Министерство науки и высшего образования Российской Федерации
ФГБОУ ВО «Тверской государственный университет»

Утверждаю:
Проректор по образовательной деятельности и молодежной политике
Сердитова Н.Е.
«04» февраля 2025 г.

Рабочая программа факультативной дисциплины (с аннотацией)

# СПОРТИВНОЕ ПРОГРАММИРОВАНИЕ
## (для этичных хакеров)

Для обучающихся математического факультета
очной формы обучения

Составитель: Шавыкин О.В.

Тверь, 2025

**I. Аннотация**

**1. Цель и задачи дисциплины**

*Цель* – овладение знаниями и навыками проектирования и разработки систем информационной безопасности с использованием современных языков программирования. Изучение методологии тестирования на проникновения и решение задач из соответствующей дисциплины спортивного программирования.

*Задача дисциплины:*

формирование навыков использования совокупности методов и практик защиты от атак злоумышленников для компьютеров, серверов, мобильных устройств, электронных систем, сетей и данных.

**2. Место дисциплины в структуре ООП**

Дисциплина «Спортивное программирование» является факультативной.

**3. Объем дисциплины:**

2 зачетные единицы, 72 академических часа, **в том числе:**

**контактная аудиторная работа:** лекции – 24 ч., в т.ч. практическая подготовка – 0 часов;

практические занятия – 36 ч., в т.ч. практическая подготовка – 12 ч.;

**самостоятельная работа:** 12 ч.

**4. Планируемые результаты обучения по дисциплине, соотнесенные с планируемыми результатами освоения образовательной программы**

| Планируемые результаты освоения образовательной программы (формируемые компетенции) | Планируемые результаты обучения по дисциплине |
|---|---|
| **ОПК-7** Способен создавать программы на языках высокого и низкого уровня, применять методы и инструментальные средства программирования для решения профессиональных задач, осуществлять обоснованный выбор инструментария программирования и способов организации программ | **ОПК-7.1** Разрабатывает и применяет на языке высокого уровня алгоритмы решения типовых профессиональных задач<br>**ОПК-7.2** Применяет известные методы программирования и возможности базового языка программирования для решения типовых профессиональных задач<br>**ОПК-7.3** Использует основные принципы разработки, документирования, тестирования и отладки программ |

| | |
|---|---|
| **ПК-5** Способен производить установку, наладку, тестирование и обслуживание программно-аппаратных средств обеспечения информационной безопасности компьютерных систем | **ПК-5.1** Производит эксплуатацию информационно-аналитических систем в защищенном исполнении<br>**ПК-5.2** Тестирует системы защиты информации автоматизированных систем<br>**ПК-5.3** Разрабатывает эксплуатационную документацию на системы защиты информации автоматизированных систем |

**5. Форма промежуточной аттестации** – зачет.

**6. Язык преподавания** русский.

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

| Учебная программа – наименование разделов и тем | Всего (час.) | Контактная работа (час.) | | | Самостоятельная работа, в том числе Контроль (час.) |
|---|---|---|---|---|---|
| | | Лекции | Практические занятия | | |
| | | | всего | в т.ч. практическая подготовка | |
| Тема 1. Программные закладки. Шеллкод. Эксплойты | 6 | 2 | 3 | 1 | 1 |
| Тема 2. Атаки на переполнения стека | 6 | 2 | 3 | 1 | 1 |
| Тема 3. Внедрение программных закладок и SQL-кода | 6 | 2 | 3 | 1 | 1 |
| Тема 4. Компьютерные вирусы. Бэкдоры. Буткиты | 6 | 2 | 3 | 1 | 1 |
| Тема 5. Противодействие программным закладкам | 6 | 2 | 3 | 1 | 1 |
| Тема 6. Фаззинг | 6 | 2 | 3 | 1 | 1 |
| Тема 7. Уязвимости по сети | 12 | 4 | 6 | 2 | 2 |

| | | | | | |
|---|---|---|---|---|---|
| Тема 8. Спортивные соревнования типа «Атака–защита» | 6 | 2 | 3 | 1 | 1 |
| Тема 9. Стеганография | 6 | 2 | 3 | 1 | 1 |
| Тема 10. Поиск по открытым источникам | 6 | 2 | 3 | 1 | 1 |
| Тема 11. Форензика | 6 | 2 | 3 | 1 | 1 |
| **ИТОГО** | **72** | **24** | **36** | **12** | **12** |

