

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

УТВЕРЖДЕНО

**Директор физтех-школы
прикладной математики и
информатики
А.М. Райгородский**

	Рабочая программа дисциплины (модуля)
по дисциплине:	Информационная безопасность и уязвимости приложений
по направлению:	Информатика и вычислительная техника
профиль подготовки:	
	Физтех-школа Прикладной Математики и Информатики кафедра корпоративных информационных систем
курс:	4
квалификация:	бакалавр

Семестр, формы промежуточной аттестации: 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

Количество контрольных работ, заданий: 1

Программу составил: Е.А. Петухова, старший преподаватель

Программа обсуждена на заседании кафедры корпоративных информационных систем 20.02.2020

Аннотация

Дисциплина “Информационная безопасность и уязвимости приложений” направлена на создание представления о рисках и угрозах, связанных с разработкой и сопровождением веб-приложений в современных условиях. По ходу освоения программы курса студенты познакомятся с методологией аудита информационной безопасности. Помимо теоретических знаний студенты будут получать практические задания, которые помогут разобраться в различных видах уязвимостей и методах их обнаружения.

В дисциплине рассматриваются следующие темы:

- основные риски и угрозы, присущие современным web-приложениям;
- этап сбора и оценки информации относительно цели;
- обзор типичных web-уязвимостей;
- технология Whitebox-аудит;
- представление и обработка данных в web-приложении.

Заключительным этапом всего курса является дифференцированный зачет, целью которого является проверка знаний студентов по теории и выявление практических навыков, полученных при выполнении практических заданий.

1. Цели и задачи

Цель дисциплины

Дать студентам представление о рисках и угрозах, связанных с разработкой и сопровождением веб-приложений в современных условиях; познакомить студентов с методологией аудита ИБ.

Задачи дисциплины

- Освоить построение модели угроз и оценку рисков для web приложений;
- овладеть методикой анализа защищенности приложений;
- изучить инструменты, используемые для анализа безопасности;
- изучить основные типы web-уязвимостей;
- получить представление об особенностях функционирования протоколов, использующихся на прикладном уровне.

2. Перечень формируемых компетенций

Освоение дисциплины направлено на формирование следующих компетенций:

Код и наименование компетенции	Индикаторы достижения компетенции
ОПК-3 Способен составлять и оформлять научные и (или) технические (технологические, инновационные) отчеты (публикации, проекты)	ОПК-3.1 Знает основные правила оформления научных публикаций и научно-технической документации, в том числе с использованием прикладного программного обеспечения
	ОПК-3.2 Владеет на практике методологией составления научно-технических отчетов (проектов)
	ОПК-3.3 Владеет методами визуального и графического представления результатов научной (научно-технической, инновационной технологической) деятельности в виде отчетов, научных публикаций
ПК-2 Способен самостоятельно или в качестве члена (руководителя) малого коллектива организовывать и проводить научные исследования и их апробацию	ПК-2.1 Знает принципы построения научной работы, методы сбора и анализа полученного материала, способы аргументации
	ПК-2.2 Способен планировать и проводить научные исследования самостоятельно или в качестве члена (руководителя) малого научного коллектива
	ПК-2.3 Способен проводить апробацию результатов научно-исследовательской работы посредством публикации научных статей и участия в конференциях

3. Перечень планируемых результатов обучения по дисциплине (модулю)

В результате освоения дисциплины обучающиеся должны

знать:

- Основные риски и угрозы, применимые к современным web-приложениям;
- особенности и ограничения blackbox-тестирования;
- особенности и ограничения whitebox-тестирования;
- методики первоначального сбора информации относительно цели исследования;
- типы представлений данных в приложении;
- методы поиска типичных уязвимостей web-приложений;
- протоколы и стандарты: L6/L7 OSI.

уметь:

- Строить модели угроз и оценку рисков для web приложений;
- проводить аудит безопасности web-приложений;
- оперировать моделью угроз в рамках разрабатываемого приложения;
- применять инструментальные средства для автоматизации процесса аудита приложения;
- идентифицировать и проводить исправление распространенных типов уязвимостей web-приложений.

владеть:

- Методами и средствами описания моделей угроз;
- методами аудит безопасности web-приложений.

