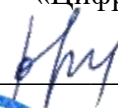


Федеральное государственное образовательное бюджетное учреждение
высшего образования
«Финансовый университет при Правительстве Российской Федерации»
(Финансовый университет)

ЦЕНТР КОМПЕТЕНЦИЙ «ЦИФРОВАЯ ЭКОНОМИКА»

УТВЕРЖДАЮ

Директор Центра компетенций
«Цифровая экономика»



Н.Ю. Сурова

«01» августа 2026 г.



ДОПОЛНИТЕЛЬНАЯ ОБЩЕОБРАЗОВАТЕЛЬНАЯ ПРОГРАММА

«Кибербезопасность. 8-9 класс (базовый уровень)»

Учебная нагрузка: 145 академических часа.

МОСКВА 2026

1. Пояснительная записка

Актуальность

Актуальность программы обусловлена стремительным ростом киберугроз – большинство подростков 8–9 классов активно пользуются цифровыми сервисами, но не имеют практических навыков защиты личных данных и распознавания угроз. Программа восполняет этот пробел, формируя у школьников навыки цифровой гигиены и безопасного программирования на Python. Кроме того, обучение служит эффективным инструментом ранней профориентации: школьники погружаются в реальные задачи ИБ-специалиста и видят, как полученные навыки соотносятся с кадровыми потребностями рынка. Информационная безопасность сегодня – одна из самых динамично развивающихся сфер, а данная программа помогает ученикам сделать первый шаг в этом направлении.

Отличительные особенности:

Обучение через призму информационной безопасности – базовый синтаксис Python осваивается в контексте реальных задач защиты информации: валидация паролей, шифрование данных, анализ логов.

Интеграция с ОГЭ – содержание включает элементы кодификатора ОГЭ по информатике, что повышает практическую значимость курса для дальнейшей аттестации.

Проектная деятельность – итогом обучения становится разработка и устная защита консольного приложения (менеджер паролей, анализатор логов или шифратор).

Новизна программы:

Искусственный интеллект как объект контроля – обучающиеся учатся проверять и исправлять код, сгенерированный нейросетями, что развивает критическое мышление и навыки отладки.

Культура кибербезопасности – с первых занятий формируется понимание триады информационной безопасности (конфиденциальность, целостность, доступность) и правовых рамок.

Связь с индустрией – в программу интегрированы кейс-задачи без единственно верного ответа, включая задачу от аккредитованной ИТ-компании, что позволяет подросткам погрузиться в реальные бизнес-контексты и актуальные проблемы отрасли.

Описание программы

Программа направлена на формирование у обучающихся базовых знаний в программировании на языке Python и понимания фундаментальных принципов информационной безопасности посредством решения прикладных практико-ориентированных задач. Программа включает в себя четыре модуля, охватывающих основные аспекты безопасной разработки, защиты данных, анализа угроз и проектной деятельности.

Формы реализации – очная без применения дистанционных образовательных технологий (в том числе, с применением средств электронного обучения).

Общий объем программы 145 академических часов.

Первый модуль посвящён основам программирования на Python в контексте информационной безопасности. Обучающиеся знакомятся с базовым синтаксисом языка, изучают переменные, условия, циклы, функции, осваивают работу с файловой системой и обработку ошибок. Все темы отрабатываются на практических задачах защиты информации: от создания валидаторов паролей и анализа URL-адресов до написания скриптов для моделирования простейших угроз. В результате обучающиеся знают базовые конструкции языка Python, умеют писать и комментировать код в соответствии с принципами читаемости, владеют навыками работы с файловой системой и пользовательским вводом, а также имеют навыки поиска и исправления ошибок в учебном коде.

Второй модуль – шифрование и защита данных. В рамках этого модуля обучающиеся изучают фундаментальные различия между кодированием, шифрованием и хешированием, осваивают применение библиотек `hashlib` и `secrets` для решения практических задач. Обучающиеся учатся вычислять хеши, генерировать криптостойкие случайные значения, знакомятся с классическими алгоритмами симметричного шифрования и принципами асимметричной криптографии. Особое внимание уделяется пониманию уместности применения каждого из методов защиты данных. В результате обучающиеся понимают разницу между кодированием, шифрованием и хешированием, знают основные виды шифрования, умеют применять библиотеки `hashlib` и `secrets` для защиты данных, а также владеют навыками проверки целостности файлов.

Третий модуль посвящён анализу угроз и цифровой гигиене. Обучающиеся знакомятся с триадой информационной безопасности – конфиденциальностью, целостностью и доступностью, изучают типичные веб-уязвимости и методы их предотвращения, осваивают принципы безопасного поведения в сети. В модуле рассматриваются основы анализа логов и выявления подозрительной активности с использованием библиотеки `socket`. Уникальной особенностью модуля является работа с ИИ-инструментами как объектом контроля: обучающиеся учатся проверять и исправлять код, сгенерированный нейросетями, что развивает критическое мышление и навыки отладки. В результате обучающиеся знают типичные веб-угрозы и правовые нормы в сфере ИБ, умеют анализировать логи и распознавать подозрительную активность, владеют навыками безопасного поведения в сети, а также понимают роль и риски ИИ-инструментов в современной разработке.

Четвёртый модуль – проектная деятельность и ранняя профориентация. В этом модуле обучающиеся применяют полученные знания для разработки и устной защиты консольного приложения: менеджера паролей, анализатора логов или шифратора. Модуль включает решение кейс-задач без единственно верного ответа, в том числе от аккредитованной ИТ-компании, что позволяет школьникам погрузиться в реальные бизнес-контексты. Содержание модуля также интегрирует элементы кодификатора ОГЭ по информатике, что повышает практическую значимость курса для дальнейшей аттестации. В результате обучающиеся получают опыт завершённой инженерной деятельности от идеи до защиты, имеют представление о роли специалиста по ИБ и форматах профессионального развития в ИТ, владеют навыками командной работы и защиты проекта, а также обладают мотивацией к дальнейшему изучению информационной безопасности.

Программа предназначена для обучающихся 8–9 классов, активно пользующихся цифровыми сервисами, но не имеющих практических навыков защиты личных данных и распознавания угроз, и желающих сделать первый шаг в востребованной сфере информационной безопасности.

Программа обеспечена учебно-методическими ресурсами для качественного освоения содержания учебного материала, что также обеспечивает результативность освоения модулей. Обучающимся обеспечен доступ к современному практико-ориентированному содержанию электронных образовательных и информационных ресурсов. Предусмотрены материально-технические условия – программное обеспечение и оборудование.

Преподавательский состав включает ИТ-специалистов, имеющих большой педагогический стаж в области преподавания языков программирования и обеспечения информационной безопасности.

Аннотация

«Кибербезопасность. 8-9 класс (базовый уровень)» – дополнительная общеобразовательная программа технической направленности, ориентированная на изучение программирования и фундаментальных принципов кибербезопасности. Программа рассчитана на базовый уровень сложности.

Дополнительная общеобразовательная программа предусматривает поэтапное освоение языка Python и ключевых концепций защиты информации.

Программа направлена на формирование базового понимания принципов информационной безопасности, освоение основных конструкций языка Python применительно к задачам защиты данных, получение первоначальных навыков шифрования, анализа угроз и безопасной разработки.

Программа предназначена для школьников 8–9 классов, проявляющих интерес к программированию и желающих получить практические навыки в сфере информационной безопасности.

Программа формирует следующие навыки:

- программирование на Python и работа со стандартными библиотеками для задач информационной безопасности;
- применение алгоритмов шифрования и хеширования для защиты данных;
- анализ логов и выявление признаков подозрительной активности;
- распознавание и предотвращение простейших веб-угроз;
- критический анализ и исправление кода, в том числе сгенерированного ИИ-инструментами.

Программа способствует формированию целостного понимания информационной безопасности, её этических и правовых аспектов. Обучающиеся научатся использовать цифровые технологии осознанно и ответственно, критически оценивая риски и соблюдая культуру цифровой гигиены.

Входные требования к обучающимся: необходимо базовое знакомство с алгоритмическими конструкциями (ветвления, циклы) и начальные навыки работы с компьютером. Специальной подготовки в области программирования и информационной безопасности не требуется.

Программа базового уровня сочетает глубокую техническую подготовку с развитием командных навыков и правовой грамотности. Содержание и материалы программы разработаны с учётом возрастных особенностей целевой аудитории и обеспечивают последовательное усвоение материала от базового синтаксиса Python до разработки и защиты итогового проекта. Предусмотрена система повторения: каждый модуль опирается на навыки предыдущего, а в четвёртом модуле обучающиеся интегрируют все полученные знания в итоговом проекте. Программа построена на дифференцированном подходе и предусматривает практические задания двух уровней сложности.

Программа ориентирована на обеспечение вклада в развитие дальнейшей образовательной траектории в сфере ИТ за счёт включения элементов содержания из кодификатора ОГЭ по информатике и практических заданий, направленных на подготовку к экзамену. Начиная со второго модуля, программа предусматривает вариативность образовательной траектории, которая выражается в предоставлении обучающимся выбора контекста практических заданий.

В программу интегрированы кейс-задачи, не имеющие единственно верного ответа, включая задачу, представленную аккредитованной ИТ-организацией. В практических заданиях предусмотрены основы коллективной работы: парное программирование, командный аудит кода с распределением ролей и критериями оценки индивидуального вклада каждого участника.

Программа включает работу с использованием искусственного интеллекта (ИИ): нейросети используются как инструмент для поиска уязвимостей и анализа кода, а обучающиеся учатся проверять и исправлять сгенерированный ИИ код. Предусмотрена «Политика использования ИИ-инструментов», регламентирующая допустимые и запрещённые виды деятельности. Правовой блок программы охватывает Доктрину информационной безопасности РФ, защиту персональных данных, уголовную ответственность в сфере компьютерной информации и этику ответственного раскрытия уязвимостей.

Промежуточные аттестации более чем наполовину состоят из практико-ориентированных заданий на написание кода, а итоговая аттестация реализована в формате, устойчивом к ИИ-генерации, и включает тестирование и защиту проекта с демонстрацией результатов проектной работы.

Результаты освоения программы востребованы как для дальнейшего обучения, так и в повседневной цифровой жизни. Изучение базовых методов защиты информации, освоение инструментов программирования и практических подходов к решению задач формируют прочную основу для успешного старта в сфере информационной безопасности и смежных направлениях ИТ.

Цель программы: формирование у обучающихся 8–9 классов базовых компетенций в программировании на языке Python и понимания фундаментальных принципов информационной безопасности (ИБ) посредством решения прикладных практико-ориентированных задач, а также создание условий для разработки и успешной защиты итогового проекта.

Задачи

1. Сформировать навыки работы с базовым синтаксисом Python на основе задач информационной безопасности.
2. Познакомить с основами защиты данных: сформировать понимание разницы между кодированием, шифрованием и хешированием; научить применять классические алгоритмы.
3. Научить распознавать и предотвращать простейшие веб-угрозы.
4. Развить алгоритмическое мышление, а также навыки критического анализа кода.
5. Воспитать культуру цифровой гигиены и этичного поведения.
6. Сформировать опыт завершённой инженерной деятельности: от выбора идеи проекта до его защиты.

