

Министерство науки и высшего образования Российской Федерации  
Федеральное государственное бюджетное образовательное учреждение  
высшего образования  
«Амурский государственный университет»

УТВЕРЖДАЮ

Проректор по ИиНОТ

 А.А. Остапенко

«30»  2019 г.

РАБОЧАЯ ПРОГРАММА  
ОСНОВЫ КОМПЬЮТЕРНОЙ БЕЗОПАСНОСТИ

Уровень образования: дополнительное

Направление: малая академия

Форма обучения: очная

Год обучения: 2020

Общая трудоемкость дисциплины – 72 (час.)

Составитель – Саяпин В.А.

ЦРСКД «АмурТехноЦентр» (ДНК им. академика РАН М.Т. Луценко)

2019 г.


Рабочая программа одобрена на заседании методического совета ЦРСКД  
«АмурТехноЦентр» (ДНК им. академика РАН М.Т. Луценко)

«30» декабря 2019 г., протокол № 5

Председатель  В.В. Еремина  
подпись И.О.Ф.


СОГЛАСОВАНО

Директор

 Еремина В.В.  
«30» декабря 2019 г.

СОГЛАСОВАНО

Руководитель проекта

 Сяпин В.А.  
«30» декабря 2019 г.

## ПОЯСНИТЕЛЬНАЯ ЗАПИСКА

Компьютерная безопасность — меры безопасности, применяемые для защиты вычислительных устройств (компьютеры, смартфоны и другие), а также компьютерных сетей (частных и публичных сетей, включая Интернет).

Содержание программы направлено на формирование у обучающихся научно-технических знаний, профессионально-прикладных навыков и создание условий для социального, культурного и профессионального самоопределения, творческой самореализации личности ребенка в окружающем мире. А также на воспитание у обучающихся общей информационной культуры, развитие достаточно широкого взгляда на методы и технологии защиты компьютеров, программных сервисов и программного обеспечения, сильно повышают компьютерную грамотность.

Актуальность программы. Компьютерная безопасность является перспективной областью для применения образовательных методик в процессе обучения за счет объединения в себе различных инженерных и естественнонаучных дисциплин, огромного охвата широкого спектра компьютерных технологий. Программа даёт возможность обучить детей профессиональным навыкам в области программирования, прототипирования, выявления компьютерных уязвимостей, применения методов борьбы с ними. Обучение по данной программе формировать компетентность в вопросах связанных с криптографией, стеганографией, архитектурой компьютерных сетей, методов обеспечения безопасности компьютерных сетей, архитектурой веб приложений, веб уязвимостями, архитектуры операционных сетей, низкоуровневым программированием, синтаксисом ассемблера.

Новизна данной дополнительной образовательной программы заключается в том, что по форме организации образовательного процесса она является модульной.

Уровень подготовки детей, участвующих в реализации данной дополнительной образовательной программы, колеблется от 10-11 классов. Для занятий по данной программе учащиеся должны отлично знать школьный курс информатики, владеть основами программирования (желательно язык C/C++), знания о компьютерных сетях, работе операционных систем и современных приложений.

Сроки реализации программы: 1 год. Режим занятий – 1 раз в неделю по 2 академических часа, наполняемость в группе – 12 учащихся.

**Цель:** теоретическая и практическая подготовка обучающихся в области компьютерной безопасности с использованием современных программных инструментов.

### **Задачи:**

ознакомить со сферой компьютерной безопасности, основными компьютерными уязвимостями и методами их устранения;

обучить находить уязвимости компьютерных сетей, операционных систем, современных приложений, решать задания основных категорий соревнований CTF;

научить основам алгоритмического мышления и низкоуровневого программирования;

определить дальнейшее направления обучения после освоения данной программы;

способствовать формированию творческого отношения к выполняемой работе;

воспитывать умение работать в коллективе, эффективно распределять обязанности;

развивать творческую инициативу и самостоятельность;

развивать психофизиологические качества учащихся: память, внимание, способность логически мыслить, анализировать, концентрировать внимание на главном;

развивать умения излагать мысли в четкой логической последовательности, отстаивать свою точку зрения, анализировать ситуацию и самостоятельно находить ответы на вопросы путем логических рассуждений.

Для реализации данной программы используются педагогические технологии уровневой дифференциации обучения, технологии на основе личностной ориентации, а также следующие методы и формы обучения и контроля: фронтальный опрос, индивидуальная, парная, групповая работа.