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	Основные риски и угрозы, присущие современным web-приложениям.	6	5		6
2	Этап сбора и оценки информации относительно цели.	6	6		6
3	Обзор типичных web-уязвимостей.	6	7		6
4	Технология Whitebox-аудит.	7	6		6
5	Представление и обработка данных в web-приложении.	5	6		6
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: 8 (Весенний)

1. Основные риски и угрозы, присущие современным web-приложениям.

Обзор эволюции сферы ИБ, оценка рисков, текущее состояние области с точки зрения злоумышленника.

2. Этап сбора и оценки информации относительно цели.

Методы начального сбора информации о цели. пассивный сбор информации: поисковые машины, dns, whois, http fingerprint, активный анализ: сетевые сканеры, file enumeration, security-сканеры.

3. Обзор типичных web-уязвимостей.

Цикл blackbox-анализа, разбор типичных уязвимостей сервисов, методики поиска, подтверждения и эксплуатации.

4. Технология Whitebox-аудит.

Методика аудита информационной системы, стандарты безопасности, практика статического анализа, практика написания защищенного кода.

5. Представление и обработка данных в web-приложении.

Обзор используемых протоколов и стандартов: L6/L7 OSI.

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

Учебная аудитория, оснащенная компьютерной техникой с подключением к сети «Интернет» и мультимедийным оборудованием (проектор, звуковая система) для проведения занятий лекционного и семинарского типа.

6.Перечень рекомендуемой литературы

Основная литература

1. Лапони́на О.Р. Основы сетевой безопасности: криптографические алгоритмы и протоколы взаимодействия / О.Р. Лапони́на. - Москва : Национальный Открытый Университет ИНТУИТ, 2016. - 461 с. - ISBN 5-9556-00020-5. - URL: <https://ibooks.ru/bookshelf/363042/reading>. - Текст: электронный.
2. Информационная безопасность и защита информации : учебное пособие / Е. К. Баранова, А. В. Бабаш. - 4-е изд., перераб. и доп. - Москва : РИОР : ИНФРА-М, 2020. - 336 с. - (Высшее образование). - Библиогр.: с. 327-330. - 30 экз. - ISBN 978-5-369-0176-6)

Дополнительная литература

1. Информационная безопасность открытых систем [Электронный ресурс] : учебник / Д. А. Мельников. - 2-е изд., стереотип. - М.: Флинта, 2014. - Электрон. версия печ. публикации. - Режим доступа: <https://e.lanbook.com/reader/book/48368/>

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

Не используются

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

На лекционных занятиях используются мультимедийные технологии, включая демонстрацию презентаций.

Для контроля и коррекции знаний, обучающиеся могут использовать компьютерное тестирование.

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

Методические рекомендации позволяют студенту оптимальным образом организовать процесс обучения. В структуре учебного плана значительное время отводится на самостоятельное изучение данной дисциплины. В рабочей программе приведено примерное распределение часов аудиторной и внеаудиторной нагрузки по различным темам данной дисциплины.

Для успешного освоения данной дисциплины студенту необходимо:

- посещать лекции и семинары, при этом конспектирование материалов не является необходимым, поскольку основные материалы хранятся в кафедральной папке в облачном хранилище данных, к которому предоставлен доступ всем студентам кафедры;
- самостоятельно регистрировать задания, полученные от преподавателей на лекциях и семинарах, а также результаты их выполнения на корпоративном портале кафедры;
- выполнить итоговое письменное задание по дисциплине, которое вносит основной вклад в изучение дисциплины, а также в итоговую оценку.