Задачи обучения, развития, воспитания:

Задачи обучения:

сформировать отношение к компьютерной технике, смартфону, планшету и другим современным техническим устройствам как к инструменту, требующему осознанного и безопасного использования;

сформировать мотивацию к изучению программных ИТ-инструментов для создания и реализации проектов в области защиты информации;

сформировать базовое представление о программных разработках с помощью языка программирования Python в контексте задач информационной безопасности;

сформировать первичное представление о триаде информационной безопасности (конфиденциальность, целостность, доступность) и основных видах киберугроз;

сформировать базовое представление о принципах шифрования, хеширования и кодирования данных, а также о различиях между ними;

изучить ключевые стандартные библиотеки Python для решения задач информационной безопасности (hashlib, secrets, socket);

изучить базовые принципы анализа логов и выявления признаков подозрительной активности.

Задачи воспитания:

сформировать нормы культурного проявления социальной активности и гражданской позиции в отношении защиты персональных данных и соблюдения цифровой гигиены;

сформировать морально-этическую основу для развития профессиональной позиции в отношении использования технологий искусственного интеллекта и нейронных сетей, включая критическую оценку сгенерированного кода;

сформировать основу для развития культуры профессионального общения в IT-сфере, в том числе навыков парного программирования и командного аудита кода;

воспитать ответственное отношение к соблюдению правовых и этических норм в сфере информационной безопасности.

Задачи развития:

способствовать развитию алгоритмического и критического мышления;

развивать творческий подход к решению задач защиты информации;

развивать профессиональный тезаурус и понимание принципов безопасной разработки программного обеспечения;

развивать навыки отладки и анализа чужого кода, включая код, сгенерированный ИИ-инструментами.

Формы и режим занятий

Формы занятий – теоретическая подготовка, практическая работа, самостоятельная работа.

Объем часов в неделю – до 6 академических часов.

Описание планируемых результатов обучения:

Сформированные у обучающихся базовые умения и навыки в области кибербезопасности.

По окончании обучения по программе базового уровня обучающиеся будут иметь представление:

- о роли специалиста по ИБ и форматах профессионального развития в IT.

знать:

- базовые конструкции языка Python;
- принципы информационной безопасности (конфиденциальность, целостность, доступность);
- основные виды шифрования (симметричное, асимметричное), хеширование и их применение;
- типичные веб-уязвимости;
- правовые и этические нормы в сфере ИБ.

понимать:

- разницу между кодированием, шифрованием и хешированием и уместность применения каждого из методов;
- роль ИИ-инструментов в современном процессе разработки и аудита кода, а также риски, связанные с некритическим использованием сгенерированного кода.

уметь:

- писать программы на Python для шифрования/дешифрования данных, проверки паролей, анализа URL-адресов;
- использовать библиотеки hashlib, secrets, socket для решения задач ИБ;
- анализировать логи и выявлять подозрительную активность.

владеть:

- навыками работы со стандартными библиотеками Python для задач ИБ;

- навыками чтения, написания и комментирования кода на Python в соответствии с базовыми принципами читаемости;
- навыками поиска и исправления уязвимостей в учебном коде;
- навыками защиты итогового проекта.

У обучающегося будут сформированы:

- культура цифровой гигиены и ответственного поведения в сети;
- понимание правовой ответственности и этических границ деятельности специалиста по ИБ;
- критическое мышление при работе с ИИ-инструментами;
- навыки командной работы;
- мотивация к дальнейшему изучению ИТ и информационной безопасности, в том числе к участию в олимпиадах и соревнованиях.

Планируемые результаты обучения измеримы и проверяемы через систему текущего контроля, промежуточной аттестации по каждому модулю и итогового контроля по ДОП.

Личностные результаты:

ответственное отношение к учению, способность к саморазвитию и самообразованию, осознанному выбору и построению дальнейшей индивидуальной траектории образования на базе ориентировки в профессиональных предпочтениях, с учётом устойчивых познавательных интересов и уважительного отношения к труду;

готовность и способность к самообразованию на протяжении всей жизни как условию успешной профессиональной и общественной деятельности;

формирование культуры цифровой гигиены и ответственного поведения в сети, осознание ценности личных данных и необходимости их защиты;

понимание правовой ответственности и этических границ деятельности в сфере информационной безопасности.

Метапредметные результаты:

умение самостоятельно определять цели своего обучения, ставить и формулировать для себя новые задачи в познавательной деятельности, развивать её мотивы и интересы;

умение самостоятельно планировать альтернативные пути достижения целей, осознанно выбирать наиболее эффективные способы решения учебных и познавательных задач;

умение соотносить свои действия с планируемыми результатами, осуществлять контроль своей деятельности, определять способы действий в рамках предложенных условий и требований, корректировать их в соответствии с изменяющейся ситуацией;

умение самостоятельно определять цели деятельности и составлять её планы; контролировать и корректировать деятельность; использовать все возможные ресурсы для реализации планов деятельности; выбирать успешные стратегии в различных ситуациях;

умение продуктивно общаться и взаимодействовать в процессе совместной деятельности, учитывать позиции других участников, эффективно разрешать конфликты;

развитие критического мышления при работе с информацией, в том числе с кодом, сгенерированным ИИ-инструментами.

Предметные результаты:

представление о триаде информационной безопасности (конфиденциальность, целостность, доступность) и основных видах киберугроз;

представление о возможностях языка программирования Python для решения задач информационной безопасности;

представление о программных инструментах и стандартных библиотеках, используемых для шифрования, хеширования и анализа данных;

базовые навыки и умения написания программного кода на языке программирования Python для решения практических задач защиты информации;

базовые навыки и умения работы со стандартными библиотеками Python (hashlib, secrets, socket) для шифрования данных, генерации криптостойких значений и анализа логов;

базовые навыки распознавания простейших веб-угроз и применения методов их нейтрализации.

2. Учебный план

Наименование модулей/тем программы	Всего, час	Виды учебных занятий				Формы контроля
		Теория	Практика	Самостоятельная работа	Контроль/ аттестация, ак. час	
Модуль 1. Основы кибербезопасности и программирование	36	10	18	6	2	
Тема 1.1. Знакомство с образовательной платформой, инструментами обучения и триадой информационной безопасности: конфиденциальность, целостность, доступность	2	2	0	0	0	
Тема 1.2. Ответственное использование ИТ: персональные данные, безопасность, цифровой след и этика ИИ	3	2	0	1	0	
Тема 1.3. Безопасная среда разработки и работа со строками	6	1	3	1	1	Выполнение тестовых заданий для текущего контроля знаний и навыков по пройденному материалу
Тема 1.4. Логика защиты: валидаторы	5	1	3	1	0	

Наименование модулей/тем программы	Всего, час	Виды учебных занятий				Формы контроля
		Теория	Практика	Самостоятельная работа	Контроль/ аттестация, ак. час	
Тема 1.5. Циклы в безопасности	10	2	6	2	0	
Тема 1.6. Случайные числа. Кейс-задача	9	2	6	1	0	
Промежуточная аттестация по модулю 1	1	0	0	0	1	Тестирование и выполнение практико-ориентированных заданий на написание программного кода
Модуль 2. Шифрование и защита данных	36	7	21	6	2	
Тема 2.1. Кодирование и шифрование	10	2	6	2	0	
Тема 2.2. Операция XOR как основа шифрования	5	1	3	1	0	
Тема 2.3. Цифровые отпечатки: введение в хеширование	5	1	3	0	1	Выполнение тестовых заданий для текущего контроля знаний и навыков по пройденному материалу
Тема 2.4. Стеганография: искусство скрывать	5	1	3	1	0	
Тема 2.5. Шифрование файлов. Кейс-задача	10	2	6	2	0	

Наименование модулей/тем программы	Всего, час	Виды учебных занятий				Формы контроля
		Теория	Практика	Самостоятельная работа	Контроль/ аттестация, ак. час	
Промежуточная аттестация по модулю 2	1	0	0	0	1	Тестирование и выполнение практико-ориентированных заданий на написание программного кода
Модуль 3. Безопасность в сетях и веб-среде	36	7	21	6	2	
Тема 3.1. Как компьютеры общаются: IP-адреса, порты и сокет	10	2	6	2	0	
Тема 3.2. Веб-запросы, библиотеки, искусственный интеллект как инструмент в ИБ	5	1	3	1	0	
Тема 3.3. Табличные данные цифрового двойника: работа с CSV	5	1	3	0	1	Выполнение тестовых заданий для текущего контроля знаний и навыков по пройденному материалу
Тема 3.4. Межсайтовый скриптинг (XSS): как вредоносный код попадает на сайт. Проверка уязвимостей с применением ИИ	5	1	3	1	0	

Наименование модулей/тем программы	Всего, час	Виды учебных занятий				Формы контроля
		Теория	Практика	Самостоятельная работа	Контроль/ аттестация, ак. час	
Тема 3.5. Фишинг и проверка URL-адресов	5	1	3	1	0	
Тема 3.6. Безопасное хранение данных: введение в базы данных и SQL-инъекции. Кейс-задача	5	1	3	1	0	
Промежуточная аттестация по модулю 3	1	0	0	0	1	Тестирование и выполнение практико-ориентированных заданий на написание программного кода
Модуль 4. Итоговый проект	36	6	18	10	2	
Тема 4.1. Доктрина информационной безопасности. Белые, серые, черные хакеры. Этика и закон	5	1	3	1	0	
Тема 4.2. Аудит кода: ищем уязвимости в чужих и своих программах	10	2	6	2	0	
Тема 4.3. Проектирование итогового проекта	7	1	3	2	1	Выполнение тестовых заданий для текущего контроля знаний и навыков по пройденному материалу

Наименование модулей/тем программы	Всего, час	Виды учебных занятий				Формы контроля
		Теория	Практика	Самостоятельная работа	Контроль/ аттестация, ак. час	
Тема 4.4. Разработка и отладка проекта	8	1	3	4	0	
Тема 4.5. Оформление проекта и подготовка к защите	5	1	3	1	0	
Промежуточная аттестация по модулю 4	1	0	0	0	1	Тестирование и выполнение практико-ориентированных заданий на написание программного кода
Итоговый контроль	1	0	0	0	1	Комплексное задание: тест и защита проекта
Итого	145	30	78	28	9	
ИТиСИ	Объем часов ИТиСИ не входит в общую трудоемкость ДОП, но участие в ИТиСИ обязательно для всех успешно прошедших Итоговый контроль/аттестацию по ДОП					

3. Календарно-тематическое планирование

Название ДОП	№ потока	Дата начала обучения по ДОП	№ модуля ДОП	Начало обучения по модулю ДОП	Календарный период (количество дней) длительности модуля	Дата окончания обучения по ДОП
Кибербезопасность. 8-9 класс (базовый уровень)	1	2026-10-01	1	2026-10-01	61	2027-05-28
			2	2026-12-01	67	
			3	2027-02-08	54	
			4	2027-04-05	54	

4. Рабочая программа

Порядковый номер модуля	Наименование темы	Лекции. Количество академических часов	Содержание теоретической подготовки	Практическое занятие. Количество академических часов	Содержание практической работы	Самостоятельная работа. Количество академических часов	Содержание самостоятельной работы
1	Основы кибербезопасности и программирование						
1	Тема 1.1. Знакомство с образовательной платформой, инструментами обучения и триадой информационной безопасности: конфиденциальность, целостность, доступность	2	Знакомство с LMS и основными инструментами обучения: теоретическими материалами, тренажёрами кода, тестами и самостоятельной работой. Основы кибербезопасности и три главных правила защиты данных. Формирование цифрового следа и какие угрозы нас подстерегают: от фишинга и вирусов до утечек паролей. Составление базовой модели угроз, для понимания, кто и как может атаковать наши устройства.	0	Практическая работа в указанной теме Дополнительной общеобразовательной программы не предусмотрена и проводиться не будет.	0	Самостоятельная работа и самоконтроль в указанной теме Дополнительной общеобразовательной программы не предусмотрены и проводиться не будут.

