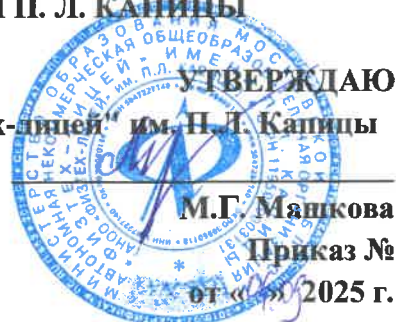


**МИНИСТЕРСТВО ОБРАЗОВАНИЯ МОСКОВСКОЙ ОБЛАСТИ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ
УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«МОСКОВСКИЙ ФИЗИКО-ТЕХНИЧЕСКИЙ ИНСТИТУТ (НАЦИОНАЛЬНЫЙ
ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ)»
АВТОНОМНАЯ НЕКОММЕРЧЕСКАЯ ОБЩЕОБРАЗОВАТЕЛЬНАЯ
ОРГАНИЗАЦИЯ «ФИЗТЕХ-ЛИЦЕЙ» ИМЕНИ П. Л. КАПИЦЫ**

Директор АНОО "Физтех-лицей" им. П. Л. Капицы



Принята на заседании
методического совета
Протокол № 3 от 19.06.2025

СОГЛАСОВАНО
Заведующий кафедры Информатики
Мерзляков В.В.

СОГЛАСОВАНО
Заместитель директора
по дополнительному
образованию
Меньшакова С.А.

**Дополнительная общеобразовательная общеразвивающая программа
«Информационная безопасность»
(Естественно-научной направленности)**

Уровень программы: продвинутый
Срок реализации программы: 7 месяцев
Возрастная категория: 15 – 18 лет
Состав группы: 15 обучающихся
Форма обучения: очная

Составитель:
Мерзляков А.В.,
учитель информатики

г. Долгопрудный
2025

Содержание

Введение

Нормативно-правовая база

1. Раздел 1. Комплекс основных характеристик образования:

- 1.1. Пояснительная записка
- 1.2. Цель и задачи
- 1.3. Содержание программы
- 1.4. Планируемые результаты
- 1.5. Учебный план

2. Раздел 2. Комплекс организационно-педагогических условий:

- 2.1. Календарный учебный график
- 2.2. Условия реализации программы
- 2.3. Формы аттестации
- 2.4. Оценочные материалы
- 2.5. Методические материалы
- 2.6. Раздел воспитания
- 2.7. Список литературы

Введение

В современном цифровом обществе информационная безопасность (ИБ) является одним из ключевых направлений инженерной подготовки. С ростом числа киберугроз, масштабов хранения персональных данных, сложности сетевой инфраструктуры и автоматизации бизнес-процессов возрастает потребность в специалистах, обладающих не только техническими навыками, но и системным пониманием принципов защиты информации.

Курс «Информационная безопасность» предназначен для школьников старших классов, обладающих продвинутым уровнем подготовки в области программирования и математики. Программа ориентирована на развитие практических навыков в сферах анализа уязвимостей, криптографии, реверс-инжиниринга, а также на подготовку к соревнованиям по кибербезопасности: CTF (Capture The Flag) и профильным олимпиадам.

В рамках курса обучающиеся осваивают как теоретические основы защиты информации, так и применяют знания в ходе практических работ и проектной деятельности. Занятия включают как индивидуальные, так и командные форматы, позволяют развивать навыки стратегического мышления, анализа угроз, восстановления логики программного кода и моделирования атак.

Программа рассчитана на 28 учебных недель и включает 84 академических часа. В процессе обучения также рассматриваются правовые и этические аспекты ИБ, включая отечественное и международное законодательство, что формирует комплексный подход к кибербезопасности.