Методами обучения являются: поисковый метод, самостоятельная работа, метод кейсов, дидактические игры, метод проблемного обучения, дискуссия, практическая деятельность, ИКТ.

## ЛИЧНОСТНЫЕ, МЕТАПРЕДМЕТНЫЕ И ПРЕДМЕТНЫЕ РЕЗУЛЬТАТЫ ОСВОЕНИЯ УЧЕБНОГО ПРЕДМЕТА

*Личностные результаты:*

- ответственное отношение к выполнению заданий и стремление к получению результата;
- навык самостоятельного решения задач;
- умение работать в команде при решении задач.

*Метапредметные результаты:* программа направлена на развитие мышления учащихся и воспитания у них информационной культуры. На занятиях выполняются задания, развивающие творчество учащихся, умение анализировать, систематизировать, визуализировать информацию. Учащиеся учатся моделировать реально происходящие процессы, т.е. создавать информационную модель поставленной задачи.

*Предметные результаты:*

- осуществление поиска компьютерных уязвимостей и решение их;
- умение решать задания с соревнований CTF;
- получает и анализирует опыт разработки оригинальных задач в заданной ситуации: подборка вариантов, отбор решений, проектирование, тестирование, анализ, способы модернизации, альтернативные решения.

Содержание курса представлено в составе восьми модулей: Введение в компьютерную безопасность, Криптография, Хеш-функции и криптовалюты, Стеганография, Сети, Web приложения, Инъекции, Низкоуровневое программирование.

## УЧЕБНО-ТЕМАТИЧЕСКИЙ ПЛАН

Структура курса рассчитана на 72 часов

№ урока	Содержание учебного материала	Количество часов		
		всего	теория	практик
1	Введение в компьютерную безопасность	2	2	0
2	Криптография	10	5	5
3	Хеш-функции и криптовалюты	10	5	5
4	Стеганография	10	5	5
5	Сети	12	6	6
6	Web приложения	11	4	7
7	Инъекции	5	2	3
8	Низкоуровневое программирование	12	8	4
	ИТОГО	72	37	35

## СОДЕРЖАНИЕ ТЕМ УЧЕБНОГО КУРСА

### Модуль 1 «Введение компьютерную безопасность» (2 часа)

Реализация этого модуля направлена на ознакомление со сферой компьютерной безопасности, с соревнованиями CTF проводимые в данной области, с темами данного курса.

**Цель модуля:** ознакомление с компьютерной безопасностью.

**Задачи модели:** изучить области компьютерной безопасности, соревнования CTF.

### Учебно-тематический план Модуля 1

№ п/п	Наименование темы	Количество часов			Формы аттестации/контроля
		всего	теория	практика	
1	Введение в компьютерную безопасность. Соревнования и платформы CTF.	2	2	0	-
	Итого:	2	2	0	

### Модуль 2 «Криптография» (10 часов)

Реализация этого модуля направлена на знакомство с криптографией, изучения основных алгоритмов шифров, решение практических заданий по криптоанализу.

**Цель модуля:** ознакомление с криптографией.

**Задачи модели:** изучить основы криптографии, алгоритм Цезаря, симметричные и асимметричные шифры, электронно-цифровая подпись, научиться решать задачи по криптоанализу.

### Учебно-тематический план Модуля 2

№ п/п	Наименование темы	Количество часов			Формы аттестации/контроля
		всего	теория	практика	
1	Введение в криптографию. История криптографии. Простейшие шифры. Алгоритм цезаря.	2	1	1	Выполнение домашнего задания №1
2	Симметричные и асимметричные шифры. Алгоритм Диффи-Хеллмана.	2	1	1	Выполнение домашнего задания №2
3	Алгоритм RSA. Корректность работы алгоритма RSA.	2	1	1	Выполнение домашнего задания №3
4	Электронно-цифровая подпись.	2	1	1	Выполнение домашнего задания №4
5	Решение заданий CTF по криптоанализу.	2	1	1	Выполнение домашнего задания №5

	Итого:	2	2	0	
--	--------	---	---	---	--

### Модуль 3 «Хеш функции и криптовалюты» (10 часов)

Реализация этого модуля направлена на знакомство с хеш-функциями, криптовалютой Bitcoin.

**Цель модуля:** ознакомление с хеш функциями.

**Задачи модели:** изучить основы криптографии, алгоритм Цезаря, симметричные и асимметричные шифры, электронно-цифровая подпись, научиться решать задачи по криптоанализу.