1	Тема 1.2. Ответственное использование ИТ: персональные данные, безопасность, цифровой след и этика ИИ	2	Персональные данные и законодательство об их защите. Уголовная ответственность за киберпреступления (статьи УК РФ). Этика специалиста по информационной безопасности. Отличие легального поиска уязвимостей от киберпреступления. Безопасное использование нейросетей при написании кода.	0	Практическая работа в указанной теме Дополнительной общеобразовательной программы не предусмотрена и проводиться не будет.	1	Повторение и систематизация пройденного материала по ключевым понятиям и практическим навыкам темы. Закрепление теоретических знаний и практических умений через выполнение заданий для самостоятельной работы с автоматической системой оценивания.
1	Тема 1.3. Безопасная среда разработки и работа со строками	1	Базовые конструкции Python: переменные, типы данных, условия. Виртуальное окружение и изоляция зависимостей проекта. Переменные окружения как способ хранения конфигурации и чувствительных данных. Почему пароли, токены нельзя хранить в	3	Повторение теории, необходимой для выполнения практических заданий по применению базовых конструкций Python. Подробный разбор совместно с обучающимися решения задач по созданию виртуального окружения. Выполнение практических заданий по работе со строками. Подробное описание практических заданий	1	Повторение и систематизация пройденного материала по ключевым понятиям и практическим навыкам темы. Закрепление теоретических знаний и практических умений через выполнение заданий для самостоятельной работы с автоматической системой оценивания.

			коде. Введение в системы контроля версий.		представлено в приложении к ДОП. Проведение диагностического опроса «Повторим главное» для повторения и закрепления полученных знаний. Дополнительные упражнения по теме представлены в методической разработке «Материалы для преподавателя по проведению практических занятий».		
1	Тема 1.4. Логика защиты: валидаторы	1	Списки, словари и множества для хранения логов и черных списков. Влияние выбора структуры данных на скорость работы программы и её защиту от атак перебором. Готовые инструменты Python для решения задач информационной безопасности	3	Повторение теории, необходимой для выполнения практических заданий по применению структур данных для хранения логов. Подробный разбор совместно с обучающимися решения задач по влиянию выбора структуры данных на скорость работы программы и её защиту от атак перебором. Выполнение практических заданий по использованию готовых инструментов Python для решения задач информационной	1	Повторение и систематизация пройденного материала по ключевым понятиям и практическим навыкам темы. Закрепление теоретических знаний и практических умений через выполнение заданий для самостоятельной работы и самоконтроля/самопроверки с автоматической системой оценивания.

					безопасности. Подробное описание практических заданий представлено в приложении к ДОП. Проведение диагностического опроса «Повторим главное» для повторения и закрепления полученных знаний. Дополнительные упражнения по теме представлены в методической разработке «Материалы для преподавателя по проведению практических занятий».		
1	Тема 1.5. Циклы в безопасности	2	Циклы для построения безопасных систем. Скрытие важных данных с помощью циклов. Строгая проверка данных на входе для защиты программы от сбоев и вредоносного ввода.	6	Повторение теории, необходимой для выполнения практических заданий по применению циклов для построения безопасных систем. Подробный разбор совместно с обучающимися решения задач по сокрытию важных данных с помощью циклов. Выполнение практических заданий по проверке данных на входе. Подробное описание практических заданий представлено в	2	Повторение и систематизация пройденного материала по ключевым понятиям и практическим навыкам темы. Закрепление теоретических знаний и практических умений через выполнение заданий для самостоятельной работы с автоматической системой оценивания.

					приложении к ДОП. Проведение диагностического опроса «Повторим главное» для повторения и закрепления полученных знаний. Дополнительные упражнения по теме представлены в методической разработке «Материалы для преподавателя по проведению практических занятий».		
1	Тема 1.6. Случайные числа. Кейс-задача	2	Предсказуемость обычной случайности в программировании и её непригодность для создания паролей. Работа с байтами и генерация криптографически стойких случайных чисел. Понятие энтропии. Создание надежных одноразовых токенов для защиты систем.	6	Повторение теории, необходимой для выполнения практических заданий по демонстрации предсказуемости обычной случайности и её непригодности для создания паролей. Подробный разбор совместно с обучающимися решения задач по работе с байтами. Выполнение практических заданий по указанным темам. Разбор кейс-задачи. Подробное описание практических заданий представлено в приложении к ДОП. Проведение	1	Повторение и систематизация пройденного материала по ключевым понятиям и практическим навыкам темы. Закрепление теоретических знаний и практических умений через выполнение заданий для самостоятельной работы и самоконтроля/самопроверки с автоматической системой оценивания.

					диагностического опроса «Повторим главное» для повторения и закрепления полученных знаний. Дополнительные упражнения по теме представлены в методической разработке «Материалы для преподавателя по проведению практических занятий».		
2	Шифрование и защита данных						
2	Тема 2.1. Кодирование и шифрование	2	Различие между сокрытием смысла (шифрование) и изменением формата (кодирование). Написание классического шифра со сдвигом символов с использованием циклов и операции взятия остатка от деления (%), а также знакомство с модулем base64.	6	Повторение теории, необходимой для выполнения практических заданий по различию между сокрытием смысла (шифрование) и изменением формата (кодирование). Подробный разбор совместно с обучающимися решения задач по написанию классического шифра. Выполнение практических заданий по применению методов кодирования в задачах ИБ. Подробное описание практических заданий представлено в приложении к ДОП.	2	Повторение и систематизация пройденного материала по ключевым понятиям и практическим навыкам темы. Закрепление теоретических знаний и практических умений через выполнение заданий для самостоятельной работы с автоматической системой оценивания.

					Проведение диагностического опроса «Повторим главное» для повторения и закрепления полученных знаний. Дополнительные упражнения по теме представлены в методической разработке «Материалы для преподавателя по проведению практических занятий».		
2	Тема 2.2. Операция XOR как основа шифрования	1	Объяснение двоичной системы и побитовых операции. Использование двоичных систем в шифровании.	3	Повторение теории, необходимой для выполнения практических заданий по основам двоичной системы. Подробный разбор совместно с обучающимися решения задач по использованию двоичных систем в шифровании. Выполнение практических заданий по применению операции XOR для шифрования и дешифрования сообщений. Подробное описание практических заданий представлено в приложении к ДОП. Проведение диагностического опроса	1	Повторение и систематизация пройденного материала по ключевым понятиям и практическим навыкам темы. Закрепление теоретических знаний и практических умений через выполнение заданий для самостоятельной работы и самоконтроля/самопроверки с автоматической системой оценивания.

					«Повторим главное» для повторения и закрепления полученных знаний. Дополнительные упражнения по теме представлены в методической разработке «Материалы для преподавателя по проведению практических занятий».		
2	Тема 2.3. Цифровые отпечатки: введение в хеширование	1	Использование обычных хеш-функций для проверки подлинности сообщений. Причины запрета на простое хеширование паролей. Использование хакерами словарей и радужных таблиц. Роль «соли». Современные медленные алгоритмы, делающие перебор паролей невозможным.	3	Повторение теории, необходимой для выполнения практических заданий по использованию обычных хеш-функций для проверки подлинности сообщений. Подробный разбор совместно с обучающимися решения задач по анализу причин запрета на простое хеширование паролей. Выполнение практических заданий по практическому применению роли «соли». Подробное описание практических заданий представлено в приложении к ДОП. Проведение диагностического опроса «Повторим главное» для	0	Самостоятельная работа и самоконтроль в указанной теме Дополнительной общеобразовательной программы не предусмотрены и проводиться не будут.

					повторения и закрепления полученных знаний. Дополнительные упражнения по теме представлены в методической разработке «Материалы для преподавателя по проведению практических занятий».		
2	Тема 2.4. Стеганография: искусство скрывать	1	Введение в методы сокрытия данных внутри других данных. Почему зашифрованный текст выглядит как бессмысленный набор символов. Каким образом стеганография прячет «контейнер». Маскировка сообщений.	3	Повторение теории, необходимой для выполнения практических заданий по методам сокрытия данных внутри других данных и пониманию различий между зашифрованным текстом и бессмысленным набором символов. Подробный разбор совместно с обучающимися решения задач по принципам стеганографии. Выполнение практических заданий по маскировке сообщений. Подробное описание практических заданий представлено в приложении к ДОП. Проведение диагностического опроса	1	Повторение и систематизация пройденного материала по ключевым понятиям и практическим навыкам темы. Закрепление теоретических знаний и практических умений через выполнение заданий для самостоятельной работы и самоконтроля/самопроверки с автоматической системой оценивания.

					«Повторим главное» для повторения и закрепления полученных знаний. Дополнительные упражнения по теме представлены в методической разработке «Материалы для преподавателя по проведению практических занятий».		
2	Тема 2.5. Шифрование файлов. Кейс-задача	2	Введение в шифрование файлов и файловых систем. Как работать с разными директориями, системами чтения и записи. Разбор вспомогательных встроенных модулей языка программирования Python для решения задач шифрования файлов.	6	Повторение теории, необходимой для выполнения практических заданий по основам шифрования файлов и файловых систем. Подробный разбор совместно с обучающимися решения задач и выполнение практических заданий по применению встроенных модулей языка программирования Python для решения задач шифрования. Разбор кейс-задачи. Подробное описание практических заданий представлено в приложении к ДОП. Проведение диагностического опроса «Повторим главное» для повторения и	2	Повторение и систематизация пройденного материала по ключевым понятиям и практическим навыкам темы. Закрепление теоретических знаний и практических умений через выполнение заданий для самостоятельной работы с автоматической системой оценивания.

					закрепления полученных знаний. Дополнительные упражнения по теме представлены в методической разработке «Материалы для преподавателя по проведению практических занятий».		
3	Безопасность в сетях и веб-среде						
3	Тема 3.1. Как компьютеры общаются: IP-адреса, порты и сокет	2	Сетевое общение устройств друг с другом. Клиент-сервер и принцип работы сокетов. Передача сообщений в открытом и зашифрованном виде. Применение знаний из модуля про криптографию для защиты сетевого общения от перехвата.	6	Повторение теории, необходимой для выполнения практических заданий по принципам сетевого общения устройств и архитектуры клиент-сервер. Подробный разбор совместно с обучающимися решения задач и выполнение практических заданий по работе с сокетами и передаче сообщений. Подробное описание практических заданий представлено в приложении к ДОП. Проведение диагностического опроса «Повторим главное» для повторения и закрепления полученных знаний. Дополнительные упражнения по теме	2	Повторение и систематизация пройденного материала по ключевым понятиям и практическим навыкам темы. Закрепление теоретических знаний и практических умений через выполнение заданий для самостоятельной работы с автоматической системой оценивания.