Нормативно-правовая база

Программа разработана в соответствии с действующими нормативно-правовыми актами и методическими рекомендациями:

- Федеральный закон от 29 декабря 2012 г. № 273-ФЗ «Об образовании в Российской Федерации»;
- Приказ Министерства просвещения РФ от 27 июля 2022 года № 629 «Об утверждении Порядка организации и осуществления образовательной деятельности по дополнительным общеобразовательным программам»;
- Постановление Главного государственного санитарного врача РФ от 28.09.2020 г. № 28 «Санитарные правила СП 2.4.3648-20»;
- Концепция развития дополнительного образования детей, утверждённая распоряжением Правительства РФ от 31 марта 2022 года № 678-р;
- Федеральный проект «Успех каждого ребёнка» (нацпроект «Образование»);
- Методические рекомендации по разработке и реализации раздела о воспитании в составе дополнительной общеобразовательной общеразвивающей программы (ФГБНУ «Институт изучения детства, семьи и воспитания»);
- Устав АНОО «Физтех-лицей» им. П.Л. Капицы;
- Профессиональный стандарт «Педагог дополнительного образования детей и взрослых» (приказ Минтруда РФ от 22.09.2021 № 652н).

1. Раздел 1. Комплекс основных характеристик образования

1.1. Пояснительная записка

Курс «Информационная безопасность» относится к естественно-научной направленности и реализуется в очной форме. Он предназначен для школьников 15–18 лет, проявляющих интерес к прикладной информатике, программированию и анализу цифровых систем.

Программа является курсом углублённого уровня и требует базовой подготовки в области алгоритмов, Python/C/C++ и операционных систем. Структура курса сочетает теоретические занятия, практикумы, проектную деятельность и командные тренировки.

Курс включает шесть содержательных модулей: основы ИБ, криптография, анализ уязвимостей, реверс-инжиниринг, правовые аспекты, подготовка к соревнованиям. Часть занятий посвящена работе над проектами, имитирующими задачи CTF и финальные этапы олимпиад.

Уровень программы: углублённый

Форма обучения: очная

Возрастная категория: 15–18 лет

Объём курса: 84 академических часа

Срок реализации: 28 учебных недель

Режим занятий: 1 занятие в неделю по 3 академических часа

Входной контроль: рекомендуется (по языкам программирования и основам ОС)

Формы занятий: лекции, практикумы, групповые проекты, тренировки

1.2. Цель и задачи

Цель курса:

Формирование у обучающихся системного понимания принципов информационной безопасности, развитие практических навыков в области защиты информации, а также подготовка к олимпиадным и командным соревнованиям по кибербезопасности.

Задачи курса:

Предметные:

- изучение ключевых понятий, моделей и методов информационной безопасности;
- освоение основ симметричной и асимметричной криптографии;
- развитие навыков анализа уязвимостей и построения эксплойтов;
- применение реверс-инжиниринга для анализа поведения программ;
- понимание архитектуры CTF-задач и стратегий решения.

Метапредметные:

- развитие аналитического и логического мышления;
- формирование исследовательской позиции и навыков работы с документацией;
- освоение принципов командной работы и проектной деятельности.

Личностные:

- формирование ответственного отношения к вопросам ИБ;

- развитие понимания этических и правовых аспектов цифровой деятельности;
- повышение интереса к исследовательской и инженерной профессии в сфере ИТ.

1.3. Содержание курса

Раздел 1. Введение в информационную безопасность

- Понятие и цели ИБ
- Классификация угроз и нарушителей
- Модели защиты: Bell-LaPadula, Biba, Clark-Wilson

Раздел 2. Основы криптографии

- Исторические шифры, частотный анализ
- Блочные и поточные шифры
- RSA, DH, эллиптические кривые
- Хэш-функции и цифровые подписи

Раздел 3. Анализ уязвимостей

- Типовые уязвимости: BOF, Use-After-Free, race condition
- Инструменты поиска: Ghidra, gdb, ASAN
- Основы безопасного программирования

Раздел 4. Реверс-инжиниринг

- Архитектура исполняемых файлов (ELF, PE)
- Дизассемблирование и декомпиляция
- Работа с IDA Pro, Radare2
- Практика анализа вредоносного ПО

Раздел 5. Правовые и этические аспекты

- Законодательство РФ и международное право в ИБ
- Уголовная ответственность и границы этики
- Цифровая гигиена и защита персональных данных

Раздел 6. Подготовка к CTF и олимпиадам

- Форматы задач: pwn, crypto, forensics, web
- Практикумы по решению задач прошлых лет
- Разработка собственных задач и тренировка в командах

1.4. Планируемые результаты

Предметные:

- знание моделей и архитектур защиты информации;
- умение использовать криптографические примитивы;
- способность проводить реверс-программы и анализ уязвимостей;
- базовые навыки участия в CTF-соревнованиях.

