

**Федеральное государственное автономное образовательное
учреждение высшего образования
«Московский физико-технический институт
(национальный исследовательский университет)»**

УТВЕРЖДЕНО

**Директор физтех-школы
радиотехники и компьютерных
технологий**

Д.А. Гаврилов

	Рабочая программа дисциплины (модуля)
по дисциплине:	Интеллектуальные технологии в информационной безопасности
по направлению:	Прикладные математика и физика
профиль подготовки:	Радиотехника и компьютерные технологии Физтех-школа Радиотехники и Компьютерных Технологий кафедра интеллектуальных информационных систем и технологий
курс:	4
квалификация:	бакалавр

Семестры, формы промежуточной аттестации:

7 (осенний) - Дифференцированный зачет

8 (весенний) - Дифференцированный зачет

Аудиторных часов: 60 всего, в том числе:

лекции: 30 час.

семинары: 30 час.

лабораторные занятия: 0 час.

Самостоятельная работа: 30 час.

Всего часов: 90, всего зач. ед.: 2

Программу составил: А.Н. Назаров, д-р техн. наук, профессор, профессор

Программа обсуждена на заседании кафедры интеллектуальных информационных систем и технологий
30.03.2023

Аннотация

- введение в методологию интеллектуальных систем в информационной безопасности;
- освоение современных подходов и методов для анализа и синтеза систем информационной безопасности на основе интеллектуальных технологий;
- освоение технологических механизмов идентификации кибер-атак на основе интеллектуальных технологий в инфокоммуникационных системах различного назначения (компьютерные сети, дата-центры, социальные сети и др.);
- приобретение навыков анализа создания множеств признаков, инцидентов кибер-атак на основе новейших достижений искусственного интеллекта
- формирование практических навыков применения изученных методов и схем рассуждений при принятии решений по разработке архитектур и базовых алгоритмов создания систем противодействия бот-атакам на основе интеллектуальных технологий в условиях множественного выбора.

1. Цели и задачи

Цель дисциплины

- 1.Привить студентам навыки разработки методов генерации гипотез о риск-моделях веб-атак в высокодинамичных веб-системах.
- 2.Приобретение навыков анализа применимости нейро-нечеткого и байесовского подходов (объединение априорных и наблюдаемых данных) к синтезу интеллектуальных систем принятия решений по инцидентам информационной безопасности и разработке механизмов веб-программирования в Hadoop.

Задачи дисциплины

Формирование у студентов практических навыков применения изученных методов и схем и аргументации при принятии решений по противодействию веб-атакам в условиях множественного выбора.

2. Перечень формируемых компетенций

Освоение дисциплины направлено на формирование следующих компетенций:

Код и наименование компетенции	Индикаторы достижения компетенции
УК-1 Способен осуществлять поиск, критический анализ и синтез информации, применять системный подход для решения поставленных задач	УК-1.1 Анализирует задачу, выделяя этапы ее решения, действия по решению задачи
	УК-1.2 Находит, критически анализирует и выбирает информацию, необходимую для решения поставленной задачи
	УК-1.3 Рассматривает различные варианты решения задачи, оценивает их преимущества и недостатки
	УК-1.4 Грамотно, логично, аргументированно формирует собственные суждения и оценки
	УК-1.5 Определяет и оценивает практические последствия возможных вариантов решения задачи
ОПК-1 Способен применять фундаментальные знания, полученные в области физико-математических и (или) естественных наук, и использовать их в профессиональной деятельности	ОПК-1.1 Способен анализировать поставленную задачу, намечать пути ее решения
	ОПК-1.2 Способен строить математические модели, производить количественные расчеты и оценки
	ОПК-1.3 Способен определять границы применимости полученных результатов
ОПК-4 Способен осуществлять сбор и обработку научно-технической и (или) технологической информации для решения фундаментальных и прикладных задач	ОПК-4.1 Владеет методами научного поиска и интеллектуального анализа информации при решении задач профессиональной деятельности
	ОПК-4.4 Владеет навыками работы с компьютером и компьютерными сетями с целью получения, хранения и обработки научной (технической, технологической) информации

