МИНИСТЕРСТВО ТРАНСПОРТА РОССИЙСКОЙ ФЕДЕРАЦИИ

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ

«РОССИЙСКИЙ УНИВЕРСИТЕТ ТРАНСПОРТА»
(РУТ (МИИТ)

Рабочая программа дисциплины (модуля),
как компонент образовательной программы
базового высшего образования
по специальности
10.05.01 Компьютерная безопасность,
утвержденной первым проректором РУТ (МИИТ)
Тимониным В.С.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)

Системы с конструктивной информационной безопасностью

Специальность: 10.05.01 Компьютерная безопасность

Специализация: Информационная безопасность объектов информатизации на базе компьютерных систем

Форма обучения: Очная

1. Общие сведения о дисциплине (модуле).

Целью дисциплины является получение обучающимися знаний, умений и навыков для решения следующих профессиональных задач:

- определение и описание содержания работ, необходимых для согласования (синхронизации) требований безопасности информации с реализацией основного функционала соответствующих систем на всех этапах их жизненного цикла;

- формирование и использование шаблонов проектирования и разработки систем, обеспечивающих учет опыта блокирования и исправления известных (типовых) и минимизацию числа потенциальных (новых, неизвестных) уязвимостей и ошибок;

- формирование требований на создаваемые системы, реализующие информационную технологию, а также осуществляющие с помощью информационной технологии контроль и управление различными процессами информационными, телекоммуникационными, технологическими, производственными), обеспечивающие реализацию конструктивных подходов к информационной безопасности;

- обеспечение информационной безопасности систем, для которых запланирована глубокая модернизация с полной заменой оборудования, где использование наложенных (внешних и (или) встраиваемых) средств защиты затруднено и (или) невозможно.

2. Планируемые результаты обучения по дисциплине (модулю).

Перечень формируемых результатов освоения образовательной программы (компетенций) в результате обучения по дисциплине (модулю):

ОПК-2 - Способен понимать устройство и историю развития транспортной системы;

УК-1 - Способен осмысленно подходить к решению задач, выявлять проблемы, ставить цели, вырабатывать стратегию действий.

Обучение по дисциплине (модулю) предполагает, что по его результатам обучающийся будет:

Знать:

- современное программное обеспечение для программирования;

- ключевые термины методологии кибериммунитета;

- особенности программно-аппаратного обеспечения кибериммунных систем.

Уметь:

- применять современное программное обеспечение для программирования;
- формулировать цели и предположения безопасности, негативные сценарии, политики безопасности;
- разрабатывать высокоуровневые архитектурные диаграммы;
- использовать учебную инфраструктуры для решения учебных задач на внедрение кибериммунитета.

Владеть:

- навыками получения, обработки и хранения информации;
- навыками работы с прикладными программами различного назначения;
- инструментами разработки кода политик безопасности и автоматизации тестирования безопасности;
- инструментами моделирования систем;
- приемами защиты информации.

3. Объем дисциплины (модуля).

3.1. Общая трудоемкость дисциплины (модуля).

Общая трудоемкость дисциплины (модуля) составляет 4 з.е. (144 академических часа(ов).

3.2. Объем дисциплины (модуля) в форме контактной работы обучающихся с педагогическими работниками и (или) лицами, привлекаемыми к реализации образовательной программы на иных условиях, при проведении учебных занятий:

Тип учебных занятий	Количество часов	
	Всего	Семестр №8
Контактная работа при проведении учебных занятий (всего):	80	80
В том числе:		
Занятия лекционного типа	48	48
Занятия семинарского типа	32	32

3.3. Объем дисциплины (модуля) в форме самостоятельной работы обучающихся, а также в форме контактной работы обучающихся с педагогическими работниками и (или) лицами, привлекаемыми к реализации образовательной программы на иных условиях, при проведении промежуточной аттестации составляет 64 академических часа (ов).