Метапредметные:

- развитие системного подхода к безопасности;
- умение работать в исследовательском режиме;
- навыки анализа, декомпозиции и сборки решений.

Личностные:

- повышение цифровой культуры;
- осознанное отношение к кибер-рискам;
- уважение к правам пользователей и авторскому праву.

2. Раздел 2. Комплекс организационно-педагогических условий

2.1. Календарный учебный график

№	Месяц	Тема занятия	Кол-во часов	Форма занятия	Место проведения	Форма контроля
1	Октябрь	Понятие и цели информационной безопасности	3	Лекция + практикум	Кабинет информатики	Решение задач, участие в проектах
2	Октябрь	Классификация угроз, модели нарушителей	3	Лекция + практикум	Кабинет информатики	Решение задач, участие в проектах
3	Октябрь	Модели безопасности: Bell-LaPadula, Biba, Clark-Wilson	3	Лекция + практикум	Кабинет информатики	Решение задач, участие в проектах
4	Октябрь	Исторические шифры, основы криптоанализа	3	Лекция + практикум	Кабинет информатики	Решение задач, участие в проектах
5	Ноябрь	Симметричные шифры: блочные и поточные	3	Лекция + практикум	Кабинет информатики	Решение задач, участие в проектах
6	Ноябрь	Асимметричная криптография: RSA, Diffie–Hellman	3	Лекция + практикум	Кабинет информатики	Решение задач, участие в проектах

7	Ноябрь	Хэш-функции и цифровые подписи	3	Лекция + практикум	Кабинет информатики	Решение задач, участие в проектах
8	Ноябрь	Основы безопасного программирования	3	Лекция + практикум	Кабинет информатики	Решение задач, участие в проектах
9	Декабрь	Типовые уязвимости: BOF, UAF, race condition	3	Лекция + практикум	Кабинет информатики	Решение задач, участие в проектах
10	Декабрь	Инструменты анализа: gdb, ASAN, Valgrind	3	Лекция + практикум	Кабинет информатики	Решение задач, участие в проектах
11	Декабрь	Форматы исполняемых файлов: ELF и PE	3	Лекция + практикум	Кабинет информатики	Решение задач, участие в проектах
12	Декабрь	Дизассемблирование и декомпиляция	3	Лекция + практикум	Кабинет информатики	Решение задач, участие в проектах
13	Январь	Работа с IDA Pro и Ghidra	3	Лекция + практикум	Кабинет информатики	Решение задач, участие в проектах
14	Январь	Основы анализа вредоносного ПО	3	Лекция + практикум	Кабинет информатики	Решение задач, участие в проектах
15	Январь	Правовые основы ИБ в РФ	3	Лекция + практикум	Кабинет информатики	Решение задач, участие в проектах
16	Январь	Международное право и цифровые права	3	Лекция + практикум	Кабинет информатики	Решение задач, участие в проектах
17	Февраль	Этика и уголовная ответственность в ИБ	3	Лекция + практикум	Кабинет информатики	Решение задач, участие в проектах
18	Февраль	Введение в CTF: форматы и категории задач	3	Лекция + практикум	Кабинет информатики	Решение задач, участие в проектах
19	Февраль	Crypto и Reverse задачи на олимпиадах	3	Лекция + практикум	Кабинет информатики	Решение задач, участие в проектах
20	Февраль	Web и Forensics задачи: основы анализа	3	Лекция + практикум	Кабинет информатики	Решение задач, участие в проектах
21	Март	Pwn-задачи: переполнение и shellcode	3	Лекция + практикум	Кабинет информатики	Решение задач, участие в проектах
22	Март	Практикум: решение задач с CTFtime	3	Лекция + практикум	Кабинет информатики	Решение задач, участие в проектах