ПК-4 Способен критически оценивать применимость используемых методик и методов	ПК-4.1 Знает численные порядки величин, характерных для соответствующей профессиональной области
	ПК-4.3 Способен обосновать причинно-следственные отношения используемых понятий и моделей

3. Перечень планируемых результатов обучения по дисциплине (модулю)

В результате освоения дисциплины обучающиеся должны

знать:

Овладение студентами навыков создания подходов, методов и моделей анализа динамики процессов информационного противоборства различного характера

уметь:

Студенты приобретут практические навыки применения риск-моделей и методов, учитывающих многомерность данных для идентификации параметров веб-атак, а также извлечения знаний в информационном противоборстве

владеть:

Приобретение умения интерпретировать полученные результаты для построения сценариев, прогнозов, принятия решений с целью противодействия веб-инъекционным атакам и объяснения характера возникающих в информационно-коммуникационных системах инцидентов информационной безопасности.

4. Содержание дисциплины (модуля), структурированное по темам (разделам) с указанием отведенного на них количества академических часов и видов учебных занятий

4.1. Разделы дисциплины (модуля) и трудоемкости по видам учебных занятий

№	Тема (раздел) дисциплины	Трудоемкость по видам учебных занятий, включая самостоятельную работу, час.			
		Лекции	Семинары	Лаборат. работы	Самост. работа
1	Методология системного анализа риска нападения в информационно-коммуникационных технологиях. Концепция риска кибер-атаки	3	3		3
2	Примеры информационной войны. Формальная постановка исследовательской задачи	3	3		3
3	Сравнительный анализ региональных особенностей рисков атак в мире (на примере развитых и развивающихся регионов мира)	3	3		3
4	Критерии защищённости объекта кибер-атаки	3	3		3
5	Оценка рисков	3	3		3
6	Методы анализа рисков и математические методы, используемые в интеллектуальных системах информационной безопасности	5	5		5
7	Моделирование веб-атак	5	5		5
8	Предварительный анализ текущего состояния: параметры цели	5	5		5
Итого часов		30	30		30
Подготовка к экзамену		0 час.			

Общая трудоёмкость	90 час., 2 зач.ед.
--------------------	--------------------

4.2. Содержание дисциплины (модуля), структурированное по темам (разделам)

Семестр: 7 (Осенний)

1. Методология системного анализа риска нападения в информационно-коммуникационных технологиях. Концепция риска кибер-атаки.

Исторические сведения о становлении научной дисциплины – системный анализ рисков инфокоммуникаций. Основные понятия информационной войны в Интернете.

Примеры программирования информационной войны в среде Matlab.

2. Примеры информационной войны. Формальная постановка исследовательской задачи.

Характеристика особенностей сложных систем: уникальность, слабая структурированность теоретических и фактических знаний о системах, композиционный характер

(мультипротокольность), неоднородность подсистем и элементов, случайность и неопределенность факторов, действующих в системах, многокритериальность процессов оценки (игры с конфликтующими интересами), большая размерность, непрерывность переменных и немонотонность в динамике, субъективность в описании сложных систем. Интегральные характеристики. Общие свойства.

Примеры программирования информационных мультипротокольных систем в среде Matlab.

3. Обзор: глобализм и пример блоков Азии и Африки.

Пределы применимости вероятностных подходов оценки риска атак. Полнота, инвариантность случайной диаграммы риска атаки. Примеры программирования значения риска объекта риска в Matlab.

4. Критерии защищённости объекта кибер-атаки.

Условие защищенности объекта риска. Оценка защищенности объекта риска. Примеры программирования алгоритма оценки защищенности объекта риска в Матлаб.

5. Оценка Рисков.

Уточнённое условие защищённости объекта риска. Новые градации функций защиты. Примеры программирования новых градаций функций защиты объекта риска в Матлаб.

Семестр: 8 (Весенний)

6. Методы анализа рисков и математические методы, используемые в интеллектуальных системах информационной безопасности.