**III. Образовательные технологии**

| Учебная программа – наименование разделов и тем | Вид занятия | Образовательные технологии |
|---|---|---|
| Тема 1. Программные закладки. Шеллкод. Эксплойты | лекция<br>практическое занятие | Дискуссионные технологии, дистанционные образовательные технологии, проблемная лекция, кейс-технология, технология развития креативного мышления |
| Тема 2. Атаки на переполнения стека | лекция<br>практическое занятие | |
| Тема 3. Внедрение программных закладок и SQL-кода | лекция<br>практическое занятие | |
| Тема 4. Компьютерные вирусы. Бэкдоры. Буткиты | лекция<br>практическое занятие | |
| Тема 5. Противодействие программным закладкам | лекция<br>практическое занятие | |
| Тема 6. Фаззинг | лекция<br>практическое занятие | |
| Тема 7. Уязвимости по сети | лекция<br>практическое занятие | |
| Тема 8. Спортивные соревнования типа «Атака–защита» | лекция<br>практическое занятие | |
| Тема 9. Стеганография | лекция<br>практическое занятие | |
| Тема 10. Поиск по открытым источникам | лекция<br>практическое занятие | |
| Тема 11. Форензика | лекция<br>практическое занятие | |

**IV. Оценочные материалы для проведения текущей и промежуточной аттестации**

**Задание 1.** Проведите дешифрованием текста, зашифрованного XOR-ом и алгоритмом Хилла.

**Задание 2.** Проведите дизассемблирование программы и распознайте какой длины входной текст необходим для возникновения переполнения стека.

**Задание 3.** Разработайте шеллкод для открытия порта 80 для удаленного доступа.

**Задание 4.** Подберите SQL-инъекцию для проникновения на уязвимый web-сервер и предложите способы защиты от этой уязвимости.

**Задание 5.** Проведите фаззинг тестирование программы на наличие узявимости форматной строки.

**Задание 6.** При помощи стеганографических методов найдите информацию, скрытую в графическом изображении.

*Примерные вопросы к зачету*

1. Понятие кибербезопасности и современные направления в ней.
2. Области применения ассемблера в современном мире. Регистры. Области памяти. Понятие стека и кучи.
3. Описать процесс дизассемблирования и его основные отличия от декомпиляции. Сформулировать основные этапы при анализе бинарных файлов.
4. Защиты программ от изучения при помощи запутывания кода. Основные подходы к запутыванию кода. Существуют ли подход к запутыванию кода, который невозможно запутать? Обратная разработка в условиях запутанного кода.
5. Основные методы внедрения вредоносного кода. Разновидности способов доставки вредоносного кода на машину-жертву. Способы борьбы против внедрения вредоносного кода.
6. Фаззинг-тестирование. Статический анализ кода.
7. Фаззинг-тестирование. Динамический анализ кода.
8. Сетевые уязвимости веб-серверов.
9. Создание инфраструктуры для проведения соревнований типа «Атака-защита».
10. Использование основных инструментов для тестирования на проникновение nmap, metasploit и др.
11. Основные стеганографические методы сокрытия информации и способы извлечения «спрятанной» информации.
12. Что такое замыкание (closure)?
13. Сформулировать основные шаги и инструменты, которые используются при поиске по открытым источникам
14. Методология при анализе компьютерных преступлений.

**V. Учебно-методическое и информационное обеспечение дисциплины**

1) Рекомендуемая литература

а) Основная литература

Мейер, Б. Объектно-ориентированное программирование и программная инженерия : учебное пособие / Б. Мейер. — 4-е изд. — Москва : Интернет-Университет Информационных Технологий (ИНТУИТ), Ай Пи Ар Медиа, 2024. — 284 с. — ISBN 978-5-4497-2464-9. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: https://www.iprbookshop.ru/133956.html

Самуйлов, С. В. Объектно-ориентированное моделирование на основе UML : учебное пособие / С. В. Самуйлов. — Саратов : Вузовское образование, 2016. — 37 с. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: https://www.iprbookshop.ru/47277.html

Буч, Г. Язык UML. Руководство пользователя : руководство / Г. Буч, Д. Рамбо, И. Якобсон. — Москва : ДМК Пресс, 2008. — 496 с. — ISBN 5-94074-334-X. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/1246

б) Дополнительная литература:

Лафоре Роберт. Объектно-ориентированное программирование в C++ / Лафоре Роберт; пер. с англ. А. Кузнецов, М. Назаров, В. Шрага. - 4-е изд. - Москва [и др.] : Питер, 2012.