					представлены в методической разработке «Материалы для преподавателя по проведению практических занятий».		
3	Тема 3.2. Веб-запросы, библиотеки, искусственный интеллект как инструмент в ИБ	1	Принципы работы протоколов HTTP и HTTPS, проверка защищенного соединения. Анализ запросов и проверка базовых заголовков безопасности сайта. Использование ИИ для автодополнения кода, поиска уязвимостей и генерации тестов.	3	Повторение теории, необходимой для выполнения практических заданий по принципам работы протоколов HTTP и HTTPS. Подробный разбор совместно с обучающимися решения задач по анализу веб-запросов. Выполнение практических заданий по использованию ИИ для поиска уязвимостей в задачах ИБ. Подробное описание практических заданий представлено в приложении к ДОП. Проведение диагностического опроса «Повторим главное» для повторения и закрепления полученных знаний. Дополнительные упражнения по теме представлены в методической разработке «Материалы для преподавателя по	1	Повторение и систематизация пройденного материала по ключевым понятиям и практическим навыкам темы. Закрепление теоретических знаний и практических умений через выполнение заданий для самостоятельной работы и самоконтроля/самопроверки с автоматической системой оценивания.

					проведению практических занятий».		
3	Тема 3.3. Табличные данные цифрового двойника: работа с CSV	1	Принципы сетевой разведки и выявление доступных служб. Сканирование портов как способ обнаружения потенциальных точек входа. Многопоточность при сканировании сети. Заголовки безопасности HTTP: CSP, HSTS, X-Frame-Options, X-Content-Type-Options. Аудит заголовков как элемент проверки защищённости веб-приложения. Применение ИИ-инструментов для генерации и проверки кода в задачах ИБ.	3	Повторение теории, необходимой для выполнения практических заданий по принципам сетевой разведки. Подробный разбор совместно с обучающимися решения задач по работе с CSV. Выполнение практических заданий по указанной теме. Подробное описание практических заданий представлено в приложении к ДОП. Проведение диагностического опроса «Повторим главное» для повторения и закрепления полученных знаний. Дополнительные упражнения по теме представлены в методической разработке «Материалы для преподавателя по проведению практических занятий».	0	Самостоятельная работа и самоконтроль в указанной теме Дополнительной общеобразовательной программы не предусмотрены и проводиться не будут.
3	Тема 3.4. Межсайтовый скриптинг (XSS): как вредоносный	1	Разбор уязвимости XSS на простых примерах. Причины недоверия к	3	Повторение теории, необходимой для выполнения практических заданий по	1	Повторение и систематизация пройденного материала по ключевым понятиям и практическим

	код попадает на сайт. Проверка уязвимостей с применением ИИ		пользовательскому вводу. Функция, очищающая строки от опасных HTML-тегов перед показом на странице. Помощь ИИ в автоматическом поиске таких уязвимостей. Сравнение автоматического поиска с ручной проверкой кода.		разбору уязвимости XSS на простых примерах и пониманию причин недоверия к пользовательскому вводу. Подробный разбор совместно с обучающимися решения задач по проверке уязвимости. Выполнение практических заданий по применению ИИ для автоматического поиска уязвимостей. Подробное описание практических заданий представлено в приложении к ДОП. Проведение диагностического опроса «Повторим главное» для повторения и закрепления полученных знаний. Дополнительные упражнения по теме представлены в методической разработке «Материалы для преподавателя по проведению практических занятий».		навыкам темы. Закрепление теоретических знаний и практических умений через выполнение заданий для самостоятельной работы и самоконтроля/самопроверки с автоматической системой оценивания.
3	Тема 3.5. Фишинг и проверка URL-адресов	1	Изучение методов обмана пользователей. Манипуляция людьми со стороны	3	Повторение теории, необходимой для выполнения практических заданий по изучению методов	1	Повторение и систематизация пройденного материала по ключевым понятиям и практическим навыкам темы. Закрепление

			хакеров для выманивания паролей и данных. Анализатор URL-адресов на Python, ищущий подозрительные паттерны. Опечатки в доменах, лишние символы и IP-адрес вместо нормального имени. Распознавание фишинговых ссылок до клика по ним		обмана пользователей и манипуляций для выманивания данных. Подробный разбор совместно с обучающимися решения задач по разработке анализатора URL-адресов. Выполнение практических заданий по распознаванию фишинговых ссылок. Подробное описание практических заданий представлено в приложении к ДОП. Проведение диагностического опроса «Повторим главное» для повторения и закрепления полученных знаний. Дополнительные упражнения по теме представлены в методической разработке «Материалы для преподавателя по проведению практических занятий».		теоретических знаний и практических умений через выполнение заданий для самостоятельной работы с автоматической системой оценивания.
3	Тема 3.6. Безопасное хранение данных: введение в базы данных и SQL-	1	Концептуальный разбор обмана базы данных злоумышленниками через вредоносный ввод. Сравнение	3	Повторение теории, необходимой для выполнения практических заданий по безопасному хранению данных. Подробный	1	Повторение и систематизация пройденного материала по ключевым понятиям и практическим навыкам темы. Закрепление теоретических знаний и

	инъекции. Кейс-задача		опасной конкатенации строк с безопасными запросами к словарю Python.		разбор совместно с обучающимися решения задач по и выполнение практических заданий по защите от SQL-инъекций. Подробное описание практических заданий представлено в приложении к ДОП. Проведение диагностического опроса «Повторим главное» для повторения и закрепления полученных знаний. Дополнительные упражнения по теме представлены в методической разработке «Материалы для преподавателя по проведению практических занятий».		практических умений через выполнение заданий для самостоятельной работы и самоконтроля/самопроверки с автоматической системой оценивания
4	Итоговый проект						
4	Тема 4.1. Доктрина информационной безопасности. Белые, серые, черные хакеры. Этика и закон	1	Обсуждение законов, кодексов и этических принципов специалиста по ИБ. Причины запрета на тестирование чужих систем без письменного разрешения. Разбор правил ответственного раскрытия	3	Повторение теории, необходимой для выполнения практических заданий по обсуждению законов, кодексов и этических принципов специалиста по ИБ. Подробный разбор совместно с обучающимися решения задач и выполнение практических заданий по	1	Повторение и систематизация пройденного материала по ключевым понятиям и практическим навыкам темы. Закрепление теоретических знаний и практических умений через выполнение заданий для самостоятельной работы с автоматической системой оценивания.

			уязвимостей. Правильный способ сообщения о баге без причинения вреда. Понимание грани между белым и черным хакером через призму закона и этики.		разбору правил ответственного раскрытия уязвимостей. Разбор кейс-задачи. Подробное описание практических заданий представлено в приложении к ДОП. Проведение диагностического опроса «Повторим главное» для повторения и закрепления полученных знаний. Дополнительные упражнения по теме представлены в методической разработке «Материалы для преподавателя по проведению практических занятий».		
4	Тема 4.2. Аудит кода: ищем уязвимости в чужих и своих программах	2	Изучение чтения чужого кода. Поиск ошибок в парах. Жестко заданные пароли, отсутствие проверок ввода, использование random вместо secrets. Исправление найденных уязвимостей. Объяснение причин безопасности новых версий кода.	6	Повторение теории, необходимой для выполнения практических заданий по изучению чтения чужого кода и практике поиска ошибок. Подробный разбор совместно с обучающимися решения задач по аудиту своего и чужого кода. Выполнение практических заданий по исправлению найденных	2	Повторение и систематизация пройденного материала по ключевым понятиям и практическим навыкам темы. Закрепление теоретических знаний и практических умений через выполнение заданий для самостоятельной работы и самоконтроля/самопроверки с автоматической системой оценивания.

					уязвимостей и аргументированному объяснению причин безопасности новых версий кода. Подробное описание практических заданий представлено в приложении к ДОП. Проведение диагностического опроса «Повторим главное» для повторения и закрепления полученных знаний. Дополнительные упражнения по теме представлены в методической разработке «Материалы для преподавателя по проведению практических занятий».		
4	Тема 4.3. Проектирование итогового проекта	1	Выбор темы для итогового проекта из готовых вариантов. Определение объекта защиты и учитываемых угроз. Формулирование идеи для ее реализуемости и интересности. Цели и формат финального проекта. Критерии оценки.	3	Повторение теории, необходимой для выполнения практических заданий. Разбор с обучающимися примеров трёх направлений итогового проекта и критериев их оценки. Выбор обучающимися одного из вариантов проекта. Выполнение обучающимися практических заданий по	2	Повторение и систематизация пройденного материала по ключевым понятиям и практическим навыкам темы. Закрепление теоретических знаний и практических умений через выполнение заданий для самостоятельной работы с автоматической системой оценивания.

					проектированию структуры программы и созданию первого рабочего прототипа. Подробное описание практических заданий приложено к ДОП. Проведение проверочного тестирования для закрепления изученного материала. Дополнительные упражнения по теме представлены в методической разработке «Материалы для преподавателя по проведению практических занятий».		
4	Тема 4.4. Разработка и отладка проекта	1	Организация разработки проекта: итеративный подход. Отладка и тестирование решения. Оформление кода. Подготовка к презентации результатов.	3	Повторение теории, необходимой для выполнения практических заданий. Разбор с обучающимися примеров отладки кода и тестирования на граничных случаях. Выполнение обучающимися практических заданий по доработке собственного проекта, проверке обработки ошибок. Подробное описание	4	Повторение и систематизация пройденного материала по ключевым понятиям и практическим навыкам темы. Закрепление теоретических знаний и практических умений через выполнение заданий для самостоятельной работы и самоконтроля/самопроверки с автоматической системой оценивания

					практических заданий приложено к ДОП. Проведение проверочного тестирования для закрепления изученного материала. Дополнительные упражнения по теме представлены в методической разработке «Материалы для преподавателя по проведению практических занятий».		
4	Тема 4.5. Оформление проекта и подготовка к защите	1	Структура итоговой документации проекта. Описание задачи, решения и результатов. Подготовка демонстрации и защиты проекта. Оформление кода и файла README. Самооценка по критериям.	3	Повторение теории, необходимой для выполнения практических заданий. Разбор с обучающимися примеров написания технической документации (README) и подготовки к публичному выступлению. Выполнение обучающимися практических заданий по финальной доработке проекта, оформлению файла README, репетиции защиты и подготовке ответов на технические вопросы	1	Повторение и систематизация пройденного материала по ключевым понятиям и практическим навыкам темы. Закрепление теоретических знаний и практических умений через выполнение заданий для самостоятельной работы с автоматической системой оценивания.

					комиссии. Подробное описание практических заданий приложено к ДОП. Проведение проверочного тестирования для закрепления изученного материала. Дополнительные упражнения по теме представлены в методической разработке «Материалы для преподавателя по проведению практических занятий».		
--	--	--	--	--	--	--	--

5. Формы аттестации и оценочные материалы, включая примеры контрольных заданий

5.1 Текущий контроль

В таблице ниже представлены по каждому из модулей:

- количество часов текущего контроля;
- формы текущего контроля с подробным описанием процедуры оценивания результатов обучения;
- диагностические инструменты с примерами (контрольные задания, материалы, промежуточные тесты и задачи);
- показатели и критерии оценивания;
- шкала оценивания.