ОЦЕНОЧНЫЕ МАТЕРИАЛЫ ПО ДИСЦИПЛИНЕ (МОДУЛЮ)

по направлению: Информатика и вычислительная техника

профиль подготовки: Физтех-школа Прикладной Математики и Информатики
кафедра корпоративных информационных систем

курс: 4

квалификация: бакалавр

Семестр, формы промежуточной аттестации: 8 (весенний) - Дифференцированный зачет

Разработчик: Е.А. Петухова, старший преподаватель

1. Компетенции, формируемые в процессе изучения дисциплины

Код и наименование компетенции	Индикаторы достижения компетенции
ОПК-3 Способен составлять и оформлять научные и (или) технические (технологические, инновационные) отчеты (публикации, проекты)	ОПК-3.1 Знает основные правила оформления научных публикаций и научно-технической документации, в том числе с использованием прикладного программного обеспечения
	ОПК-3.2 Владеет на практике методологией составления научно-технических отчетов (проектов)
	ОПК-3.3 Владеет методами визуального и графического представления результатов научной (научно-технической, инновационной технологической) деятельности в виде отчетов, научных публикаций
ПК-2 Способен самостоятельно или в качестве члена (руководителя) малого коллектива организовывать и проводить научные исследования и их апробацию	ПК-2.1 Знает принципы построения научной работы, методы сбора и анализа полученного материала, способы аргументации
	ПК-2.2 Способен планировать и проводить научные исследования самостоятельно или в качестве члена (руководителя) малого научного коллектива
	ПК-2.3 Способен проводить апробацию результатов научно-исследовательской работы посредством публикации научных статей и участия в конференциях

2. Показатели оценивания компетенций

В результате изучения дисциплины «Информационная безопасность и уязвимости приложений» обучающийся должен:

знать:

- Основные риски и угрозы, применимые к современным web-приложениям;
- особенности и ограничения blackbox-тестирования;
- особенности и ограничения whitebox-тестирования;
- методики первоначального сбора информации относительно цели исследования;
- типы представлений данных в приложении;
- методы поиска типичных уязвимостей web-приложений;
- протоколы и стандарты: L6/L7 OSI.

уметь:

- Строить модели угроз и оценку рисков для web приложений;
- проводить аудит безопасности web-приложений;
- оперировать моделью угроз в рамках разрабатываемого приложения;
- применять инструментальные средства для автоматизации процесса аудита приложения;
- идентифицировать и проводить исправление распространенных типов уязвимостей web-приложений.

владеть:

- Методами и средствами описания моделей угроз;
- методами аудит безопасности web-приложений.

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

Перечень вопросов для промежуточного контроля:

1. Обзор сферы информационной безопасности.
2. Методы начального сбора информации о цели.
3. Примеры типичных уязвимостей сервисов.
4. Методика аудита информационной системы.
5. Стандарты безопасности.

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

1. Основные риски и угрозы, присущие современным web-приложениям.
2. Обзор эволюции сферы ИБ, оценка рисков, текущее состояние области с точки зрения злоумышленника.
3. Этап сбора и оценки информации относительно цели.
4. Методы начального сбора информации о цели. пассивный сбор информации: поисковые машины, dns, whois, http fingerprint, активный анализ: сетевые сканеры, file enumeration, security-сканеры.
5. Представление и обработка данных в web-приложении.
6. Обзор используемых протоколов и стандартов: L6/L7 OSI.
7. Обзор типичных web-уязвимостей.
8. Цикл blackbox-анализа, разбор типичных уязвимостей сервисов, методики поиска, подтверждения и эксплуатации.
9. Технология Whitebox-аудита.

Критерии оценивания

отлично (10) - Студент демонстрирует:

- ☐ систематизированные, глубокие и полные знания по всем разделам учебной программы, а также по основным вопросам, выходящим за ее пределы;
- ☐ точное использование научной терминологии, стилистически грамотное, логически правильное изложение ответа на вопросы, умение делать выводы;
- ☐ безупречное владение инструментарием учебной дисциплины, умение его эффективно использовать в постановке и решении научных и профессиональных задач;
- ☐ полное и глубокое усвоение основной и дополнительной литературы, рекомендованной учебной программой дисциплины;
- ☐ высокий уровень самостоятельности и инициативности при выполнении задач в рамках самостоятельных и практических заданий.

отлично (9) - Студент демонстрирует:

- ☐ систематизированные, глубокие и полные знания по всем разделам учебной программы;
- ☐ точное использование научной терминологии, стилистически грамотное, логически правильное изложение ответа на вопросы, умение делать выводы;
- ☐ владение инструментарием учебной дисциплины, умение его эффективно использовать в постановке и решении научных и профессиональных задач;
- ☐ полное и глубокое усвоение основной и дополнительной литературы, рекомендованной учебной программой дисциплины;
- ☐ высокий уровень самостоятельности и инициативности при выполнении задач в рамках самостоятельных и практических заданий.