Гамма Э. Приемы объектно-ориентированного проектирования : паттерны проектирования : [принципы применения паттернов проектирования, классификация паттернов, различные подходы к выбору паттернов, каталог паттернов с детальным их описанием] / Гамма Эрих [и др.]; [пер. с англ. А. Слинкин]. - Москва [и др.] : Питер, 2012.

Фримен Эрик. Паттерны проектирования / Фримен Эрик, Фримен Элизабет; при участии К. Сьерра. и Б. Бейтса ; [пер. с англ. Е. Матвеева]. - Москва [и др.] : Питер, 2012. - 645 с.

2) Программное обеспечение

| | |
|---|---|
| Adobe Acrobat Reader DC - Russian | бесплатно |
| Cadence SPB/OrCAD 16.6 | Государственный контракт на поставку лицензионных программных продуктов 103 - ГК/09 от 15.06.2009 |
| Git version 2.5.2.2 | бесплатно |
| Google Chrome | бесплатно |
| Kaspersky Endpoint Security 10 для Windows | Акт на передачу прав ПК545 от 16.12.2022 |
| Lazarus 1.4.0 | бесплатно |
| Mathcad 15 M010 | Акт предоставления прав ИС00000027 от 16.09.2011 |
| MATLAB R2012b | Акт предоставления прав № Us000311 от 25.09.2012 |

| | |
|---|---|
| Многофункциональный редактор ONLYOFFICE | бесплатно |
| ОС Linux Ubuntu бесплатное ПО | бесплатно |
| Microsoft Web Deploy 3.5 | бесплатно |
| MiKTeX 2.9 | бесплатно |
| MSXML 4.0 SP2 Parser and SDK | бесплатно |
| MySQL Workbench 6.3 CE | бесплатно |
| NetBeans IDE 8.0.2 | бесплатно |
| Notepad++ | бесплатно |
| Origin 8.1 Sr2 | договор №13918/M41 от 24.09.2009 с ЗАО «СофтЛайн Трейд» |
| PostgreSQL 9.6 | бесплатно |
| Python 3.4.3 | бесплатно |
| Visual Studio 2010 Prerequisites - English | Акт на передачу прав №785 от 06.08.2021 г. |
| WCF RIA Services V1.0 SP2 | бесплатно |
| WinDjView 2.1 | бесплатно |
| WinPcap 4.1.3 | бесплатно |
| Wireshark 2.0.0 (64-bit) | бесплатно |
| R studio | бесплатно |

3) Современные профессиональные базы данных и информационные справочные системы:

1. ЭБС Лань https://e.lanbook.com/
2. ЭБС Znanium.com https://znanium.com/
3. ЭБС Университетская библиотека online https://biblioclub.ru
4. ЭБС ЮРАЙТ https://urait.ru/
5. ЭБС IPR SMART https://www.iprbookshop.ru/
6. Репозитарий ТвГУ http://eprints.tversu.ru

4) Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины:

Независимый информационно-аналитический портал по безопасности
https://cyberleninka.ru/ научная электронная библиотека «Киберленинка».
Научная электронная библиотека eLIBRARY.RU (подписка на журналы)
https://elibrary.ru/projects/subscription/rus_titles_open.asp

## VI. Методические материалы для обучающихся по освоению дисциплины

***Методические рекомендации по организации самостоятельной работы студентов***

На лекциях будет представлен необходимый теоретически материал по темам и представлены практические задания для решения на занятиях в аудитории под руководством преподавателя и самостоятельно. Многие задачи являются стандартными и имеют уже готовые шаблоны (алгоритмы) решения, тем не менее,

для получения большего познавательного и учебного эффекта, рекомендуется написание собственного оригинального кода.

Самостоятельная работа студентов в рамках данной дисциплины в основном состоит в подготовке к практическим занятиям и работе с разными источниками. Освоению учебного материала большую помощь окажет личный творческий подход, связанный с дополнительным просмотром материала по отдельным темам.

Самостоятельная работа является необходимой на всех стадиях и при всех формах изучения предмета. Важно помнить, что часы для самостоятельной работы, из всего объема времени, затраченного на дисциплину, будут превосходить иные виды работ. Важно продумать стиль фиксации нового и важного материала.

