

**ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ НЕТИПОВОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ
«АКАДЕМИЯ ТАЛАНТОВ» САНКТ-ПЕТЕРБУРГА**

РАССМОТРЕНА

на заседании
Экспертного совета
ГБНОУ «Академия талантов»
от «28»_декабря_2022 г.
Протокол № 2/ЭС

ПРИНЯТА

на заседании
Педагогического совета
ГБНОУ «Академия талантов»
от «29»_августа_2023 г.
Протокол № 4/23

УТВЕРЖДЕНА

приказом директора
ГБНОУ «Академия талантов»
от «30»_августа_2023 г.
№ 30081

_____ И.В. Пильдес

РАССМОТРЕНА

на заседании
Методического объединения
ГБНОУ «Академия талантов»
от «25»_августа_2023 г.
Протокол № 2/23

**ДОПОЛНИТЕЛЬНАЯ
ОБЩЕРАЗВИВАЮЩАЯ ПРОГРАММА**

– «Профильная смена» (в формате интенсивной профильной образовательной программы)

«Зимний интенсив по информационной безопасности»

Срок освоения – 12 дней

Объем освоения - 36 часов

Возраст обучающихся – 15-17 лет

Разработчик:

Менщиков Александр Алексеевич,
кандидат технических наук,
доцент факультета безопасности информационных
технологий ИТМО

Санкт-Петербург
2024

ПОЯСНИТЕЛЬНАЯ ЗАПИСКА

Дополнительная общеразвивающая программа «Зимний интенсив по информационной безопасности» разработана для подготовки обучающихся к участию в городской и всероссийской олимпиадах школьников по технологии, профиль «Информационная безопасность». Поскольку задания, предлагаемые на указанных олимпиадах, выходят за рамки школьных знаний, характеризуются письменными заданиями, успешность выступления обучающихся на олимпиадах по технологии, профиль «Информационная безопасность» во многом зависит от наличия этих знаний. Данная Программа ориентирована на компенсацию пробелов знаний обучающихся в тех аспектах, которые регулярно затрагиваются в олимпиадных заданиях. В составлении данной программы разработчики опирались на банк данных олимпиадных заданий по технологии, профиль «Информационная безопасность» за последние два года.

Направленность программы: техническая, так как направлена на развитие интереса обучающихся к инженерно-техническим и информационным технологиям.

Актуальность программы

Всероссийская олимпиада школьников – наиболее востребованная школьная олимпиада РФ, единственная олимпиада, имеющая преимущество перед ЕГЭ в порядке поступления в высшие учебные заведения. Программа удовлетворяет социальный спрос на приобретение знаний и умений, адекватных современному уровню технологий в области прикладной информационной безопасности, а также соответствует государственной политике в сфере развития образования и науки в эпоху цифровой экономики.

Программа актуальна тем, что позволяет реализовать желание мотивированных и способных участников освоить основные тематики практической части профиля «Информационная безопасность» и основные методы решения практических задач олимпиадного уровня в данном направлении.

Адресат программы

Программа ориентирована на обучающихся 9-11 классов, проявивших интерес к интенсивной олимпиадной подготовке, ставших победителями и призерами районного этапа ВсОШ по технологии, профиль «Информационная безопасность», в Санкт-Петербурге в 2022/2023 учебном году, а также обучающихся, успешно прошедших отбор на профильную образовательную программу в соответствии с внутренними правилами Академии Талантов, ориентированных на участие в региональном этапе ВсОШ по технологии, профиль «Информационная безопасность».

Программа имеет **углубленный уровень освоения** материала.

Объем и сроки освоения программы

Программа «Зимний интенсив по информационной безопасности» рассчитана на 36 часов обучения в интенсивном формате (12 дней реализации).

Режим занятий

12 дней по 3 академических часа согласно расписанию (см. Приложение 1).

Отличительные особенности

Особенностью программы является практикоориентированный характер. Предварительно, при составлении Программы, были выделены направления подготовки/разделы STF, указанные в документе «Требования к организации и проведению регионального этапа Всероссийской олимпиады школьников в 2023/2024 учебном году».

CTF или Capture The Flag – распространенный по всему миру тип соревнований по кибербезопасности. Он имеет несколько форматов, один из которых, Jeopardy или Task-Based (решение задач), частично представлен в практической части регионального этапа всероссийской олимпиады школьников по технологии, профиль «Информационная безопасность».