3.4. При обучении по индивидуальному учебному плану, в том числе при ускоренном обучении, объем дисциплины (модуля) может быть реализован полностью в форме самостоятельной работы обучающихся, а также в форме контактной работы обучающихся с педагогическими работниками и (или) лицами, привлекаемыми к реализации образовательной программы на иных условиях, при проведении промежуточной аттестации.

4. Содержание дисциплины (модуля).

4.1. Занятия лекционного типа.

№ п/п	Тематика лекционных занятий / краткое содержание
1	Введение в информатику и информационные технологии Рассматриваемые вопросы: - Информация. - Информатизация. - Информационные технологии. - Средства реализации и способы описания информационных технологий. - Информационный процесс. - Структура информационного процесса.
2	Архитектура современных программных средств Рассматриваемые вопросы: - Характеристики качества программного обеспечения. - Классификация программного обеспечения. - Системное программное обеспечение. - Пакеты прикладных программ. - Системы (инструменты) программирования.
3	Устройство и архитектура современных вычислительных средств Рассматриваемые вопросы: - Обобщенная структура ЭВМ. - Структура персонального компьютера типа IBM PC. - Микропроцессоры. - Память. - Организация ввода информации. - Организация вывода информации.
4	Операционные системы Рассматриваемые вопросы: - Понятие файла. - Концепция операционной системы Windows. - Объектно-ориентированная платформа Windows. - Основные элементы программных средств операционной системы Windows.
5	Компьютерные сети Рассматриваемые вопросы: - Классификация компьютерных сетей. - Принципы построения компьютерных сетей. - Общая характеристика модели OSI.

№ п/п	Тематика лекционных занятий / краткое содержание
6	Мультимедийные технологии Рассматриваемые вопросы: - Обработка и синтез графики. - Сжатие видеоизображений. - Обработка и синтез звука. - Подготовка цифровых аудиофайлов. - Редактирование цифровой записи.
7	Сетевые технологии Рассматриваемые вопросы: - Стандартизация. - Адресация и маршрутизация. - Показатели качества функционирования.
8	Базы данных Рассматриваемые вопросы: - Классификация баз данных. - Модели данных. - Структурные элементы. - Сверхбольшие базы данных.
9	Системы управления базами данных Рассматриваемые вопросы: - Виды, приницпы построения и архитектура. - Примеры. - Корпоративные СУБД.
10	Понятие безопасной разработки ПО Рассматриваемые вопросы: - Определение безопасности ПО и ее важность. - Основные принципы безопасности. - Типы угроз и атак на ПО.
11	Отечественные и зарубежные стандарты в области разработки безопасного ПО Рассматриваемые вопросы: - Стандарты и методологии разработки безопасного ПО.
12	Криптография и шифрование Рассматриваемые вопросы: - Структура криптосистемы, методы шифрования данных.
13	Межсетевое экранирование Рассматриваемые вопросы: Механизм межсетевого экранирования.
14	Программная инженерия как подраздел системной инженерии. Метод системной инженерии. Рассматриваемые вопросы: - Ключевые концепции и стандарты системной инженерии в целом и программной инженерии в частности. - Системное мышление, системный анализ.
15	Жизненный цикл программного обеспечения. Модель SEMAT Essence. Рассматриваемые вопросы: - Понятие жизненного цикла системы, этапы жизненного цикла системы. - Этапы планирования, проектирования, разработки, тестирования, внедрения, эксплуатации и вывода из эксплуатации.