Рекомендуется немедленно обсуждать любые возникшие в процессе обучения вопросы, проблемы и неясности с преподавателем, не откладывая это обсуждение до контрольной точки. Проконсультироваться с преподавателем можно во время и после практических занятий, во время консультаций, а также по электронной почте и в личном кабинете электронной образовательной среды (LMS).

## VII. Материально-техническое обеспечение

Учебный процесс по данному факультативу проводится в аудиториях, оснащенных мультимедийными средствами обучения. Для организации самостоятельной работы студентов необходимо наличие персональных компьютеров с доступом в Интернет.

| Наименование специальных* помещений и помещений для самостоятельной работы | Оснащенность специальных помещений и помещений для самостоятельной работы | Перечень лицензионного программного обеспечения. Реквизиты подтверждающего документа |
|---|---|---|
| Учебная аудитория для проведения занятий лекционного типа, занятий семинарского типа, курсового проектирования (выполнения курсовых работ), групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации, Учебная аудитория. Математический кабинет № 213 (Корпус 3, 170002, | Столы, стулья, переносной ноутбук, проектор | Adobe Acrobat Reader DC – Russian – бесплатно; Cadence SPB/OrCAD 16.6-Государственный контракт на поставку лицензионных программных продуктов 103 - ГК/09 от 15.06.2009; Git version 2.5.2.2 – бесплатно; Google Chrome – бесплатно; Kaspersky Endpoint Security 10 для Windows – акт на передачу прав ПК545 от 16.12.2022; Lazarus 1.4.0 – бесплатно; Mathcad 15 M010 – акт предоставления прав ИС00000027 от 16.09.2011; MATLAB R2012b – акт |

| | | |
|---|---|---|
| Тверская обл., г.Тверь, пер. Садовый, дом 35)<br><br>Учебная аудитория для проведения занятий лекционного типа, занятий семинарского типа, курсового проектирования (выполнения курсовых работ), групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации,<br>Учебная аудитория № 203 (Корпус 3, 170002, Тверская обл., г.Тверь, пер. Садовый, дом 35) | Столы, стулья, переносной ноутбук, проектор | предоставления прав № Us000311 от 25.09.2012;<br>Многофункциональный редактор ONLYOFFICE – бесплатное ПО;<br>ОС Linux Ubuntu – бесплатное ПО;<br>Microsoft Web Deploy 3.5 – бесплатно;<br>MiKTeX 2.9 – бесплатно;<br>MSXML 4.0 SP2 Parser and SDK – бесплатно;<br>MySQL Workbench 6.3 CE – бесплатно;<br>NetBeans IDE 8.0.2 – бесплатно; Notepad++ – бесплатно;<br>Origin 8.1 Sr2 –договор №13918/M41 от 24.09.2009 с ЗАО «СофтЛайн Трейд»;<br>PostgreSQL 9.6 –бесплатно;<br>Python 3.4.3 –бесплатно;<br>Visual Studio 2010 Prerequisites – English – акт на передачу прав №785 от 06.08.2021 г.;<br>WCF RIA Services V1.0 SP2 – бесплатно;<br>WinDjView 2.1 – бесплатно;<br>WinPcap 4.1.3 – бесплатно;<br>Wireshark 2.0.0 (64-bit) – бесплатно; R studio – бесплатно. |
| Учебная аудитория для проведения занятий лекционного типа, занятий семинарского типа, курсового проектирования (выполнения курсовых работ), групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации,<br>Учебная | Столы, стулья, переносной ноутбук, проектор | Google Chrome – бесплатное ПО;<br>Kaspersky Endpoint Security 10 – акт на передачу прав ПК545 от 16.12.2022;<br>Lazarus – бесплатное ПО;<br>OpenOffice – бесплатное ПО;<br>Многофункциональный редактор ONLYOFFICE – бесплатное ПО;<br>ОС Linux Ubuntu — бесплатное ПО |

| | | |
|---|---|---|
| аудитория № 314<br>(Корпус 3, 170002,<br>Тверская обл., г. Тверь,<br>пер. Садовый, дом 35) | | |

## VIII. Сведения об обновлении рабочей программы дисциплины

| № п.п. | Обновленный раздел рабочей программы дисциплины | Описание внесенных изменений | Реквизиты документа, утвердившего изменения |
|---|---|---|---|
| | | | |
| | | | |