#### Учебно-тематический план Модуля 3

№ п/п	Наименование темы	Количество часов			Формы аттестации/контр оля
		всего	теория	практика	
1	Хеш-функции. Применение хеш- функций.	2	1	1	Выполнение домашнего задания №6
2	Криптографические хеш-функции. Применение криптографических хеш-функций	2	1	1	Выполнение домашнего задания №7
3	Архитектура Bitcoin. Экономика Bitcoin.	2	1	1	Выполнение домашнего задания №8
4	Решение заданий STF по криптоанализу.	4	1	3	Выполнение домашнего задания №9
	Итого:	10	4	6	

### Модуль 4 «Стеганография» (10 часов)

Реализация этого модуля направлена на знакомство с наукой стеганографии.

**Цель модуля:** ознакомление с стеганографией, методами стегоанализа.

**Задачи модели:** изучить основы стеганографии, методы стегоанализа, примеры стеганографии в тексте, изображениях, видео, звуке; цифровые водяные знаки.

#### Учебно-тематический план Модуля 4

№ п/п	Наименование темы	Количество часов			Формы аттестации/контр оля
		всего	теория	практика	
1	Введение в стеганографию. Стегоанализ.История стеганографии. Компьютерная	2	1	1	Выполнение домашнего задания №10

	стеганография. Текстовая стеганография.				
2	Стеганография в изображениях. Картинка в картинке. RARJPEG	2	1	1	Выполнение домашнего задания №11
3	Стеганография в звуке и видео.	2	1	1	Выполнение домашнего задания №12
4	Цифровые водяные знаки.	2	1	1	Выполнение домашнего задания №13
5	Решение заданий CTF по стеганографии.	2	1	1	
	Итого:	10	5	5	

#### Модуль 5 «Сети» (12 часов)

Реализация этого модуля направлена на знакомство с сетями, с основными протоколами стека OSI.

**Цель модуля:** ознакомление с сетями, стек OSI.

**Задачи модели:** изучить стек OSI, стек TCP/IP, IP-адресация, протокол DHCP, ARP, TCP, NAT, DNS, FTP, SMTP, HTTP; основы HTML, VPN и туннелирование.

#### Учебно-тематический план Модуля 5

№ п/п	Наименование темы	Количество часов			Формы аттестации/контр оля
		всего	теория	практика	
1	Стек OSI. Стек TCP/IP. Физический уровень. Канальный уровень. Сетевой уровень. IP- адреса. Протокол DHCP, ARP. Маршрутизация. Протокол TCP. Порты. Протокол NAT.	3	2	1	Выполнение домашнего задания №14
2	Протоколы прикладного уровня. Протокол DNS. Иерархия NS-серверов. Отравление кеша в	3	2	1	Выполнение домашнего задания №15

	DNS. Дополнительные подробности о DNS. Протокол FTP. Протокол SMTP. Туннелирование и VPN.				
3	История HTTP. Структура HTTP. URL. Методы HTTP. Заголовки HTTP. Авторизация и аутентификация. Протокол HTTPS. Протокол CGI. Введение в HTML. HTML формы. Атаки на HTML.	3	2	1	Выполнение домашнего задания №16
4	Решение заданий CTF по сетям.	3	0	3	-
	Итого:	12	6	6	

### Модуль 6 «Web-приложения» (11 часов)

Реализация этого модуля направлена на знакомство архитектурой веб приложений, веб технологиями, основными веб уязвимостями и методами их устранения.

**Цель модуля:** ознакомление с веб уязвимостями.

**Задачи модели:** изучить архитектура веб приложений, стеки ПО веб приложения, основные веб уязвимости и методы борьбы с ними.

#### Учебно-тематический план Модуля 6

№ п/п	Наименование темы	Количество часов			Формы аттестации/контроля
		всего	теория	практика	
1	Архитектура веб приложений. Технология "клиент-сервер". Стеки ПО: - веб-серверы: Apache, Nginx; - языки программирования: PHP, JS, Python и другие; - базы данных: SQL,	3	2	1	Выполнение домашнего задания №17



	NOSQL; Стек LAMP. CMS.				
2	Уязвимости веб приложений.	4	2	2	Выполнение домашнего задания №18
3	Решение заданий CTF по веб уязвимостям.	4	0	4	-
	Итого:	11	4	7	

### Модуль 7 «Инъекции» (5 часов)

Реализация этого модуля направлена на знакомство с областью компьютерной уязвимости, как инъекции, и методами борьбы с ними.

