестр		24/16/16		50		
	Контрольные мероприятия за 3 Семестр				50	З	З-ПК-1, У-ПК-1, В-ПК-1, З-ПК-8.2, У-ПК-8.2, В-ПК-8.2

* – 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.**
	3 Семестр	24	16	16
1-8	**Первый раздел**	12	8	8
	Информационно-аналитическая деятельность в системе безопасности Роль и функции информационно-аналитической деятельности в обеспечении безопасности. Методы сбора, обработки и анализа информации для выявления угроз и атак. Применение аналитических инструментов для прогнозирования и предотвращения инцидентов. Использование больших данных и машинного обучения в информационно-аналитической деятельности.	Всего аудиторных часов 4 Онлайн 0	2 0	2 0
	Конкурентная разведка. Противодействие промышленному шпионажу. Понятие и виды конкурентной разведки: анализ основных типов шпионажа и их мотиваций. Методы и средства сбора информации: изучение технологий и приемов, используемых в конкурентной разведке. Признаки утечки информации и определение уязвимых мест в организации. Развитие стратегий и мер по противодействию промышленному шпионажу и конкурентной разведке. Технические и организационные меры для защиты информации от несанкционированного доступа.	Всего аудиторных часов 4 Онлайн 0	3 0	3 0
	Информационные технологии в системе информационно-аналитического обеспечения безопасности. Роль и значение информационных технологий в анализе угроз и обеспечении безопасности. Применение больших данных (Big Data) для обработки и анализа информации о безопасности. Искусственный интеллект и машинное обучение в прогнозировании и обнаружении инцидентов. Развитие кибераналитики и её роль в выявлении и анализе	Всего аудиторных часов 4 Онлайн 0	3 0	3 0

	киберугроз. Применение геоинформационных систем и визуализации данных для анализа безопасности.			
9-16	**Второй раздел**	12	8	8
	Требования к информационно-аналитической системе службы безопасности. Основные функции и задачи информационно-аналитической системы в службе безопасности. Требования к сбору, хранению и обработке данных в информационно-аналитической системе. Защита информации и обеспечение конфиденциальности в рамках системы безопасности. Интеграция информационно-аналитической системы с другими системами и источниками данных. Автоматизация процессов анализа и принятия решений в рамках информационно-аналитической системы.	Всего аудиторных часов		
		6	4	4
		Онлайн		
		0	0	0
	Противодействие промышленному шпионажу. Основные методы и техники промышленного шпионажа и их характеристики. Системный подход к противодействию промышленному шпионажу: меры на уровне организации, технологий и персонала. Технические меры защиты: обнаружение и предотвращение утечек информации, контроль доступа и мониторинг активности. Роль обучения и повышения осведомленности сотрудников в противодействии промышленному шпионажу. Сотрудничество с правоохранительными органами и специализированными агентствами для предотвращения и расследования случаев промышленного шпионажа.	Всего аудиторных часов		
		6	4	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**
	3 Семестр

	Л/Р 1 Основные функции и задачи информационно-аналитической системы в службе безопасности
	Л/Р 2 Интеграция информационно-аналитической системы с другими системами и источниками данных
	Л/Р 3 Системный подход к противодействию промышленному шпионажу: меры на уровне организации, технологий и персонала

5. ОБРАЗОВАТЕЛЬНЫЕ ТЕХНОЛОГИИ

Образовательные технологии (лекции, практические работы с компьютерными программами, лабораторная работа) 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.

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-1	З-ПК-1	З, КИ-8, КИ-16
	У-ПК-1	З, КИ-8, КИ-16
	В-ПК-1	З, КИ-8, КИ-16
ПК-8.2	З-ПК-8.2	З, КИ-8, КИ-16
	У-ПК-8.2	З, КИ-8, КИ-16
	В-ПК-8.2	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:

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

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):

Епишкина Анна Васильевна, к.т.н.