Общая схема Программы выглядит следующим образом:

1. По каждому разделу формируется необходимый базовый теоретический минимум, требующийся для выполнения задач по формату.
2. В соответствии с теоретической базой формируется банк практических задач, соответствующий формату ВсОШ и CTF, в частности.
3. Дополнительно, перед завершением интенсива, преподаватель вместе с участниками разбирает задания регионального этапа ВсОШ прошлых лет, которые находятся в открытом доступе.
4. Финальным занятием преподаватель предлагает слушателям самим, на основании усвоения материала и возникновения пробелов, определить тему завершающего дня интенсива. Занятие предполагается проводить в формате диалога с предварительно подготовленными преподавателем задачами и материалами за день до финального дня интенсива.

Цели и задачи программы

Целью реализации Программы является развитие и поддержка талантливых обучающихся, проявляющих интерес и способности к прикладной, информационно-технической деятельности в области информационной безопасности, путем подготовки к практической части регионального этапа Всероссийской олимпиады школьников по технологии, профиль «Информационная безопасность».

Для достижения поставленной цели при реализации Программы решаются следующие **задачи**:

Обучающие:

- обучить методам решения практических задач ВсОШ по технологии профиля «Информационная безопасность»;
- сформировать навыки, необходимые для выполнения практических заданий профиля «Информационная безопасность»;
- сформировать умения и навыки, необходимые для участия в актуальных соревнованиях по прикладной информационной безопасности.

Развивающие:

- развить способности к самостоятельному приобретению знаний и решению проблем, возникающих в ходе работы над решением практических заданий профиля «Информационная безопасность»;
- развить устойчивую мотивацию к информационно-технической деятельности и профессиональному самоопределению в сфере, связанной с прикладной информационной безопасностью;
- развить терпение, настойчивость и находчивость в процессе решения задач в условиях неопределенности и нехватки информации.

Воспитательные:

- воспитать уважительное отношение к научному знанию;

Планируемые результаты

Личностные результаты

- развита устойчивая мотивация к информационно-технической деятельности и профессиональному самоопределению в сфере, связанной с прикладной информационной безопасностью;
- развиты терпение, настойчивость и находчивость в процессе решения задач в условиях неопределенности и нехватки информации.
- воспитано уважительное отношение к научному знанию;

Метапредметные результаты

- развиты способности к самостоятельному приобретению знаний и решению проблем, возникающих в ходе работы над решением практических заданий профиля «Информационная безопасность»;

Предметные результаты

- обучены методам решения практических задач ВСОШ по технологии профиля «Информационная безопасность»;
- сформированы навыки, необходимые для выполнения практических заданий профиля «Информационная безопасность»;
- сформированы умения и навыки, необходимые для участия в актуальных соревнованиях по прикладной информационной безопасности.

Организационно-педагогические условия реализации

Язык реализации: русский

Форма обучения: очная

Особенности реализации

Условия набора: к участию в профильной смене допускаются обучающиеся образовательных организаций Санкт-Петербурга, кандидаты в сборную команду Санкт-Петербурга для участия в региональном этапе всероссийской олимпиады школьников по технологии, профиль «Информационная безопасность», показавшие высокие результаты во ВСОШ, заявившие в добровольном порядке свое намерение участвовать в мероприятиях смены в срок, установленный Региональным центром выявления и поддержки одаренных детей Санкт-Петербурга, и прошедшие предварительный отбор по критериям и условиям, установленным в Положении о порядке организации обучения по дополнительным образовательным программам – «Профильные смены» (в формате интенсивной профильной образовательной программы) в Региональном центре выявления и поддержки одаренных детей в области искусства, спорта, образования и науки Государственного бюджетного нетипового образовательного учреждения «Академия талантов» Санкт-Петербурга. Отбор на смену осуществляется на основе рейтинга, выстроенного по сумме баллов и за достижения на предыдущих этапах ВСОШ по технологии, профиль «Информационные технологии».

Условия формирования групп

В Программе одновременно принимают участие 30 обучающихся (1 разновозрастная группа обучающихся 9-11 классов).

Формы организации и проведения занятий: занятия проводятся для всей группы обучающихся по аудиториям в традиционной форме.

Формы организации деятельности учащихся на занятии

- фронтальная: работа педагога с группой обучающихся (лекции),
- работа педагога с малыми группами обучающихся (решение задач и выполнение тренировочных упражнений),
- индивидуальная работа с обучающимися.