Оценка экстремальных рисков. Метрики для оценки рисков. Максимизация, экстремальные задачи, мультиэкстремальные задачи.

7. Моделирование веб-атак.

Класс моделей. Процесс идентификации в системно-ориентированном моделировании в облаке. Примеры программирования бот-атак в Matlab, Hadoop.

8. Предварительный анализ текущего состояния: параметры цели.

Моделирование этапов, постановка целей, построение информационной структурно-функциональной среды, построение логической среды СУБД. верификация. Примеры программирования логических сред СУБД, в среде MATLAB, Hadoop.

5. Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине (модулю)

Учебная аудитория, оснащенная мультимедиа проектором и экраном, рабочими компьютерами с установленным пакетом Matlab версии 2019 и выше, маркерной доской с маркерами.

6.Перечень рекомендуемой литературы

Основная литература

1. An introduction to Computer Security: The NIST Handbook. National Institute of Standards and Technology. 2006.
2. Georgiou D., Lambrinoudakis C. (2014) “A Security Policy for Cloud Providers The Software-as-a-Service Model ”, Conference Paper, Proc. ICMP 2014: The Ninth International Conference on Internet Monitoring and Protection, July 20 - 24, 2014 - Paris, France, pp. 12-21, DOI: 10.13140/2.1.2891.6489.

Дополнительная литература

1. NICE Framework Revision webpage, National Institute of Standards and Technology, <https://www.nist.gov/itl/applied-cybersecurity/nice/nice-cybersecurity-workforce-framework-resource-center/nice-0>
2. National Initiative for Cybersecurity Education.National Sybersecurity Workforce Framework, ver. 1.0., <https://www.nist.gov/file/359276>

7. Перечень ресурсов информационно-телекоммуникационной сети "Интернет", необходимых для освоения дисциплины (модуля)

- <http://www.elibrary.ru> - Elibrary \ библиотека Elibrary
- <https://ieeexplore.ieee.org> – IEEE library \ библиотека IEEE
- <http://www.deeplearningbook.org/> - online book \ онлайн книга
- <http://matlab.exponenta.ru> – Matlab, Simulink materials and forum \ материалы и форум по Matlab\Simulink
- CITaS Library – access from inside network \ Библиотека ЦИТиС (доступ из внутренней сети)

8. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине (модулю), включая перечень необходимого программного обеспечения и информационных справочных систем (при необходимости)

Система Matlab версии 2019 и выше с пакетами: Deeplearning Toolbox, Image Processing Toolbox, Machine Learning Toolbox, Optimization Toolbox.

9. Методические указания для обучающихся по освоению дисциплины (модуля)

Самостоятельная работа включает в себя:

- чтение и конспектирование рекомендованной литературы,
- проработку учебного материала (по учебной и научной литературе), подготовку ответов на вопросы, предназначенных для самостоятельного изучения
- решение задач, предлагаемых студентам на практических занятиях и в качестве курсового задания,
- подготовку к экзамену.

Руководство и контроль за самостоятельной работой студента осуществляется в форме индивидуальных консультаций.

Важно добиться понимания изучаемого материала, а не механического его запоминания. При затруднении изучения отдельных тем, вопросов, следует обращаться за консультациями к лектору или преподавателю, ведущему занятия.

ОЦЕНОЧНЫЕ МАТЕРИАЛЫ ПО ДИСЦИПЛИНЕ (МОДУЛЮ)

по направлению:	Прикладные математика и физика
профиль подготовки:	Радиотехника и компьютерные технологии Физтех-школа Радиотехники и Компьютерных Технологий кафедра интеллектуальных информационных систем и технологий
курс:	4
квалификация:	бакалавр

Семестры, формы промежуточной аттестации:

7 (осенний) - Дифференцированный зачет

8 (весенний) - Дифференцированный зачет

Разработчик: А.Н. Назаров, д-р техн. наук, профессор, профессор

1. Компетенции, формируемые в процессе изучения дисциплины

Код и наименование компетенции	Индикаторы достижения компетенции
УК-1 Способен осуществлять поиск, критический анализ и синтез информации, применять системный подход для решения поставленных задач	УК-1.1 Анализирует задачу, выделяя этапы ее решения, действия по решению задачи
	УК-1.2 Находит, критически анализирует и выбирает информацию, необходимую для решения поставленной задачи
	УК-1.3 Рассматривает различные варианты решения задачи, оценивает их преимущества и недостатки
	УК-1.4 Грамотно, логично, аргументированно формирует собственные суждения и оценки
	УК-1.5 Определяет и оценивает практические последствия возможных вариантов решения задачи
ОПК-1 Способен применять фундаментальные знания, полученные в области физико-математических и (или) естественных наук, и использовать их в профессиональной деятельности	ОПК-1.1 Способен анализировать поставленную задачу, намечать пути ее решения
	ОПК-1.2 Способен строить математические модели, производить количественные расчеты и оценки
	ОПК-1.3 Способен определять границы применимости полученных результатов
ОПК-4 Способен осуществлять сбор и обработку научно-технической и (или) технологической информации для решения фундаментальных и прикладных задач	ОПК-4.1 Владеет методами научного поиска и интеллектуального анализа информации при решении задач профессиональной деятельности
	ОПК-4.4 Владеет навыками работы с компьютером и компьютерными сетями с целью получения, хранения и обработки научной (технической, технологической) информации
ПК-4 Способен критически оценивать применимость используемых методик и методов	ПК-4.1 Знает численные порядки величин, характерных для соответствующей профессиональной области
	ПК-4.3 Способен обосновать причинно-следственные отношения используемых понятий и моделей

2. Показатели оценивания компетенций

В результате изучения дисциплины «Интеллектуальные технологии в информационной безопасности» обучающийся должен:

знать:

Овладение студентами навыков создания подходов, методов и моделей анализа динамики процессов информационного противоборства различного характера

уметь:

Студенты приобретут практические навыки применения риск-моделей и методов, учитывающих многомерность данных для идентификации параметров веб-атак, а также извлечения знаний в информационном противоборстве

владеть:

Приобретение умения интерпретировать полученные результаты для построения сценариев, прогнозов, принятия решений с целью противодействия веб-инъекционным атакам и объяснения характера возникающих в информационно-коммуникационных системах инцидентов информационной безопасности.

3. Перечень типовых (примерных) вопросов, заданий, тем для подготовки к текущему контролю

Семестр: 2 (Весенний)

Вопросы:

1. Методология системного анализа рисков инфокоммуникаций.
2. Понятие состояний сложных систем в условиях информационной войны.

3. Примеры информационной войны.

За каждое задание студент получает оценку в соответствии с таблицей критериев оценивания. Эта оценка учитывается при семестровой аттестации.

Семестр: 3 (Осенний)

Вопросы:

1. Методы анализа рисков и математические методы, используемые в интеллектуальных системах информационной безопасности.
2. Оценка экстремальных рисков. Метрики для оценки рисков.
3. Построение информационной структурно-функциональной среды выделенной СУБД.

За каждое задание студент получает оценку в соответствии с таблицей критериев оценивания. Эта оценка учитывается при семестровой аттестации.

4. Перечень типовых (примерных) вопросов и тем для проведения промежуточной аттестации обучающихся

Перечень контрольных вопросов:

1. Полнота, инвариантность случайной диаграммы риска нападения.
2. Онтология в описании структуры и функций системы, ее динамических сценариев на основе набора моделей (в качестве переменных выбираются инвестиции, население и т. д.).
3. Кластерный анализ. Минимаксная, многоцелевая оптимизация. .
4. Математическая теория планирования эксперимента.

Примеры контрольных заданий:

1. Разработать программу, использующую методические рекомендации по планированию эксперимента анализа процесса кибер-атаки.
2. Разработать программу, использующую нейронную сеть для решения задачи кластерного анализа кибер-атаки для заданного объекта риска.
3. Разработать программу, использующую методы многоцелевой оптимизации для решения задачи идентификации глубины проникновения кибер-атаки в структуру объекта риска.