Текущий контроль. Количество ак. часов	1	1	1	1
Текущий контроль. Формы контроля	Тестирование	Тестирование	Тестирование	Тестирование
Текущий контроль. Диагностические инструменты	Задание в виде теста. Вопрос 1. Кто такой пентестер?	Задание в виде теста. Вопрос 1. Как называется процесс проверки того, что введенные пользователем данные	Задание в виде теста. Вопрос 1. Как называется протокол, при котором данные между вашим браузером	Задание в виде теста. Вопрос 1. Какая ситуация больше всего похожа на попытку социальной инженерии (обмана

	А) Специалист, который устанавливает антивирусы и фаерволы на компьютер Б) Специалист, который читает логи и ищет подозрительную активность В) Специалист, который пишет инструкции по безопасности Г) Специалист, который по договору с владельцем ищет слабые места в системе, чтобы помочь их закрыть Правильный ответ: Г Вопрос 2. Что такое Доктрина информационной безопасности РФ? А) Раздел Уголовного кодекса о компьютерных преступлениях Б) Главный государственный документ, в котором описано, как страна защищает свою информацию В) Памятка о том, как безопасно вести себя в интернете Г) Инструкция для сисадминов по настройке серверов Правильный ответ: Б	соответствуют нужному формату и правилам? А) Замена специальных символов на безопасные Б) Шифрование введённых данных В) Проверка ввода на соответствие заданным правилам Г) Очистка строки от опасных символов Правильный ответ: В Вопрос 2. Как называется вид мошенничества, при котором злоумышленник обманом выманивает у пользователей пароли и другие секретные данные? А) Обман пользователя для получения конфиденциальной информации Б) Подбор пароля методом перебора В) Перехват сетевого трафика Г) Взлом сервера через уязвимость Правильный ответ: А Вопрос 3. Какое правило безопасности гласит, что любые данные, полученные извне, нужно считать потенциально опасными?	и сайтом передаются в зашифрованном виде, защищая их от перехвата? А) HTTP Б) FTP В) SMTP Г) HTTPS Правильный ответ: Г Вопрос 2. Какая система проверки пользователя обеспечивает наибольшую защиту аккаунта при входе? А) CAPTCHA (картинка с буквами/цифрами) Б) Только логин (имя пользователя) В) Двухфакторная аутентификация (2FA) — пароль + код из SMS или приложения Г) Только пароль Правильный ответ: В Вопрос 3. Что представляет собой файл с расширением .csv? А) Изображение в специальном формате Б) Текстовый файл, в котором данные разделены запятыми (таблица в виде текста) В) Сжатый архив с несколькими файлами	человека с целью получить секретную информацию)? А) Вам пришло письмо с просьбой срочно сообщить пароль или данные карты Б) Официальное письмо от компании с её фирменного адреса В) Письмо с электронной цифровой подписью отправителя Г) Запрос информации через защищённый зашифрованный канал Правильный ответ: А Вопрос 2. Что такое «услуга за услугу» — один из приёмов социальной инженерии? А) Взлом компьютера через интернет Б) Шифрование файлов вирусом-вымогателем В) Перехват интернет-трафика между компьютерами Г) Ситуация, когда злоумышленник предлагает помощь или услугу в обмен на секретную информацию Правильный ответ: Г Вопрос 3. Как работает автодополнение кода с помощью искусственного
--	--	--	--	---

	Вопрос 3. Задание с кратким ответом. Впишите только число. Сколько основных ролей в информационной безопасности было ранее рассмотрено в темах (пентестер, защитник, аналитик)? Ответ: _____ Правильный ответ: 3 Вопрос 4. Кто такой защитник в сфере информационной безопасности? А) Специалист, который собирает информацию о компании из открытых источников Б) Специалист, который настраивает защиту и отражает атаки на компьютеры и сети В) Специалист, который взламывает системы для проверки их надёжности Г) Специалист, который создаёт вирусы и трояны Правильный ответ: Б Вопрос 5. Что такое разведка на основе открытых источников? А) Вирус, который крадёт пароли	А) Весь ввод извне считается потенциально опасным Б) Ввод нужно шифровать перед обработкой В) Нужно спрашивать подтверждение у пользователя Г) Пользователь должен ввести пароль дважды Правильный ответ: А Вопрос 4. В каком модуле Python реализован алгоритм Mersenne Twister для создания псевдослучайных чисел? А) secrets Б) random В) hashlib Г) os Правильный ответ: Б Вопрос 5. Задание с кратким ответом. Впишите только число. Какова минимальная длина пароля, рекомендуемая стандартами безопасности? Ответ: _____ Правильный ответ: 8	Г) Программа, которую можно запустить Правильный ответ: Б Вопрос 4. Задание с кратким ответом. Впишите только число. На какой номер порта по умолчанию настроено безопасное HTTPS-соединение? Ответ: _____ Правильный ответ: 443 Вопрос 5. Как называется процесс превращения пароля в уникальную необратимую строку символов (хеш-сумму), из которой невозможно восстановить исходный пароль? А) Сжатие пароля для экономии места Б) Кодирование пароля в формат Base64 В) Шифрование пароля с возможностью расшифровки Г) Преобразование пароля в необратимую хеш-сумму Правильный ответ: Г	интеллекта (например, в редакторах кода)? А) ИИ проверяет ваш код на ошибки Б) ИИ преобразует код в машинные инструкции В) Программист пишет весь код вручную Г) ИИ автоматически предлагает и генерирует фрагменты кода, анализируя то, что вы уже написали Правильный ответ: Г Вопрос 4. Задание с кратким ответом. Впишите только число. Сколько существует основных видов задач по искусственному интеллекту, которые решают участники образовательных CTF-соревнований? Ответ: _____ Правильный ответ: 5 Вопрос 5. В системе оценки уязвимостей CVSS используется шкала от 0 до 10. Какой диапазон баллов считается критическим (самым опасным)? А) 9.0–10.0 Б) 4.0–6.9 В) 0.0–3.9 Г) 7.0–8.9 Правильный ответ: А
--	--	--	--	---

	Б) Операционная система, например, Kali Linux В) Способ шифрования сообщений в интернете Г) Сбор информации о человеке или организации из открытых источников: соцсетей, сайтов, новостей Правильный ответ: Г			
Текущий контроль. Описание процедуры оценивания Показатели и критерии оценивания	Критерий оценивания: правильность ответа на тестовый вопрос. Показатель оценивания: количество правильных ответов на тестовые задания. За каждый правильный ответ начисляется 1 балл. В случае неправильного ответа баллы не начисляются.	Критерий оценивания: правильность ответа на тестовый вопрос. Показатель оценивания: количество правильных ответов на тестовые задания. За каждый правильный ответ начисляется 1 балл. В случае неправильного ответа баллы не начисляются.	Критерий оценивания: правильность ответа на тестовый вопрос. Показатель оценивания: количество правильных ответов на тестовые задания. За каждый правильный ответ начисляется 1 балл. В случае неправильного ответа баллы не начисляются.	Критерий оценивания: правильность ответа на тестовый вопрос. Показатель оценивания: количество правильных ответов на тестовые задания. За каждый правильный ответ начисляется 1 балл. В случае неправильного ответа баллы не начисляются.
Текущий контроль. Шкала оценивания, нижнее значение	0	0	0	0
Текущий контроль. Шкала оценивания, верхнее значение	5	5	5	5
Текущий контроль. Шкала оценивания, минимальный проходной балл для успешной сдачи	3	3	3	3

5.2 Промежуточная аттестация

В таблице ниже представлены по каждому из модулей:

- количество часов промежуточной аттестации;
- формы контроля (промежуточной аттестации) с подробным описанием процедуры оценивания результатов обучения;
- диагностические инструменты с примерами (контрольные задания, материалы, промежуточные тесты и задачи);
- показатели и критерии оценивания;
- шкала оценивания.

Аттестация по итогам модуля. Количество ак. часов	1	1	1	1
Аттестация по итогам модуля. Формы контроля	Тестирование и выполнение практико-ориентированных заданий на написание программного кода	Тестирование и выполнение практико-ориентированных заданий на написание программного кода	Тестирование и выполнение практико-ориентированных заданий на написание программного кода	Тестирование и выполнение практико-ориентированных заданий на написание программного кода
Аттестация по итогам модуля. Диагностические инструменты	Тест и практико-ориентированные задания. Вопрос 1. Задание с кратким ответом. Впишите только число. Сколько основных ролей специалистов по информационной безопасности мы рассматривали в теме (пентестер, защитник, аналитик)? Ответ: _____ Правильный ответ: 3 Вопрос 2. Задание с кратким ответом. Впишите только число.	Тест и практико-ориентированные задания. Вопрос 1. Задание с кратким ответом. Впишите только число. При кодировании данных в формат Base64 каждые 3 байта исходных данных превращаются в определённое количество символов. Сколько символов Base64 получается из 3 байт? Ответ: _____ Правильный ответ: 4 Вопрос 2. Задание с кратким ответом. Впишите только число.	Тест и практико-ориентированные задания. Вопрос 1. Задание с кратким ответом. Впишите только число. HTML-тег <a> используется для создания ссылок на веб-страницах. Чтобы ссылка работала, у неё должен быть хотя бы один обязательный атрибут (например, href, в котором указывается адрес). Сколько обязательных атрибутов нужно указать для работы тега <a>? Ответ: _____ Правильный ответ: 1	Тест и практико-ориентированные задания. Вопрос 1. Задание с кратким ответом. Впишите только число. В курсе рассматриваются основные принципы безопасного написания кода (например, проверка ввода, защита паролей, шифрование данных и другие). Сколько всего таких принципов мы изучили? Ответ: _____ Правильный ответ: 6 Вопрос 2. Задание с кратким ответом. Впишите только число. Логирование — это запись событий, происходящих в программе (ошибок, действий

	Согласно стандартной международной практике, сколько дней обычно даётся компании на исправление найденной уязвимости, прежде чем о ней объявят публично? Ответ: _____ Правильный ответ: 90 Вопрос 3. Задание с кратким ответом. Впишите только число. Из скольких основных шагов состоит стандартная модель кибератаки (разведка, проникновение, закрепление, развитие атаки, достижение цели)? Ответ: _____ Правильный ответ: 5 Вопрос 4. Чем занимается пентестер? А) По договору с владельцем ищет слабые места в системе и тестирует её на уязвимости Б) Читает логи безопасности и ищет подозрительную активность	Алгоритм хеширования MD5 обрабатывает данные в несколько раундов. Сколько раундов выполняется в алгоритме MD5? Ответ: _____ Правильный ответ: 64 Вопрос 3. Задание с кратким ответом. Впишите только число. В задачах по стеганографии (скрытной передаче сообщений) для успешного извлечения скрытых данных из изображения или файла обычно требуется сообщение определённой минимальной длины. Какова минимальная длина такого сообщения (в символах)? Ответ: _____ Правильный ответ: 10 Вопрос 4. Какая главная особенность асимметричного шифрования (например, RSA)? А) Используется пара ключей: открытый (публичный) для шифрования и закрытый	Вопрос 2. Задание с кратким ответом. Впишите только число. OWASP Top 10 — это список самых опасных уязвимостей веб-приложений, составленный международной организацией OWASP. Сколько типов уязвимостей входит в этот список (судя по названию)? Ответ: _____ Правильный ответ: 10 Вопрос 3. Задание с кратким ответом. Впишите только число. IP-адрес (например, 192.168.1.1) состоит из нескольких частей, разделённых точками. Каждая такая часть называется «октет» и содержит число от 0 до 255. Из скольких октетов состоит стандартный IPv4-адрес? Ответ: _____ Правильный ответ: 4 Вопрос 4. Что такое UNION-инъекция? А) Атака, при которой злоумышленник перегружает сайт огромным количеством запросов (DDoS) Б) Разновидность SQL-инъекции, при которой хакер использует оператор UNION,	пользователей, предупреждений). На сколько основных типов делится логирование по уровню важности (например, информация, предупреждение, ошибка)? Ответ: _____ Правильный ответ: 3 Вопрос 3. Задание с кратким ответом. Впишите только число. ИИ-детекторы определяют, написан ли текст человеком или сгенерирован нейросетью. Для этого они анализируют различные признаки стиля текста (например, разнообразие слов, длину предложений, сложность фраз). Сколько основных признаков стиля анализирует такой детектор? Ответ: _____ Правильный ответ: 7 Вопрос 4. Что такое классификация текста в задачах искусственного интеллекта? А) Автоматическое определение категории текста — например, отнесение письма к спаму или обычным сообщениям, новости к спорту или политике Б) Сжатие текста для экономии места на диске В) Шифрование текста, чтобы его нельзя было прочитать Г) Удаление текста из базы данных
--	---	---	---	---