№ п/п	Тематика лекционных занятий / краткое содержание
16	Теоретические основы кибериммунной разработки и основные артефакты. Рассматриваемые вопросы: - Ключевые концепции MILS, FLASK. - ЦПБ, сценарии, декомпозиция.
17	Особенности постановки задач и методика их решения на примере "безопасное обновление" Рассматриваемые вопросы: - Обязательные разделы. - Критерии качества задания. - Функциональные и нефункциональные требования. - Инструменты построения диаграмм и документирование решения.
18	Инструментарий для решения учебных примеров Рассматриваемые вопросы: - Шина сообщений (Kafka) и монитор безопасности как облегчённая реализация FLASK. - Контейнеризация как облегчённая реализация MILS. - Политики безопасности: как выглядят, как их писать и отлаживать.
19	Аутентификация Рассматриваемые вопросы: - Правила безопасного хранения эталонной копии аутентификационной информации. - Правила безопасной передачи по каналам связи аутентификационной информации. - Понятие о специализированных сетевых протоколах безопасной аутентификаци. - Проблемы парольной аутентификации.
20	Средства защиты систем аутентификации Рассматриваемые вопросы: - Методы подбора пароля. - Средства защиты от подбора и компрометации паролей. - Особенности аутентификации с использованием внешних носителей информации. - Проблемы генерации и распределения ключей. - Особенности биометрической аутентификации. - Особенности аутентификации в системах управления базами данных. - Реализация подсистем аутентификации в распространенных операционных системах.
21	Разграничение доступа Рассматриваемые вопросы: - Избирательное разграничения доступа. - Понятие матрицы доступа. - Два подхода к кодированию матрицы доступа: векторы и списки.
22	Защита от вредоносных воздействий компьютерных вирусов и программных закладок Рассматриваемые вопросы: - Основные типы компьютерных вирусов: файловые, сетевые, почтовые, макровирусы. - Основные модели программных закладок: наблюдатель, перехват, искажение. - Типичные признаки присутствия в системе компьютерных вирусов и программных закладок.
23	Антивирусная защита Рассматриваемые вопросы: - Основные средства и методы противодействия компьютерным вирусам и программным закладкам: сигнатурное и эвристическое сканирование, контроль целостности, антивирусный мониторинг. - Факторы, ограничивающие эффективность антивирусных средств.
24	Защита программ и данных от несанкционированного копирования Рассматриваемые вопросы:

№ п/п	Тематика лекционных занятий / краткое содержание
	- Задача защиты от несанкционированного копирования. - Методы привязки к программно-аппаратной среде. - Применение специальных аппаратных устройств для защиты от несанкционированного копирования информации.

4.2. Занятия семинарского типа.

Лабораторные работы

№ п/п	Наименование лабораторных работ / краткое содержание
1	Формирование отчётной документации к решённым задачам дисциплины В результате выполнения лабораторной работы студент получает умение по формированию отчетной документации к выполненным работам по дисциплины.
2	Изучение основных возможностей текстового процессора Writer В результате выполнения лабораторной работы студент получает навыки в форматировании текста, создании и форматировании таблиц и блок-схем алгоритмов, работе редактора формул.
3	Инструментарий для решения учебных примеров В результате выполнения лабораторной работы студент получает умения по тестированию и отладке политик безопасности, программного обеспечения. Знакомится с средствами автоматического тестирования.
4	Apache Kafka В результате выполнения лабораторной работы студент получает навыки работы с брокерами сообщений и их программного применения.
5	Docker В результате выполнения лабораторной работы студент получает умения работы с системами контейниризации приложений, проводит анализ систем виртуализации и контейниризации.
6	Разбор решения учебных примеров «робот-доставщик» В результате выполнения лабораторной работы студент изучает способ формирования целей безопасности и предположений, реализует диаграммы потока данных.
7	Разбор решения учебных примеров «дрон-опрыскиватель» В результате выполнения лабораторной работы студент исследует информационную систему, проводит последующую доработку программного обеспечения.
8	Модель SEMAT Essence В результате выполнения лабораторной работы студент реализует программное обеспечение с применением модели Essence.
9	Разработка прототипа информационной системы Часть 1 В результате выполнения лабораторной работы студент создаёт архитектурной и текстовое описание исследуемой информационной системы.
10	Разработка прототипа информационной системы Часть 2 В результате выполнения лабораторной работы студент разрабатывает программную реализацию информационной системы, прорабатывает функциональные особенности.
11	Разработка прототипа информационной системы Часть 3 В результате выполнения лабораторной работы студент реализует сквозные тесты функционала системы и создает проектную документацию к системе.
12	Разработка кибериммунной системы на основе прототипа информационной системы Часть 1 В результате выполнения лабораторной работы студент изучает особенности проектирования систем защиты информации.