Материально-техническое оснащение программы

1. Учебное пространство: помещения для проведения занятий вместимостью до 30 человек.
 2. Оборудование: ноутбуки с доступом к сети Интернет, установленным на них необходимым ПО, проектор, презентер;
 3. Раздаточный материал: бумага А4, шариковые ручки, цветные карандаши, фломастеры, цветные маркеры для досок, бейджи (35 шт.), папка-планшет (34 шт.).
 4. Кадровое обеспечение: педагоги-организаторы, тьюторы, специалисты IT-отдела, педагоги:
- Меншиков Александр Алексеевич, кандидат технических наук, доцент факультета безопасности информационных технологий ИТМО;

Учебный план (36 часов)

№ п/п	Название раздела, темы	Количество часов			Формы контроля/аттестации
		Всего	Теория	Практика	
1.	Тема 1. Знакомство с инфраструктурой и форматами заданий (Jeopardy). Освоение программ семейства Linux	3	2	1	Педагогическое наблюдение, семинарское обсуждение, решение задач, выполнение тренировочных упражнений
2.	Тема 2. Освоение программ, необходимых для выполнения заданий по анализу сетевого трафика (Wireshark, netcat, python)	7	4	3	
3.	Тема 3. Освоение программ, необходимых для поиска уязвимостей web-приложений (BurpSuite)	5	2	3	
4.	Тема 4. Освоение программ, необходимых для поиска следов инцидентов информационной безопасности (ftk imager/mount, grep, strings, Hex-редактор, Volatility)	6	4	2	
5.	Тема 5. Освоение программ, необходимых для анализа исходных текстов компьютерных программ (gdb, gcc, IDE для C)	6	4	2	
6.	Тема 6. Инфраструктура открытых ключей (PKI). Цифровые сертификаты	3	2	1	

7.	Тема 7. Структура практической части регионального этапа ВСОШ по технологии, профиль «Информационная безопасность»	3	1	2	
8.	Тема 8. Дополнительное экспертное занятие с тематиками по выбору слушателей	3	1	2	
	Всего:	36	20	16	

УТВЕРЖДЕНА
приказом директора
ГБНОУ «Академия талантов»
от «30» августа 2023 г.
№ 30081

_____ И.В. Пильдес

**РАБОЧАЯ ПРОГРАММА
ДОПОЛНИТЕЛЬНОЙ ОБЩЕРАЗВИВАЮЩЕЙ ПРОГРАММЫ
«Зимний интенсив по информационной безопасности»**

Цели и задачи программы

Целью реализации Программы является развитие и поддержка талантливых обучающихся, проявляющих интерес и способности к прикладной, информационно-технической деятельности в области информационной безопасности, путем подготовки к практической части регионального этапа Всероссийской олимпиады школьников по технологии, профиль «Информационная безопасность».

Для достижения поставленной цели при реализации Программы решаются следующие **задачи**:

Обучающие:

- обучить методам решения практических задач ВсОШ по технологии профиля «Информационная безопасность»;
- сформировать навыки, необходимые для выполнения практических заданий профиля «Информационная безопасность»;
- сформировать умения и навыки, необходимые для участия в актуальных соревнованиях по прикладной информационной безопасности.

Развивающие:

- развить способности к самостоятельному приобретению знаний и решению проблем, возникающих в ходе работы над решением практических заданий профиля «Информационная безопасность»;
- развить устойчивую мотивацию к информационно-технической деятельности и профессиональному самоопределению в сфере, связанной с прикладной информационной безопасностью;
- развить терпение, настойчивость и находчивость в процессе решения задач в условиях неопределенности и нехватки информации.

Воспитательные:

- воспитать уважительное отношение к научному знанию;

Планируемые результаты

Личностные результаты

- развита устойчивая мотивация к информационно-технической деятельности и профессиональному самоопределению в сфере, связанной с прикладной информационной безопасностью;

- развиты терпение, настойчивость и находчивость в процессе решения задач в условиях неопределенности и нехватки информации.
- воспитано уважительное отношение к научному знанию;

Метапредметные результаты

- развиты способности к самостоятельному приобретению знаний и решению проблем, возникающих в ходе работы над решением практических заданий профиля «Информационная безопасность»;

Предметные результаты

- обучены методам решения практических задач ВСОШ по технологии профиля «Информационная безопасность»;
- сформированы навыки, необходимые для выполнения практических заданий профиля «Информационная безопасность»;
- сформированы умения и навыки, необходимые для участия в актуальных соревнованиях по прикладной информационной безопасности.