В) Пишет инструкции и документацию по защите информации Г) Настраивает файрволы и защищает системы от атак Правильный ответ: А Вопрос 5. Что означает аббревиатура NDA в сфере информационной безопасности? А) Соглашение о неразглашении (Non-Disclosure Agreement) — договор, запрещающий разглашать секретную информацию Б) Нормативный документ компании В) Национальная директива по безопасности Г) Новый документ о разработке Правильный ответ: А Вопрос 6. Что такое OSINT (ОСИИТ)? А) Вредоносная программа для кражи данных Б) Сбор информации о человеке или организации из открытых источников:	(секретный) для расшифровки Б) Используется только один ключ для шифрования и расшифровки В) Используются три разных ключа Г) Ключи вообще не используются Правильный ответ: А Вопрос 5. Что такое «радужная таблица» в контексте информационной безопасности? А) Способ кодирования данных в цвета Б) Метод шифрования с использованием цветовых палитр В) Таблица для подбора цветов в дизайне Г) Заранее вычисленная таблица хешей для быстрого подбора паролей Правильный ответ: Г Вопрос 6. Что такое ключ стеганографии? А) Название алгоритма шифрования Б) Секретный ключ, который нужен для извлечения скрытого	чтобы добавить свои данные к результатам запроса к базе данных В) Тип XSS-атаки, при которой в страницу внедряется вредоносный JavaScript Г) Атака, при которой хакер заставляет браузер пользователя выполнить нежелательный запрос (CSRF) Правильный ответ: Б Вопрос 5. Что такое «патч» (patch) в сфере информационной безопасности? А) Вид хакерской атаки на компьютер Б) Уязвимость в программе, которую нашли хакеры В) Файл с логами (журнал событий) системы Г) Обновление программы, которое исправляет найденную уязвимость или ошибку Правильный ответ: Г Вопрос 6. Почему доменное имя google.com считается подозрительным? А) Это официальный домен компании Google Б) Домен слишком короткий В) Домен использует защищённое соединение HTTPS Г) Это фишинговый домен: вместо буквы «о» использована	Правильный ответ: А Вопрос 5. Что такое дипфейк (deepfake)? А) Глубокая нейронная сеть для обработки данных Б) Ложная новость, распространяемая в интернете В) Ложный аккаунт в социальной сети Г) Видео, аудио или изображение, созданное с помощью искусственного интеллекта, на котором один человек изображён как другой (например, подделка голоса или лица) Правильный ответ: Г Вопрос 6. Что такое анализ аномалий в информационной безопасности? А) Поиск отклонений от нормального поведения — например, обнаружение подозрительных действий пользователя, необычного сетевого трафика или странных запросов к базе данных Б) Шифрование данных для защиты от взлома В) Кэширование — сохранение часто используемых данных для быстрого доступа Г) Сжатие данных для уменьшения размера файлов Правильный ответ: А
--	--	---	--

	соцсетей, сайтов, новостей В) Специальная операционная система для хакеров Г) Протокол защищённой передачи данных Правильный ответ: Б Вопрос 7. Задание с несколькими правильными ответами. Выберите все верные варианты. Какие из перечисленных специалистов относятся к основным ролям в информационной безопасности? ☐ Пентестер (этичный хакер) ☐ Защитник (defender) ☐ Аналитик ИБ ☐ Менеджер проектов Правильные ответы: Пентестер, Защитник, Аналитик ТРЕНАЖЁРЫ КОДА Вопрос 8 Напишите функцию, которая принимает список ролей и	сообщения из файла-контейнера В) Пароль для входа в систему Г) Хеш-сумма файла Правильный ответ: Б Вопрос 7. Задание с несколькими правильными ответами. Выберите все верные варианты. Какие из перечисленных алгоритмов являются симметричными (используют один и тот же ключ для шифрования и расшифровки)? ☐ AES (Advanced Encryption Standard) ☐ DES (Data Encryption Standard) ☐ RSA (алгоритм с открытым ключом) ☐ ECC (Elliptic Curve Cryptography — алгоритм с открытым ключом) Правильные ответы: AES, DES ТРЕНАЖЁРЫ КОДА Вопрос 8 Напишите функцию, которая проверяет письмо на признаки фишинга. Шаблон кода:	цифра «0», чтобы обмануть пользователя и выдать себя за google.com Правильный ответ: Г Вопрос 7. Задание с несколькими правильными ответами. Выберите все верные варианты. Какие из перечисленных методов помогают защитить программу от SQL-инъекций (внедрения вредоносного кода в запросы к базе данных)? ☐ Параметризованные запросы (данные и команды передаются отдельно) ☐ Санитизация (очистка ввода от опасных символов) ☐ Конкатенация строк (склеивание строк) ☐ Экранирование (замена спецсимволов на безопасные) Правильные ответы: Параметризованные запросы, Санитизация, Экранирование ТРЕНАЖЁРЫ КОДА Вопрос 8 Напишите функцию, которая парсит HTTP-ответ и извлекает статус. Шаблон кода: <pre>def parse_http_response(response_text):</pre>	Вопрос 7. Задание с несколькими правильными ответами. Выберите все верные варианты. Большие языковые модели (LLM) могут быть уязвимы к специальным атакам. Какие из перечисленных атак направлены именно на обман языковых моделей? ☐ Prompt injection (внедрение вредоносной инструкции в запрос, чтобы модель выполнила опасное действие) ☐ Jailbreak (взлом защиты модели, чтобы заставить её игнорировать ограничения и отвечать на запрещённые вопросы) ☐ Атака на сеть (DDoS-атака на серверы — это не специфично для LLM) ☐ DDoS-атака (перегрузка сервера запросами — это общая сетевая атака, не специфичная для ИИ) Правильные ответы: Prompt injection, Jailbreak ТРЕНАЖЁРЫ КОДА Вопрос 8 Напишите функцию, которая проверяет промпт на признаки инъекции. Шаблон кода: <pre>def check_prompt_injection(prompt): # TODO: напишите код pass</pre>
--	---	---	---	--

	возвращает количество уникальных ролей. Шаблон кода: def count_roles(roles): # TODO: напишите код pass Данное поле предназначено для вашего кода: ЭТАЛОННОЕ РЕШЕНИЕ: def count_roles(roles): return len(set(roles)) Вопрос 9 Напишите функцию, которая классифицирует угрозы по типу. Шаблон кода: def classify_threat(threat_type): # TODO: напишите код pass Данное поле предназначено для вашего кода: ЭТАЛОННОЕ РЕШЕНИЕ: def classify_threat(threat_type):	def check_phishing_email(sender, subject, body): # TODO: напишите код pass Данное поле предназначено для вашего кода: ЭТАЛОННОЕ РЕШЕНИЕ: def check_phishing_email(sender, subject, body): suspicious_domains = ['fake.com', 'phish.net'] urgent_words = ['срочно', 'urgent', 'немедленно'] score = 0 if any(domain in sender for domain in suspicious_domains): score += 1 if any(word in subject.lower() for word in urgent_words): score += 1 if len(sender) > 50: score += 1 return 'suspicious' if score >= 2 else 'safe' Вопрос 9	# TODO: напишите код pass Данное поле предназначено для вашего кода: ЭТАЛОННОЕ РЕШЕНИЕ: def parse_http_response(response_text): lines = response_text.split('\n') if lines: first_line = lines[0] parts = first_line.split(' ') if len(parts) >= 2: return int(parts[1]) return None Вопрос 9 Напишите функцию, которая принимает URL как строку и проверяет наличие подозрительных паттернов Шаблон кода: def check_url(url): # TODO: напишите код pass Данное поле предназначено для вашего кода: ЭТАЛОННОЕ РЕШЕНИЕ: import re def check_url(url): suspicious = [] if re.search(r'd{1,3}\.d{1,3}\.d{1,3}\.d{1,3}', url):	Данное поле предназначено для вашего кода: ЭТАЛОННОЕ РЕШЕНИЕ: def check_prompt_injection(prompt): dangerous_patterns = ['ignore previous', 'disregard', 'override', 'system prompt'] return any(p in prompt.lower() for p in dangerous_patterns) Вопрос 9 Напишите функцию, которая находит аномалии в наборе данных. Шаблон кода: def analyze_anomalies(data_points): # TODO: напишите код pass Данное поле предназначено для вашего кода: ЭТАЛОННОЕ РЕШЕНИЕ: def analyze_anomalies(data_points): if not data_points: return [] avg = sum(data_points) / len(data_points) threshold = avg * 2 return [x for x in data_points if x > threshold] Вопрос 10 Напишите функцию, которая рассчитывает вклад участника. Шаблон кода:
--	---	--	--	--

	threats = {'hacker': 'attacker'} return threats.get(threat_type, 'unknown') Вопрос 10 Напишите функцию, которая проверяет срок NDA. Шаблон кода: def check_nda(days): # TODO: напишите код pass Данное поле предназначено для вашего кода: ЭТАЛОННОЕ РЕШЕНИЕ: def check_nda(days): return 'valid' if days <= 90 else 'expired' Вопрос 11 Напишите функцию, которая извлекает номера статей из НПА. Шаблон кода: def parse_articles(text): # TODO: напишите код pass Данное поле предназначено для вашего кода:	Напишите функцию, которая извлекает домен из email. Шаблон кода: def extract_domain(email): # TODO: напишите код pass Данное поле предназначено для вашего кода: ЭТАЛОННОЕ РЕШЕНИЕ: def extract_domain(email): if '@' in email: return email.split('@')[1] return None Вопрос 10 Напишите функцию, которая шифрует сущность XOR операцией. Шаблон кода: def xor_cipher(text, key): # TODO: напишите код pass Данное поле предназначено для вашего кода: ЭТАЛОННОЕ РЕШЕНИЕ: def xor_cipher(text, key): result = [] for i, char in enumerate(text):	suspicious.append('ip_in_url') if url.count('@') > 1: suspicious.append('multiple_at') known = ['google.com', 'yandex.ru', 'vk.com'] for k in known: if k.replace('o', '0') in url or k.replace('e', '3') in url: suspicious.append('typo') return suspicious Вопрос 10 Напишите функцию, которая находит IP с количеством неуспешных входов >= threshold. Шаблон кода: def find_suspicious_ips(log_entries, threshold): # TODO: напишите код pass Данное поле предназначено для вашего кода: ЭТАЛОННОЕ РЕШЕНИЕ: def find_suspicious_ips(log_entries, threshold): ip_counts = {} for entry in log_entries: if 'failed' in entry.lower(): parts = entry.split(',') ip = parts[0].strip() if parts else None if ip:	def calculate_individual_contribution(team_results, member_id): # TODO: напишите код pass Данное поле предназначено для вашего кода: ЭТАЛОННОЕ РЕШЕНИЕ: def calculate_individual_contribution(team_results, member_id): member = team_results.get(member_id, {}) findings = member.get('findings_count', 0) fixes = member.get('fixes_count', 0) docs = member.get('documentation_score', 0) total = findings * 3 + fixes * 2 + docs return {'member_id': member_id, 'contribution_score': total} Вопрос 11 Напишите функцию, которая проверяет код на соответствие принципам безопасности. Шаблон кода: def validate_code_security(code): # TODO: напишите код pass Данное поле предназначено для вашего кода:
--	---	---	--	--