отлично (8) - Студент демонстрирует:

- ☐ систематизированные, глубокие и полные знания по всем разделам учебной программы;
- ☐ использование научной терминологии, стилистически грамотное, логически правильное изложение ответа на вопросы, умение делать выводы;
- ☐ владение инструментарием учебной дисциплины, умение его эффективно использовать в постановке и решении научных и профессиональных задач;
- ☐ усвоение основной литературы, рекомендованной учебной программой дисциплины;
- ☐ самостоятельность и инициативность при выполнении задач в рамках самостоятельных и практических заданий.

хорошо (7) - Студент демонстрирует:

- ☐ систематизированные, глубокие и полные знания по всем поставленным вопросам в объеме учебной программы;
- ☐ использование научной терминологии, стилистически грамотное, логически правильное изложение ответа на вопросы, умение делать выводы;
- ☐ владение инструментарием учебной дисциплины, умение его использовать в постановке и решении научных и профессиональных задач;
- ☐ усвоение основной литературы, рекомендованной учебной программой дисциплины;

☐ самостоятельность при выполнении задач в рамках самостоятельных и практических заданий.

хорошо (6) - Студент демонстрирует:

☐ достаточно полные и систематизированные знания по большинству поставленных вопросов в объеме учебной программы;

☐ использование научной терминологии, стилистически грамотное, логически правильное изложение ответа на вопросы, умение делать выводы;

☐ владение инструментарием учебной дисциплины, умение его использовать в постановке и решении научных и профессиональных задач;

☐ усвоение основной литературы, рекомендованной учебной программой дисциплины;

☐ самостоятельность при выполнении задач в рамках самостоятельных и практических заданий.

хорошо (5) - Студент демонстрирует:

☐ достаточные знания в объеме учебной программы;

☐ использование научной терминологии, стилистически грамотное, логически правильное изложение ответа на вопросы, умение делать выводы;

☐ владение инструментарием учебной дисциплины, умение его использовать в решении научных и профессиональных задач;

☐ усвоение основной литературы, рекомендованной учебной программой дисциплины;

☐ самостоятельность при выполнении задач в рамках самостоятельных и практических заданий.

удовлетворительно (4) - Студент демонстрирует:

☐ достаточный объем знаний в рамках образовательного стандарта;

☐ в целом корректное использование научной терминологии, стилистически грамотное, логически правильное изложение ответа на вопросы, умение делать выводы без существенных ошибок;

☐ владение инструментарием учебной дисциплины, умение его использовать в решении стандартных научных и профессиональных задач;

☐ усвоение основной литературы, рекомендованной учебной программой дисциплины;

☐ способность работать под руководством преподавателя при выполнении задач в рамках самостоятельных и практических заданий.

удовлетворительно (3) - Студент демонстрирует:

☐ недостаточно полный объем знаний в рамках образовательного стандарта;

☐ частично корректное использование научной терминологии, изложение ответа с существенными стилистическими и логическими ошибками;

☐ слабое владение инструментарием учебной дисциплины, некорректное его использование в решении стандартных научных и профессиональных задач;

☐ знание части основной литературы, рекомендованной учебной программой дисциплины;

☐ пассивность при выполнении задач в рамках самостоятельных и практических заданий.

неудовлетворительно (2) - Студент демонстрирует:

☐ фрагментарные знания в рамках образовательного стандарта;

☐ неумение использовать научную терминологию дисциплины, изложение ответа с существенными стилистическими и логическими ошибками;

☐ фрагментарные знания основной литературы, рекомендованной учебной программой дисциплины;

☐ пассивность при выполнении задач в рамках самостоятельных и практических заданий.

неудовлетворительно (1) - Студент демонстрирует:

☐ отсутствие знаний в рамках образовательного стандарта или отказ от ответа.

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

Во время проведения дифференцированного зачета обучающиеся могут пользоваться программой дисциплины, а также справочной литературой, конспектами лекций или другими материалами.