Содержание обучения

Программа содержит следующие тематические разделы:

Тема 1. Знакомство с инфраструктурой и форматами заданий (Jeopardy). Освоение программ семейства Linux.

Теория. Знакомство с инфраструктурой и форматами заданий (Jeopardy). Освоение программ, необходимых для выполнения заданий по администрированию операционных систем семейства Linux. Раздел CTF – Admin. Введение в администрирование операционных систем семейства Linux.

Практика. Выполнение тренировочных упражнений по администрированию операционных систем семейства Linux в формате Jeopardy.

Форма контроля: педагогическое наблюдение, семинарское обсуждение, решение задач, выполнение тренировочных упражнений.

Тема 2. Освоение программ, необходимых для выполнения заданий по анализу сетевого трафика (Wireshark, netcat, python).

Теория. Освоение программ, необходимых для выполнения заданий по анализу сетевого трафика (Wireshark, netcat, python). Раздел CTF – Network. Введение в анализ сетевого трафика. Модель OSI. Основы сетевого взаимодействия. Дополнительные главы анализа сетевого трафика. Протоколы. Типовые уязвимости на разных уровнях модели OSI. Клиент-серверное взаимодействие.

Практика. Выполнение простых и комплексных тренировочных упражнений по анализу сетевого трафика в формате Jeopardy.

Форма контроля: педагогическое наблюдение, семинарское обсуждение, решение задач, выполнение тренировочных упражнений.

Тема 3. Освоение программ, необходимых для поиска уязвимостей web-приложений (BurpSuite).

Теория. Освоение программ, необходимых для поиска уязвимостей web-приложений (BurpSuite). Раздел CTF – Web. Устройство и механизм работы веб-приложений. Типы HTTP-запросов. Типовые уязвимости веб-приложений. Инъекции. CSRF. XSS.

Практика. Выполнение простых и комплексных тренировочных упражнений по поиску уязвимостей web-приложений в формате Jeopardy.

Форма контроля: педагогическое наблюдение, семинарское обсуждение, решение задач, выполнение тренировочных упражнений.

Тема 4. Освоение программ, необходимых для поиска следов инцидентов информационной безопасности (ftk imager/mount, grep, strings, Hex-редактор, Volatility).

Теория. Освоение программ, необходимых для поиска следов инцидентов информационной безопасности (ftk imager/mount, grep, strings, Hex-редактор, Volatility). Раздел CTF – Forensics. Введение в поиск следов инцидентов информационной безопасности. Представления файлов в шестнадцатеричной системе. Заголовки. Дополнительные главы поиска следов инцидентов информационной безопасности. Файловые системы. Дампы файловой системы. Оперативная память и процессы. Дампы оперативной памяти и процессов.

Практика. Выполнение простых и комплексных тренировочных упражнений по поиску следов инцидентов информационной безопасности в формате Jeopardy.

Форма контроля: педагогическое наблюдение, семинарское обсуждение, решение задач, выполнение тренировочных упражнений.

Тема 5. Освоение программ, необходимых для анализа исходных текстов компьютерных программ (gdb, gcc, IDE для C).

Теория. Освоение программ, необходимых для анализа исходных текстов компьютерных программ (gdb, gcc, IDE для C). Разделы CTF – Reverse и PWN. Введение в анализ исходных текстов компьютерных программ. Язык C. Методы анализа кода. Дополнительные главы анализа исходных текстов компьютерных программ. Сегменты, структуры данных, адресное пространство. Переполнение буфера. IDA. Уязвимости стандартных библиотек C.

Практика. Выполнение простых и комплексных тренировочных упражнений по анализу исходных текстов компьютерных программ в формате Jeopardy.

Форма контроля: педагогическое наблюдение, семинарское обсуждение, решение задач, выполнение тренировочных упражнений.

Тема 6. Инфраструктура открытых ключей (PKI). Цифровые сертификаты.

Теория. Инфраструктура открытых ключей (PKI). Цифровые сертификаты. OpenSSL. Защищенные соединения.

Практика. Создание цепочки сертификатов. Создание инфраструктуры открытых ключей.

Форма контроля: педагогическое наблюдение, семинарское обсуждение, решение задач, выполнение тренировочных упражнений.

Тема 7. Структура практической части регионального этапа ВСОШ по технологии, профиль «Информационная безопасность».