	ЭТАЛОННОЕ РЕШЕНИЕ: <pre>def parse_articles(text): import re return re.findall(r'ct\.s*(\d+)', text)</pre> Вопрос 12 Напишите функцию, которая извлекает домены из URL. Шаблон кода: <pre>def extract_domains(urls): # TODO: напишите код</pre> pass Данное поле предназначено для вашего кода: ЭТАЛОННОЕ РЕШЕНИЕ: <pre>def extract_domains(urls): domains = [] for url in urls: if '://' in url: domain = url.split('://')[1].split('/')[0]</pre> domains.append(domain) return domains Вопрос 13	<pre>result.append(chr(ord(char) ^ ord(key[i % len(key)]))) return ".join(result)</pre> Вопрос 11 Напишите функцию, которая шифрует текст шифром Цезаря. Шаблон кода: <pre>def caesar_encrypt(text, shift): # TODO: напишите код</pre> pass Данное поле предназначено для вашего кода: ЭТАЛОННОЕ РЕШЕНИЕ: <pre>def caesar_encrypt(text, shift): result = [] for char in text: if char.isalpha(): base = ord('A') if char.isupper() else ord('a') result.append(chr((ord(char) - base + shift) % 26 + base)) else: result.append(char) return ".join(result)</pre> Вопрос 12 Напишите функцию, которая вычисляет MD5 хеш текста.	<pre>ip_counts[ip] = ip_counts.get(ip, 0) + 1 return [ip for ip, count in ip_counts.items() if count >= threshold]</pre> Вопрос 11 Напишите функцию, которая читает CSV-строки с логами и подсчитывает успешные и неуспешные входы. Шаблон кода: <pre>def count_logins_from_csv(csv_lines): # TODO: напишите код</pre> pass Данное поле предназначено для вашего кода: ЭТАЛОННОЕ РЕШЕНИЕ: <pre>def count_logins_from_csv(csv_lines): success = 0 failed = 0 for line in csv_lines: if 'success' in line.lower(): success += 1 elif 'failed' in line.lower() or 'error' in line.lower(): failed += 1 return {'success': success, 'failed': failed}</pre> Вопрос 12	ЭТАЛОННОЕ РЕШЕНИЕ: <pre>def validate_code_security(code): checks = { 'input_validation': 'sanitize' in code.lower() or 'validate' in code.lower(), 'error_handling': 'try' in code and 'except' in code, 'logging': 'log' in code.lower(), 'no_hardcoded': 'password' not in code.lower() or '=' not in code } score = sum(1 for v in checks.values() if v) return {'checks': checks, 'score': score, 'total': len(checks)}</pre> Вопрос 12 Напишите функцию, которая ищет типовые уязвимости в коде. Шаблон кода: <pre>def find_vulnerabilities(code): # TODO: напишите код</pre> pass Данное поле предназначено для вашего кода: ЭТАЛОННОЕ РЕШЕНИЕ: <pre>def find_vulnerabilities(code): vulnerabilities = [] if 'SELECT * FROM' in code and '+' in code: vulnerabilities.append('SQL_injection')</pre>
--	---	---	---	--

	Напишите функцию, которая подсчитывает IP. Шаблон кода: <pre>def count_unique_ips(ip_list): # TODO: напишите код pass</pre> Данное поле предназначено для вашего кода: ЭТАЛОННОЕ РЕШЕНИЕ: <pre>def count_unique_ips(ip_list): return len(set(ip_list))</pre> Вопрос 14 Напишите функцию, которая проверяет email. Шаблон кода: <pre>def validate_email(email): # TODO: напишите код pass</pre> Данное поле предназначено для вашего кода: ЭТАЛОННОЕ РЕШЕНИЕ <pre>f validate_email(email):</pre>	Шаблон кода: <pre>def calculate_md5(text): # TODO: напишите код pass</pre> Данное поле предназначено для вашего кода: ЭТАЛОННОЕ РЕШЕНИЕ: <pre>import hashlib def calculate_md5(text): return hashlib.md5(text.encode()).hexdigest()</pre> Вопрос 13 Напишите функцию, которая проверяет целостность данных. Шаблон кода: <pre>def verify_integrity(data, expected_hash): # TODO: напишите код pass</pre> Данное поле предназначено для вашего кода: ЭТАЛОННОЕ РЕШЕНИЕ: <pre>import hashlib def verify_integrity(data, expected_hash):</pre>	Напишите функцию, которая строит параметризованный SQL-запрос из шаблона и словаря параметров. Шаблон кода: <pre>def build_safe_query(template, params): # TODO: напишите код pass</pre> Данное поле предназначено для вашего кода: ЭТАЛОННОЕ РЕШЕНИЕ: <pre>def build_safe_query(template, params): query = template for key, value in params.items(): query = query.replace(f'{{key}}', str(value)) return query</pre> Вопрос 13 Напишите функцию, которая экранирует опасные HTML-символы в пользовательском вводе. Шаблон кода: <pre>def sanitize_html_input(user_input): # TODO: напишите код pass</pre> Данное поле предназначено для вашего кода: ЭТАЛОННОЕ РЕШЕНИЕ:	<pre>if 'innerHTML' in code or 'eval(' in code: vulnerabilities.append('XSS') if 'password' in code.lower() and '=' in code: vulnerabilities.append('hardcoded_password') return vulnerabilities</pre> Вопрос 13 Напишите функцию, которая анализирует текст на признаки генерации ИИ Шаблон кода: <pre>def detect_ai_text(text): # TODO: напишите код pass</pre> Данное поле предназначено для вашего кода: ЭТАЛОННОЕ РЕШЕНИЕ: <pre>def detect_ai_text(text): ai_patterns = ['в заключение', 'важно отметить', 'следует учитывать'] score = sum(1 for p in ai_patterns if p in text.lower()) return 'likely_ai' if score >= 2 else 'likely_human'</pre> Вопрос 14 Напишите функцию, которая ищет признаки лжи в метаданных видео. Шаблон кода:
--	--	---	---	---

	return '@' in email and len(email) > 5 Вопрос 15 Напишите функцию, которая генерирует 6-значный OTP код. Шаблон кода: <pre>def generate_otp(): # TODO: напишите код pass</pre> Данное поле предназначено для вашего кода: ЭТАЛОННОЕ РЕШЕНИЕ: <pre>import secrets def generate_otp(): return str(secrets.randbelow(900000) + 100000)</pre>	<pre>actual_hash = hashlib.sha256(data.encode()).hexdigest() return actual_hash == expected_hash</pre> Вопрос 14 Напишите функцию, которая извлекает метаданные из имени файла. Шаблон кода: <pre>def extract_metadata(filename): # TODO: напишите код pass</pre> Данное поле предназначено для вашего кода: ЭТАЛОННОЕ РЕШЕНИЕ: <pre>def extract_metadata(filename): metadata = {} if '.' in filename: metadata['extension'] = filename.split('.')[-1] metadata['name'] = filename.split('.')[0] metadata['length'] = len(filename) return metadata</pre> Вопрос 15 Тема 2.5	<pre>def sanitize_html_input(user_input): return (user_input .replace('&', '&amp;') .replace('<', '&lt;') .replace('>', '&gt;') .replace('"', '&quot;') .replace("'", '&#x27;'))</pre> Вопрос 14 Напишите функцию, которая извлекает флаг формата flag{...} из текста. Шаблон кода: <pre>def parse_ctf_flag(text): # TODO: напишите код pass</pre> Данное поле предназначено для вашего кода: ЭТАЛОННОЕ РЕШЕНИЕ: <pre>import re def parse_ctf_flag(text): match = re.search(r'flag\{([^\}]+\)}', text) return match.group(1) if match else None</pre> Вопрос 15 Напишите функцию, которая ищет подозрительные паттерны в URL. Шаблон кода: <pre>def analyze_url_patterns(url): # TODO: напишите код pass</pre>	<pre>def analyze_deepfake_indicators(video_ metadata): # TODO: напишите код pass</pre> Данное поле предназначено для вашего кода: ЭТАЛОННОЕ РЕШЕНИЕ: <pre>def analyze_deepfake_indicators(video_ metadata): indicators = [] if 'fps' in video_metadata and video_metadata['fps'] < 24: indicators.append('low_fps') if 'resolution' in video_metadata: w, h = video_metadata['resolution'] if w % 2 != 0 or h % 2 != 0: indicators.append('odd_resolution') return indicators</pre> Вопрос 15 Напишите функцию, которая генерирует отчёт по найденным уязвимостям. Шаблон кода: <pre>def generate_audit_report(findings): # TODO: напишите код pass</pre> Данное поле предназначено для вашего кода: ЭТАЛОННОЕ РЕШЕНИЕ: <pre>def generate_audit_report(findings): report = {</pre>
--	--	--	--	--

		Напишите функцию, которая генерирует токен. Шаблон кода: <pre>def generate_session_token(use r_id): # TODO: напишите код pass</pre> Данное поле предназначено для вашего кода: ЭТАЛОННОЕ РЕШЕНИЕ: <pre>import secrets def generate_session_token(use r_id): token = secrets.token_hex(16) return f"{user_id}_{token}"</pre>	Данное поле предназначено для вашего кода: ЭТАЛОННОЕ РЕШЕНИЕ: <pre>import re def analyze_url_patterns(url): findings = [] if re.search(r'd{1,3}\.d{1,3}\.d{1,3}\.d{1,3}', url): findings.append('ip_instead_of_domain') known = ['google.com', 'yandex.ru', 'vk.com'] for k in known: typo = k.replace('o', '0').replace('e', '3') if typo in url: findings.append(f'typo_of_{k}') if url.count('@') > 1: findings.append('multiple_at_signs') return findings</pre>	<pre>'total_findings': len(findings), 'critical': sum(1 for f in findings if f.get('severity') == 'critical'), 'high': sum(1 for f in findings if f.get('severity') == 'high'), 'medium': sum(1 for f in findings if f.get('severity') == 'medium'), 'recommendations': [f['recommendation'] for f in findings] } return report</pre>
Аттестация по итогам модуля. Описание процедуры оценивания Показатели и критерии оценивания	Критерий оценивания: для тестовой части – правильность ответа на тестовый вопрос; для практико-ориентированных заданий – правильность работы программы. Показатели оценивания: для	Критерий оценивания: для тестовой части – правильность ответа на тестовый вопрос; для практико-ориентированных заданий – правильность работы программы. Показатели оценивания: для тестовой части – количество	Критерий оценивания: для тестовой части – правильность ответа на тестовый вопрос; для практико-ориентированных заданий – правильность работы программы. Показатели оценивания: для тестовой части – количество правильных ответов на тестовые задания; для практико-ориентированных	Критерий оценивания: для тестовой части – правильность ответа на тестовый вопрос; для практико-ориентированных заданий – правильность работы программы. Показатели оценивания: для тестовой части – количество правильных ответов на тестовые задания; для практико-ориентированных заданий –