№ п/п	Наименование лабораторных работ / краткое содержание
13	Разработка кибериммунной системы на основе прототипа информационной системы Часть 2 В результате выполнения лабораторной работы студент моделирует негативные сценарии работы системы, создаёт цели и предположения безопасности к прототипу информационной системы.
14	Разработка кибериммунной системы на основе прототипа информационной системы Часть 3 В результате выполнения лабораторной работы студент реализует возможную декомпозицию системы на основе проведенного моделирования негативных сценариев.
15	Разработка кибериммунной системы на основе прототипа информационной системы Часть 4 В результате выполнения лабораторной работы студент разрабатывает кибериммунный прототип информационной системы.
16	Разработка кибериммунной системы на основе прототипа информационной системы Часть 5 В результате выполнения лабораторной работы студент производит тестирование политики безопасности и так же проверяет сохранение работоспособности функциональности информационной системы.

4.3. Самостоятельная работа обучающихся.

№ п/п	Вид самостоятельной работы
1	Подготовка к лабораторных работам.
2	Изучение литературы по дисциплине.
3	Подготовка к промежуточной аттестации.
4	Подготовка к текущему контролю.

5. Перечень изданий, которые рекомендуется использовать при освоении дисциплины (модуля).

№ п/п	Библиографическое описание	Место доступа
1	Сертификация средств защиты информации Миняев А.А,, Юркин Д.В., Ковцур М.М., Ахрамеева К.А. Учебное пособие СПбГУТ. - СПб., - 88 с. - ISBN 78-5-89160-213-7 , 2020	https://reader.lanbook.com/book/180100#3
2	Обработкка информации в распределенных системах Фомичева С.Г. Учебное пособие СПб.: ГУАП - 132 с. - ISBN 978-5-8088-1487-5 , 2020	https://reader.lanbook.com/book/165237#2

6. Перечень современных профессиональных баз данных и информационных справочных систем, которые могут использоваться при освоении дисциплины (модуля).

Официальный сайт РУТ (МИИТ) (https://www.miit.ru/)

Научно-техническая библиотека РУТ (МИИТ) (http:/library.miit.ru)

Образовательная платформа «Юрайт» (https://urait.ru/)

Общие информационные, справочные и поисковые «Консультант Плюс» (http://www.consultant.ru/)

«Гарант» (http://www.garant.ru/)

Электронно-библиотечная система издательства (http://e.lanbook.com/)

Электронно-библиотечная система ibooks.ru (http://ibooks.ru/)

Stackoverflow (http://stackoverflow.com/)

7. Перечень лицензионного и свободно распространяемого программного обеспечения, в том числе отечественного производства, необходимого для освоения дисциплины (модуля).

Microsoft Internet Explorer (или другой браузер).

Операционная система Ubuntu.

LibreOffice.

Пакет прикладных программ VS Code

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

Учебные аудитории для проведения учебных занятий, оснащенные компьютерной техникой и наборами демонстрационного оборудования.

9. Форма промежуточной аттестации:

Зачет в 8 семестре.

10. Оценочные материалы.

Оценочные материалы, применяемые при проведении промежуточной аттестации, разрабатываются в соответствии с локальным нормативным актом РУТ (МИИТ).

Авторы:

профессор, старший научный сотрудник, д.н. кафедры "Интеллектуальное управление и информационная безопасность в высокоавтоматизированных транспортных системах" Института железнодорожного транспорта — И.Ф. Михалевич

доцент, доцент, к.н. кафедры "Интеллектуальное управление и информационная безопасность в высокоавтоматизированных транспортных системах" Института железнодорожного транспорта — Л.Н. Логинова

А.Д. Домашкин

Согласовано:

Заведующий кафедрой УиЗИ — Л.А. Баранов

Председатель учебно-методической комиссии — С.В. Володин