Теория. Структура практической части регионального этапа ВСОШ по технологии (профиль – информационная безопасность).

Практика. Разбор задач регионального этапа 2022/2023 года. Совместное решение задач регионального этапа 2022/2023 года. Решение дополнительных задач. Выбор тем и задач для последнего дня интенсива слушателями.

Форма контроля: педагогическое наблюдение, семинарское обсуждение, решение задач, выполнение тренировочных упражнений.

Тема 8. Дополнительное экспертное занятие с тематиками по выбору слушателей.

Теория. Дополнительное экспертное занятие с тематиками по выбору слушателей.

Практика. Выполнение дополнительных заданий по выбранным темам.

Форма контроля: педагогическое наблюдение, семинарское обсуждение, решение задач, выполнение тренировочных упражнений.

Оценка реализации программы и образовательные результаты

По итогам реализации Программы предусмотрено проведение анализа выполнения заданий обучающимися с последующей экспертной оценкой. Образовательный результат оценивается

через применение обучающимися полученных знаний, умений, навыков на практике, рефлексию и экспертную оценку педагогов смены. В дальнейшем отслеживается результативность образовательного процесса по итогам участия во ВсОШ по технологии, профиль «Информационная безопасность».

Методическое обеспечение программы

№ п/п	Раздел/тема	Форма деятельности обучающихся	Приемы и методы	Дидактический материал	Формы контроля/аттестации
1.	Тема 1. Знакомство с инфраструктурой и форматами заданий (Jeopardy). Освоение программ семейства Linux	Усвоение нового материала, решение задач, выполнение тренировочных упражнений	Приемы: объяснительно-иллюстративный, репродуктивный, исследовательский, самооценка. Эмоциональные методы: поощрение, создание ситуации успеха.	Учебная литература, фото-, аудио- и видеоматериалы, цифровые материалы, интернет-источники.	Педагогическое наблюдение, семинарское обсуждение, решение задач, выполнение тренировочных упражнений
2.	Тема 2. Освоение программ, необходимых для выполнения заданий по анализу сетевого трафика (Wireshark, netcat, python)		Познавательные: слушание, получение новых знаний, систематизация знаний, учебные дискуссии.		
3.	Тема 3. Освоение программ, необходимых для поиска уязвимостей web-приложений (BurpSuite)		Социальные методы: создание ситуации взаимопомощи, обмен мнениями, работа в команде.		
4.	Тема 4. Освоение программ, необходимых для поиска следов инцидентов информационно		Практические: разбор нового материала, самостоятельная работа над проектами,		

	й безопасности (ftk imager/mount, grep, strings, Hex-редактор, Volatility)		задачами и тренировочными упражнениями, дискуссия		
5.	Тема 5. Освоение программ, необходимых для анализа исходных текстов компьютерных программ (gdb, gcc, IDE для C)				
6.	Тема 6. Инфраструктура открытых ключей (PKI). Цифровые сертификаты				
7.	Тема 7. Структура практической части регионального этапа ВСОШ по технологии, профиль «Информационная безопасность»				
8.	Тема 8. Дополнительное экспертное занятие с тематиками по выбору слушателей				

Мониторинг реализации программы:

Методы проверки, оценки знаний и исполнительских навыков:

Проверка и оценка знаний и навыков учащихся являются неотъемлемой и важной составляющей частью процесса обучения, они строятся на принципах систематичности и проводятся в течение всего процесса обучения.

В ходе реализации программы используются входной, текущий, итоговый контроль.

Входной контроль – рейтинг, выстроенный по сумме баллов за достижения на предыдущих этапах ВсОШ по технологии, профиль «Информационная безопасность».

Текущий контроль - проводится в течение всего процесса обучения в форме педагогического наблюдения, опроса обучающихся.

Итоговый контроль проводится в конце обучения по программе в форме анализа решения обучающимися задач и выполнения тренировочных упражнений.

Итоговое оценивание осуществляется педагогом в отношении каждого обучающегося, результаты фиксируются в «Диагностической карте оценки результатов».