**Цель модуля:** ознакомление с инъекции и методами борьбы с ними.

**Задачи модели:** изучить инъекции, виды инъекций, методы борьбы с ними.

### Учебно-тематический план Модуля 7

№ п/п	Наименование темы	Количество часов			Формы аттестации/контроля
		всего	теория	практика	
1	Инъекции. SQL-инъекции. SQL-инъекции с UNION. Группировка, сортировка и работа с файлами. Экранирование символов. Множественные запросы. Слепые инъекции. NoSQL. CSS. LDAP. XPath. Инъекции в командах ОС. Инъекции в HTTP заголовки.	2	2	0	Выполнение домашнего задания №19
2	Решение заданий CTF по инъекциям.	3	0	3	-
	Итого:	5	2	3	

### Модуль 8 «Низкоуровневое программирование» (12 часов)

Реализация этого модуля направлена на знакомство с операционными системами, историей операционных систем, основы низкоуровневого программирования, reverse engineering, бинарных уязвимостей.

**Цель модуля:** ознакомление с инъекции и методами борьбы с ними.

**Задачи модели:** изучить инъекции, виды инъекций, методы борьбы с ними.

#### Учебно-тематический план Модуля 8

№ п/п	Наименование темы	Количество часов			Формы аттестации/контр оля
		всего	теория	практика	
1	Операционные системы. GNU, FSF. Стандарт POSIX, Minix. История Linux, дистрибутивы. Unix Way. Загрузка системы. Пользователи. Команды Linux. Виртуальные машины. Основные команды Bash.	2	2	0	Выполнение домашнего задания №20
2	Архитектура компьютера. Принцип Фон Неймана. Регистры процессоров. Ассемблер. Команда MOV. Стек. Арифметические и логические операции. Знаковые числа. Безусловный переход. Управление выполнением программы. Функции. Структура исполняемого файла.	2	2	0	Выполнение домашнего задания №21
3	Введение в Reverse Engineering. Форматы исполняемых файлов. Как устроен PE-файл. Паттерны исполняемого кода.	2	2	0	Выполнение домашнего задания №22

	Объектно-ориентированное программирование. Пакеры. Антиотладка.				
4	Введение в бинарные уязвимости. Отладчик GDB. Переполнение стека. Исполнение кода, шеллкод. OpenSSL Heartbleed. Уязвимость форматной строки. Запись произвольной памяти.	2	2	0	Выполнение домашнего задания №23
5	Решение заданий CTF по reverse engineering.	4	0	0	-
	Итого:	12	8	4	

#### **МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ:**

Занятия реализовываться в учебном кабинете (компьютерный класс). Классы оснащены необходимой мебелью: столы, стулья по количеству обучающихся, рабочее место для педагога, флипчарт. Кабинет оснащен техническими средствами: мультимедиа-проектор, интерактивная доска, ноутбуки для каждого обучающегося с необходимым установленным ПО; компьютер для педагога, веб-камерами, МФУ формата А4, соединение с Интернетом. Кабинеты оснащены расходными материалами для проведения занятий: бумага формата А4, карандаши, ластик, ручки, циркули, линейки, маркеры для доски, ножницы, др.

#### **ПЕРЕЧЕНЬ УЧЕБНО-МЕТОДИЧЕСКОГО ОБЕСПЕЧЕНИЯ**

- 1) Фленов - Linux глазами хакера
- 2) Костромин - Linux для пользователя
- 3) Стахнов Linux 4-е изд.
- 4) Жуков - "Основы веб-хакинга"
- 5) Clarke - "SQL Injection Attacks and Defense, Second Edition"
- 6) Низамутдинов М.Ф. - Тактика защиты и нападения на Web-приложения.
- 7) Панов - "Реверсинг и защита программ от взлома"
- 8) Крис Касперски - "Искусство дизассемблирования"
- 9) Н.Н.Федотов - Форензика – компьютерная криминалистика
- 10) Ресурсы Хакердома:  
<https://ulearn.azurewebsites.net/Course/Hackerdom>  
<http://training.hackerdom.ru/>
- 11) Курс молодого бойца от Андрея Петухова:  
[https://docs.google.com/document/d/13zgZ\\_CRRHADwxf41m..](https://docs.google.com/document/d/13zgZ_CRRHADwxf41m..)
- 12) Курс CTF на Физтехе  
<https://github.com/xairy/mipt-ctf>
- 13) <http://itsecwiki.org>
- 14) <http://kmb.ufoctf.ru/>
- 15) <http://pycode.ru/2011/01/ctf/>