23	Март	Разработка собственных задач	3	Лекция + практикум	Кабинет информатики	Решение задач, участие в проектах
24	Март	Проект: имитация командного CTF	3	Лекция + практикум	Кабинет информатики	Решение задач, участие в проектах
25	Апрель	Подготовка к олимпиаде по ИБ	3	Лекция + практикум	Кабинет информатики	Решение задач, участие в проектах
26	Апрель	Защита проектов и задач	3	Лекция + практикум	Кабинет информатики	Решение задач, участие в проектах
27	Апрель	Обсуждение результатов и анализа атак	3	Лекция + практикум	Кабинет информатики	Решение задач, участие в проектах
28	Апрель	Обобщение и закрытие курса	3	Лекция + практикум	Кабинет информатики	Решение задач, участие в проектах

2.2. Условия реализации курса

Материально-технические условия:

- специализированный кабинет или лаборатория с индивидуальными рабочими местами (ПК с ОС Linux/Windows, доступом в интернет);
- наличие ПО: IDA Pro, Ghidra, Radare2, Python, GDB, Burp Suite, Wireshark, инструментов CTF (например, pwntools, angr);
- использование онлайн-платформ для CTF/тренировок (например, pwnable.kr, root-me.org, CTFtime.org).

Кадровое обеспечение:

- курс ведёт педагог, обладающий опытом в области кибербезопасности, подготовке CTF-команд, знанием языка низкоуровневого программирования (например, C) и инструментов анализа уязвимостей;
- педагог должен владеть как теоретическим материалом (криптография, модели угроз), так и практическими инструментами реверса и эксплуатации.

Методическое обеспечение:

- учебный план и календарный график;
- тематические листы с задачами (с разбалловкой и уровнями сложности);
- авторские и открытые задачи CTF (pwn, crypto, reversing, web, forensic);
- законодательные и нормативные акты, регулирующие сферу ИБ.

2.3. Формы аттестации

Текущий контроль:

- выполнение лабораторных заданий по каждому тематическому блоку;

- участие в мини-контестах и практических сессиях по задачам CTF-формата;
- командная разработка собственных задач и их защита.

Итоговая аттестация:

- проект (видеопрезентация, writeup и защита) по одному из направлений: crypto, reverse, pwn, forensic;
- защита — индивидуальная или командная;
- письменный мини-экзамен по ключевым темам (модели, криптография, право, уязвимости).

2.4. Оценочные материалы

- лабораторные задания с разбалловкой;
- карточки анализа задач (вход, выход, эксплойт, writeup);
- шаблоны writeup и презентаций проекта;
- чек-листы защиты проекта;
- контрольные вопросы по праву и криптографии;
- инструменты самопроверки и рефлексии (письменные и устные форматы).

2.5. Методические материалы

Для преподавателя:

- структура занятий по модулям;
- сборники актуальных CTF-задач и writeup'ов;
- ссылки на открытые тренажёры и песочницы;
- чек-листы подготовки к олимпиадам и локальным турнирам.

Для обучающихся:

- подборка статей по криптографии и реверсу;
- шпаргалки по основным форматам задач CTF;
- видеоразборы и инструкции по работе с анализаторами (IDA, Ghidra, Burp);
- правовые памятки: что можно и что нельзя в тестировании на проникновение.

2.6. Раздел воспитания

Курс формирует ответственное, этичное и осознанное отношение к вопросам информационной безопасности. Учащиеся осваивают не только методы защиты и атаки, но и границы правомерного применения знаний в рамках законодательства и профессиональной этики.

Формы реализации:

- тематические дискуссии об этике в ИБ;
- сравнение white hat, grey hat и black hat моделей;
- кейсы и реальные истории (анализ инцидентов с юридическим последствием);
- совместная работа над проектами, формирующая доверие, уважение и культуру командной деятельности.

2.7. Список литературы

1. Касперски Е. «Основы информационной безопасности». — М.: Эксмо, 2020.
2. Гутман М. «Взлом и защита: введение в CTF». — СПб.: Питер, 2022.
3. Tanenbaum A., Bos H. «Современные операционные системы». — М.: Питер, 2023.
4. Ferguson N., Schneier B. «Практическая криптография». — М.: Вильямс, 2021.
5. Документация Ghidra, IDA Pro, Radare2 (официальные сайты).
6. Сайты open-source тренажёров: ctftime.org, picoCTF.org, [Hack The Box](https://hackthebox.org).
7. Закон РФ «О персональных данных» № 152-ФЗ; УК РФ, ст. 272–274.
8. Авторские методические материалы преподавателя.