Критерии оценки освоения программы (итоговое оценивание)

№	Критерий оценивания	Мнение педагога
1.	развита устойчивая мотивация к информационно-технической деятельности и профессиональному самоопределению в сфере, связанной с прикладной информационной безопасностью	1 2 3 4 5
2.	развиты терпение, настойчивость и находчивость в процессе решения задач в условиях неопределенности и нехватки информации	1 2 3 4 5
3.	уважительное отношение к научному знанию	1 2 3 4 5
4.	обучены методам решения практических задач ВсОШ по технологии профиля «Информационная безопасность»	1 2 3 4 5
5.	сформированы навыки, необходимые для выполнения практических заданий профиля «Информационная безопасность»	1 2 3 4 5
6.	сформированы умения и навыки, необходимые для участия в актуальных соревнованиях по прикладной информационной безопасности	1 2 3 4 5
7.	развиты способности к самостоятельному приобретению знаний и решению проблем, возникающих в ходе работы над решением практических заданий профиля «Информационная безопасность»	1 2 3 4 5

Уровни усвоения программы:

28 – 35 баллов. Высокий уровень. Уверенное знание теоретического материала и умения применить его на практике.

15-27 баллов. Средний уровень освоения программы.

7-14 баллов. Низкий уровень. Программа не усвоена в полном объеме.

Диагностическая карта оценки результатов

№	ФИ обучающегося	Критерии оценки						Средний балл
		развиты терпение, настойчивость и находчивость в процессе решения задач в условиях неопределенности и нехватки информации	обучены методам решения практических задач ВСОШ по технологии профиля «Информационная безопасность»	сформированы навыки, необходимые для выполнения практических заданий профиля «Информационная безопасность»	уважительное отношение к научному знанию	развита устойчивая мотивация к информационно-технической деятельности и профессиональному самоопределению в сфере, связанной с прикладной информационной безопасностью	сформированы умения и навыки, необходимые для участия в актуальных соревнованиях по прикладной информационной безопасности	
1.								
2.								
3.								
4.								
...								

Педагог подсчитывает баллы каждого обучающегося и группы в целом, делая вывод о прохождении обучающимися программы.

Информационные источники

Литература для педагогов

1. Педагогика. Учебник для ВУЗов. Стандарт третьего поколения / Под ред. П. Тряпицкой. - СПб.: Питер, 2018. - 304 с.
2. Гуслова, М.Н. Инновационные педагогические технологии: Учебник / М.Н. Гуслова. - М.: Academia, 2018. - 672 с.
3. Родичев Ю.А. Информационная безопасность. Национальные стандарты Российской Федерации. Учебное пособие. Изд.: Питер, 2023. – 384 с.
4. Гумбинская М.В., Петровский М.В. Комплексное обеспечение информационной безопасности на предприятии. Учебник. Изд.: Лань, 2022. – 344 с.
5. Шаньгин В.Ф. Информационная безопасность и защита информации. Изд.: ДМК-Пресс, 2017. – 702 с.
6. Бирюков А.А. Информационная безопасность. Защита и нападение. Изд. ДМК-Пресс, 2017. – 434 с.

Литература для обучающихся

1. Гумбинская М.В., Петровский М.В. Комплексное обеспечение информационной безопасности на предприятии. Учебник. Изд.: Лань, 2022. – 344 с.
2. Нестеров С.А. Основы информационной безопасности. Учебник для СПО. Изд.: Лань, 2022. – 324 с.
3. Шаньгин В.Ф. Информационная безопасность и защита информации. Изд.: ДМК-Пресс, 2017. – 702 с.

Интернет ресурсы

1. <https://pirit.biz/resheniya/informacionnaja-bezopasnost> Информационная безопасность;
2. <https://searchinform.ru/informatsionnaya-bezopasnost/> Информационная безопасность;

Программа составлена в соответствии с нормативно-правовой базой:

- Федеральный закон от 29.12.2012 № 273-ФЗ «Об образовании в Российской Федерации»;
- Федеральный закон от 31.07.2020 № 304-ФЗ «Об изменении федерального закона «Об образовании в Российской Федерации» по вопросам воспитания обучающихся»;
- Указ Президента Российской Федерации от 25.04.2022 № 231 «Об объявлении в Российской Федерации Десятилетия науки и технологий»;
- Постановление Правительства РФ от 26.12.2017 N 1642 (ред. от 11.04.2022) «Об утверждении государственной программы Российской Федерации «Развитие образования»;
- Распоряжение Правительства РФ от 31 марта 2022 г. N 678-р «Об утверждении Концепции развития дополнительного образования детей до 2030 г. и плана мероприятий по ее реализации»;
- Приказ Министерства Просвещения Российской Федерации от 03 сентября 2019 года №467 «Об утверждении Целевой модели развития региональных систем дополнительного образования детей»;
- Приказ Министерства просвещения РФ от 27 июля 2022 г. N 629 «Об утверждении Порядка организации и осуществления образовательной деятельности по дополнительным общеобразовательным программам»;
- Распоряжение Правительства Российской Федерации от 29.05.2015 № 996-р «О стратегии развития воспитания до 2025 года»;
- Постановление Главного государственного санитарного врача Российской Федерации от 30.06.2020 № 16 «Об утверждении санитарно-эпидемиологических правил СП 3.1/2.4. 3598-20 «Санитарно-эпидемиологические требования к устройству, содержанию и организации работы образовательных организаций и других объектов социальной инфраструктуры для детей и молодежи в условиях распространения новой коронавирусной инфекции (COVID-19)»;
- Постановление Правительства Санкт-Петербурга от 13 марта 2020 года № 121 «О мерах по противодействию распространению в Санкт-Петербурге новой коронавирусной инфекции (COVID-19)» (с изменениями на 24 марта 2022 года);
- Стандарт безопасной деятельности образовательной организации, реализующей дополнительные общеобразовательные, общеразвивающие программы, в том числе санитарно-гигиенические безопасности в целях противодействия распространения в Санкт-Петербурге новой коронавирусной инфекции (COVID-19) для учреждений дополнительного образования, находящихся в ведении Комитета по образованию и администраций районов Санкт-Петербурга за исключением образовательных организаций, реализующих образовательные программы основного образования;
- Постановления Главного государственного врача Российской Федерации от 28.01.2021 №2 «Об утверждении санитарных правил и норм СанПин 1.2.36.85-21 «Гигиенические нормативы и требования к обеспечению безопасности и (или) безвредности для человека факторов среды обитания»;
- Постановления Главного государственного врача Российской Федерации от 28.09.2020 № 28 «Об утверждении правил СП 2.4.3648-20 «Санитарно-эпидемиологические требования к организации воспитания и обучения, отдыха и оздоровления детей и молодежи»;
- Устава государственного бюджетного нетипового образовательного учреждения «Академия талантов» Санкт-Петербурга; лицензией ГБНОУ «Академия талантов» на образовательную деятельность; Положения о порядке организации обучения по дополнительным образовательным программам – «Профильные смены» (в формате интенсивной профильной образовательной программы) в Региональном центре выявления и поддержки одаренных детей в области искусства, спорта, образования и науки Государственного бюджетного нетипового образовательного учреждения «Академия талантов» Санкт-Петербурга и другими локальными актами учреждения.

**Расписание занятий профильной смены
«Зимний интенсив по информационной безопасности»**

Время	Тема занятия	Преподаватель
5 февраля (понедельник) (Раздел - Admin)		
17:00–17:45	Знакомство с инфраструктурой и форматами заданий (Jeopardy).	Менщиков А. А.
17:55–18:40	Введение в администрирование операционных систем семейства Linux	Менщиков А. А.
18:50–19:35	Выполнение тренировочных упражнений по администрированию операционных систем семейства Linux в формате Jeopardy	Менщиков А. А.
6 февраля (вторник) (Раздел - Network)		
17:00–17:45	Введение. Освоение программ, необходимых для выполнения заданий по анализу сетевого трафика (Wireshark, netcat, python). Раздел CTF – Network	Менщиков А. А.
17:55–18:40	Введение в анализ сетевого трафика. Модель OSI. Основы сетевого взаимодействия.	Менщиков А. А.
18:50–19:35	Выполнение простых тренировочных упражнений по анализу сетевого трафика в формате Jeopardy	Менщиков А. А.
7 февраля (среда) (Раздел - Network)		
17:00–17:45	Дополнительные главы анализа сетевого трафика. Протоколы.	Менщиков А. А.
17:55–18:40	Дополнительные главы анализа сетевого трафика. Типовые уязвимости на разных уровнях модели OSI.	Менщиков А. А.
18:50–19:35	Выполнение комплексных тренировочных упражнений по анализу сетевого трафика в формате Jeopardy	Менщиков А. А.