Семестр: 2 (Весенний)

Примеры билетов для проведения дифференциального зачёта:

Билет 1.

1. Модели оценки экстремального риска кибер-атаки.
2. Разработать программу по применению нейронных сетей для анализа сценариев проникновения кибер-атаки в объект риска.

Билет 2.

1. Глубокое обучение. Подходы к применению в отношении кибер-атак..
2. Разработать программу с использованием нейронной сети для решения задачи оценки состояния защищённости заданного объекта риска.

Семестр: 3 (Осенний)

Примеры билетов для проведения экзамена:

Билет 1.

1. Парето-оптимальное решение минимаксной задачи информационного противоборства.
2. Алгоритмы решения задачи обучения интеллектуальной системы обнаружения кибер-атак.

Билет 2.

1. Облачные решения по созданию интеллектуальных систем обнаружения кибер-атак.
2. Алгоритм решения задачи оценки необходимого ресурса IaaS-системы для идентификации начала кибер-атаки.

- оценка «отлично (10)» выставляется студенту, показавшему всесторонние, систематизированные, глубокие знания учебной программы дисциплины и умение уверенно применять их на практике при решении конкретных задач, свободное и правильное обоснование принятых решений
- оценка «отлично (9)» выставляется студенту, показавшему всесторонние, систематизированные, глубокие знания учебной программы дисциплины и умение применять их на практике при решении конкретных задач, свободное и правильное обоснование принятых решений
- оценка «отлично (8)» выставляется студенту, показавшему всесторонние систематизированные, глубокие знания учебной программы дисциплины и умение применять их на практике при решении конкретных задач, и правильное обоснование принятых решений
- оценка «хорошо (7)» выставляется студенту, если он твердо знает материал, грамотно и по существу излагает его, умеет применять полученные знания на практике, но допускает в ответе или в решении задач некоторые неточности;
- оценка «хорошо (6)» выставляется студенту, если он знает материал, грамотно и по существу излагает его, умеет применять полученные знания на практике, но допускает в ответе или в решении задач некоторые неточности;
- оценка «хорошо (5)» выставляется студенту, если он знает материал, и по существу излагает его, умеет применять полученные знания на практике, но допускает в ответе или в решении задач некоторые неточности;
- оценка «удовлетворительно (4)» выставляется студенту, показавшему фрагментарный, разрозненный характер знаний, недостаточно правильные формулировки базовых понятий, нарушения логической последовательности в изложении программного материала, но при этом он владеет основными разделами учебной программы, необходимыми для дальнейшего обучения и может применять полученные знания по образцу в стандартной ситуации;
- оценка «удовлетворительно (3)» выставляется студенту, показавшему фрагментарный, разрозненный характер знаний, недостаточно правильные формулировки базовых понятий, нарушения логической последовательности в изложении программного материала, но при этом он владеет фрагментарно основными разделами учебной программы, необходимыми для дальнейшего обучения и может применять полученные знания по образцу в стандартной ситуации;
- оценка «неудовлетворительно (2)» выставляется студенту, который не знает большей части основного содержания учебной программы дисциплины, допускает грубые ошибки в формулировках основных понятий дисциплины и не умеет использовать полученные знания при решении типовых практических задач
- оценка «неудовлетворительно (1)» выставляется студенту, который не знает формулировок основных понятий дисциплины.

5. Методические материалы, определяющие процедуры оценивания знаний, умений, навыков и (или) опыта деятельности

Зачёт и экзамен проводятся в устной форме с практическим (компьютерным) заданием.

При проведении зачёта и экзамена обучающемуся предоставляется не менее 60 минут на подготовку.

Опрос обучающегося на дифференциальном зачёте и экзамене не должен превышать 60 минут.

Во время проведения зачёта и экзамена обучающиеся могут пользоваться программой дисциплины, компьютером с Matlab и справочной системой.