8 февраля (четверг) (Раздел - Web)		
17:00–17:45	Введение. Освоение программ, необходимых для поиска уязвимостей web-приложений (BurpSuite). Раздел CTF - Web	Менщиков А. А.
17:55–18:40	Устройство и механизм работы веб-приложений. Типы HTTP-запросов.	Менщиков А. А.
18:50–19:35	Выполнение простых тренировочных упражнений по поиску уязвимостей web-приложений в формате Jeopardy	Менщиков А. А.
9 февраля (пятница) (Раздел - Web)		
17:00–17:45	Дополнительные главы анализа сетевого трафика. Клиент-серверное взаимодействие.	Менщиков А. А.
17:55–18:40	Типовые уязвимости веб-приложений. Инъекции. CSRF. XSS	Менщиков А. А.
18:50–19:35	Выполнение комплексных тренировочных упражнений по поиску уязвимостей web-приложений в формате Jeopardy	Менщиков А. А.
10 февраля (суббота) (Раздел - Forensics)		
10:00–10:45	Введение. Освоение программ, необходимых для поиска следов инцидентов информационной безопасности (fki imager/mount, grep, strings, Hex-редактор, Volatility). Раздел CTF – Forensics	Менщиков А. А.
11:55–12:40	Введение в поиск следов инцидентов информационной безопасности. Представления файлов в шестнадцатеричной системе. Заголовки.	Менщиков А. А.
12:50–13:35	Выполнение простых тренировочных упражнений по поиску следов инцидентов информационной безопасности в формате Jeopardy	Менщиков А. А.

Время	Тема занятия	Преподаватель
12 февраля (понедельник) (Раздел - Forensics)		
17:00–17:45	Дополнительные главы поиска следов инцидентов информационной безопасности. Файловые системы. Дампы файловой системы	Менщиков А. А.
17:55–18:40	Дополнительные главы поиска следов инцидентов информационной безопасности. Оперативная память и процессы. Дампы оперативной памяти и процессов.	Менщиков А. А.
18:50–19:35	Выполнение комплексных тренировочных упражнений по поиску следов инцидентов информационной безопасности в формате Jeopardy	Менщиков А. А.
13 февраля (вторник) (Раздел – Reverse и PWN)		
17:00–17:45	Введение. Освоение программ, необходимых для анализа исходных текстов компьютерных программ (gdb, gcc, IDE для C). Разделы CTF – Reverse и PWN	Менщиков А. А.
17:55–18:40	Введение в анализ исходных текстов компьютерных программ. Язык C. Методы анализа кода	Менщиков А. А.
18:50–19:35	Выполнение простых тренировочных упражнений по анализу исходных текстов компьютерных программ в формате Jeopardy	Менщиков А. А.
14 февраля (среда) (Раздел - Reverse и PWN)		
17:00–17:45	Дополнительные главы анализа исходных текстов компьютерных программ. Сегменты, структуры данных, адресное пространство. Переполнение буфера.	Менщиков А. А.
17:55–18:40	Дополнительные главы анализа исходных текстов компьютерных программ. IDA. Уязвимости стандартных библиотек C.	Менщиков А. А.
18:50–19:35	Выполнение комплексных тренировочных упражнений по анализу исходных текстов компьютерных программ в формате Jeopardy	Менщиков А. А.

15 февраля (четверг)		
17:00–17:45	Инфраструктура открытых ключей (PKI). Цифровые сертификаты.	Менщиков А. А.
17:55–18:40	OpenSSL. Защищенные соединения	Менщиков А. А.
18:50–19:35	Создание цепочки сертификатов. Создание инфраструктуры открытых ключей.	Менщиков А. А.
16 февраля (пятница)		
17:00–17:45	Структура практической части регионального этапа ВСОШ по технологии (профиль – информационная безопасность)	Менщиков А. А.
17:55–18:40	Разбор задач регионального этапа 2022/2023 года	Менщиков А. А.
18:50–19:35	Совместное решение задач регионального этапа 2022/2023 года. Решение дополнительных задач. Выбор тем и задач для последнего дня интенсива слушателями	Менщиков А. А.
17 февраля (суббота)		
10:00–10:45	Дополнительное экспертное занятие с тематиками по выбору слушателей. Теория и практика. Выполнение дополнительных заданий по выбранным темам	Менщиков А. А.
11:55–12:40	Дополнительное экспертное занятие с тематиками по выбору слушателей. Теория и практика. Выполнение дополнительных заданий по выбранным темам	Менщиков А. А.
12:50–13:35	Дополнительное экспертное занятие с тематиками по выбору слушателей. Теория и практика. Выполнение дополнительных заданий по выбранным темам	Менщиков А. А.