	тестовой части – количество правильных ответов на тестовые задания; для практико-ориентированных заданий – количество заданий, в которых программа работает правильно. За каждый правильный ответ/правильно выполненное практико-ориентированное задание начисляется 1 балл. В случае неправильного ответа/неправильно выполненное практико-ориентированное задание баллы не начисляются.	правильных ответов на тестовые задания; для практико-ориентированных заданий – количество заданий, в которых программа работает правильно. За каждый правильный ответ/правильно выполненное практико-ориентированное задание начисляется 1 балл. В случае неправильного ответа/неправильно выполненное практико-ориентированное задание баллы не начисляются.	заданий – количество заданий, в которых программа работает правильно. За каждый правильный ответ/правильно выполненное практико-ориентированное задание начисляется 1 балл. В случае неправильного ответа/неправильно выполненное практико-ориентированное задание баллы не начисляются.	количество заданий, в которых программа работает правильно. За каждый правильный ответ/правильно выполненное практико-ориентированное задание начисляется 1 балл. В случае неправильного ответа/неправильно выполненное практико-ориентированное задание баллы не начисляются.
Аттестация по итогам модуля. Шкала оценивания, нижнее значение	0	0	0	0
Аттестация по итогам модуля. Шкала оценивания, верхнее значение	15	15	15	15

Аттестация по итогам модуля. Шкала оценивания, минимальный проходной балл для успешной сдачи	8	8	8	8
--	---	---	---	---

5.3 Итоговый контроль

Итоговый контроль. Количество академических часов	1
Итоговый контроль. Формы контроля	Комплексное задание: тест и защита проекта. Итоговый контроль не входит в 4 модуль (является отдельным элементом ДОП).
Итоговый контроль. Диагностические инструменты	Комплект заданий: тестовые вопросы и процедура защиты проекта
Итоговый контроль. Показатели и критерии оценивания	Показатели и критерии (с весами) оценивания: Этап 1. Тестирование Тестовая часть итогового контроля выполняется и проверяется автоматизированно на Образовательной платформе. Каждый верный ответ оценивается в 1 балл, неверный или отсутствующий — 0 баллов. Максимальный балл 1 этапа – 10 Минимальный пороговый балл – 5 Этап 2. Защита проекта (с презентацией) Критерии и веса внутри проектной части (каждый критерий оценивается членами комиссии по шкале от 0 до 10): 1. Содержательная часть (качество продукта, глубина проработки) - вес 0,7 0 – 4 - Код работает с ошибками или не запускается. Реализована только часть заявленной функциональности (менее 50% функций). Отсутствуют ключевые функции. Нарушены требования безопасности. Код нечитаем: отсутствуют комментарии, осмысленные имена переменных, логическая структура. Не обработаны ошибки и граничные случаи. Описание проекта отсутствует или содержит минимум информации. Проект не демонстрирует понимания темы. 5 – 7 – Код запускается и выполняет основные функции без критических ошибок. Реализованы все минимально необходимые функции для проекта. Соблюдены базовые требования безопасности. Код в целом читаем, но есть замечания к структуре или именованию переменных. Обработаны основные ошибки, но не все граничные случаи. Описание проекта присутствует, содержит описание проекта и примеры использования. Проект демонстрирует базовое понимание темы и способность применить изученные инструменты. Структура проекта логична, но без дополнительных улучшений. 8 – 10 - Код работает без ошибок, все функции выполняют заявленную функциональность корректно. Реализованы все заявленные функции + дополнительные улучшения. Строго соблюдены требования безопасности. Код читаемый: осмысленные имена переменных, логическая структура, отступы, комментарии к функциям и ключевым блокам. Полностью обработаны ошибки и граничные случаи

	(программа корректно работает при любом вводе). Описание проекта содержит инструкции по запуску, примеры использования. Проект демонстрирует глубокое понимание темы, творческий подход и способность применять знания на практике. Структура проекта логична и соответствует лучшим практикам разработки. Обучающийся уверенно отвечает на технические вопросы и обосновывает принятые решения. 2. Визуальное оформление презентации - вес 0,3 0 – 4 - Слайды перегружены текстом; нет единого стиля; шрифты нечитаемы; изображения низкого качества; есть ошибки в оформлении. 5 – 7 – Текст и графика сбалансированы; единый стиль прослеживается; информация структурирована; визуализация данных присутствует. 8 – 10 - Дизайн эстетичный и функциональный; все визуальные элементы работают на раскрытие темы. Максимальный балл 2 этапа – 10 Минимальный пороговый балл – 6 Алгоритм расчета оценки/балла итогового контроля по ДОП Итоговый показатель аттестации рассчитывается в 20-балльной шкале как сумма результатов обоих этапов: Максимально возможное значение: 20 баллов
Итоговый контроль. Примеры заданий	Вариант 1 1. Тест. Ответьте на тестовые вопросы, выбрав один из предложенных вариантов ответа. В отдельных вопросах нужно будет ввести свой ответ в поле для ответа. Вопрос 1. Как убедиться, что скачанный файл не был повреждён или подменён при загрузке? А) Вычислить его «цифровой отпечаток» (хеш) и сравнить с хешем, указанным на официальном сайте Б) Проверить дату создания файла В) Открыть файл в текстовом редакторе и посмотреть содержимое Г) Сравнить размер файла с размером оригинала Правильный ответ: А Вопрос 2. Какой способ защиты от SQL-инъекций (внедрения вредоносного кода в запросы к базе данных) считается самым надёжным? А) Проверять длину введенной строки Б) Запрещать использование определённых SQL-слов (SELECT, DROP и т.д.) В) Использовать параметризованные запросы — когда данные и команды передаются отдельно Г) Вручную заменять кавычки и другие спецсимволы на безопасные Правильный ответ: В

	Вопрос 3. Злоумышленник пытается подобрать короткий PIN-код (например, из 4 цифр) методом грубой силы — перебором всех возможных комбинаций. Какая защита будет самой эффективной? А) Зашифровать базу данных с PIN-кодами Б) Добавить CAPTCHA (защиту от роботов) В) Блокировать доступ после нескольких неудачных попыток ввода Г) Увеличить сложность самого PIN-кода Правильный ответ: В Вопрос 4. Задание с кратким ответом. Впишите только число. Сколько основных ролей специалистов в области информационной безопасности рассматривается в курсе (пентестер, защитник, аналитик)? Ответ: _____ Правильный ответ: 3 Вопрос 5. Что такое инцидент информационной безопасности? А) Сотрудник сменил свой пароль на новый Б) Администратор установил новый сервер в офисе В) Плановое обновление антивируса на компьютерах Г) Происшествие, при котором нарушена конфиденциальность (утечка данных), целостность (данные изменены) или доступность (данные недоступны) информации Правильный ответ: Г Вопрос 6. Задание с кратким ответом. Впишите только число. Сколько уровней опасности обычно определяет программа-анализатор при проверке подозрительного email-сообщения (например: низкий, средний, высокий)? Ответ: _____ Правильный ответ: 3 Вопрос 7. В чём главное отличие шифрования от кодирования (например, Base64)? А) Кодирование — более сложный процесс, чем шифрование Б) Шифрование можно расшифровать, а кодирование — нет В) Для шифрования нужен секретный ключ, а для кодирования ключ не нужен — декодировать может кто угодно Г) Разницы нет, это одно и то же Правильный ответ: В Вопрос 8. Какой федеральный закон в России регулирует защиту персональных данных граждан (имя, паспорт, телефон и т.д.)? А) Федеральный закон № 152-ФЗ «О персональных данных»
--	---

	Б) Федеральный закон № 98-ФЗ «О коммерческой тайне» В) Федеральный закон № 187-ФЗ «О безопасности критической информационной инфраструктуры» Г) Федеральный закон № 149-ФЗ «Об информации, информационных технологиях и о защите информации» Правильный ответ: А Вопрос 9. Что такое «китовая охота» в контексте фишинга? А) Массовая атака на обычных пользователей интернета Б) Рассылка спама миллионам людей В) Атака на серверы и оборудование компании Г) Целевая атака на руководителей компании, директоров и других важных персон Правильный ответ: Г Вопрос 10. Какой этап является первым в стандартной модели кибератаки (перед тем как взломать систему)? А) Достижение цели (кража данных, шифрование файлов) Б) Проникновение в систему (взлом пароля, использование уязвимости) В) Сбор информации о цели (разведка): поиск данных о компании, сотрудниках, технологиях Г) Закрепление в системе (создание бэкдора для повторного доступа) Правильный ответ: В 2. Защита проекта. Представьте с использованием презентационных материалов результаты проектной работы на курсе. Полный комплект оценочных материалов (7 вариантов заданий) представлен в документе «Оценочные материалы для проведения итогового контроля» в составе УМК в приложении к ДОП.
Итоговый контроль. Шкала оценивания, нижнее значение	0
Итоговый контроль. Шкала оценивания, верхнее значение	20
Итоговый контроль. Шкала оценивания, минимальный проходной балл	11

6. Организационно-педагогические условия

6.1 Методическое обеспечение: методы, формы и технологии, применяемые при реализации программы

Методы обучения: модульный, проблемный и контекстный подходы.

Формы занятий: лекции с демонстрацией мультимедийных материалов, практические работы, самостоятельная работа.

Технологии: традиционные (объяснительно-иллюстративные) и интерактивные (групповые обсуждения, решение кейсов).

6.2 Материально-техническое обеспечение

Наименование требуемого оборудования и программного обеспечения:

Рабочее место обучающегося: оборудование и мебель, необходимые для обучения, включая расходные материалы.

Рабочее место педагога: оборудование (включая демонстрационное) и мебель.

Иное оборудование и мебель.

Сетевое оборудование и подключение к сети Интернет.

Программное обеспечение.

Средства индивидуальной защиты и охраны труда.

Зонирование площадки.

Компьютер/ноутбук

Windows/Linux (не ранее 2020)

Интернет от 2 Мбит/сек

Веб-браузер (не ранее 2020)

Микрофон, наушники и колонки

Клавиатура, мышь

Проектор/интерактивная доска

7. Учебно-методические материалы

Ниже представлен перечень методических разработок и материалов для обучения:

Методические разработки

Пакет методических разработок содержит:

- Методическую разработку «Материалы для преподавателя по проведению практических занятий».
- Методическую разработку «Материалы для преподавателя по организации самостоятельной работы и самоконтроля/самопроверки».
- Оценочные материалы текущего контроля и промежуточной аттестации.
- Оценочные материалы для проведения итогового контроля по ДОП

Материалы для обучения

Пакет материалов модуля содержит:

- Презентации для теоретических занятий.
- Презентации для практических занятий.
- Описание практических заданий.
- Задания для самоконтроля (самопроверки).
- Задания для самостоятельной работы.
- Задания системы контроля: текущего контроля, промежуточной аттестации.

8. Перечень источников информационного сопровождения (учебная литература и др.)

Учебная литература:

1. Солдатова Г. У., Чигарькова С. В., Пермькова И. Д. Кибербезопасность: учебник для 8 класса общеобразовательных организаций. — Москва: Русское Слово, 2025. — 80 с. — ISBN 978-5-533-01920-0.

2. Солдатова Г. У., Чигарькова С. В., Пермякова И. Д. Кибербезопасность: учебник для 9 класса общеобразовательных организаций. — Москва: Русское Слово, 2025. — 112 с. — ISBN 978-5-533-01921-7.
3. Цветкова М. С., Хлобыстова И. Ю. Информационная безопасность. Кибербезопасность. 7–9 классы: учебник. — Москва: Просвещение, 2021. — 64 с. — (Инженерная и IT-подготовка школьников). — ISBN 978-5-09-085308-8.
4. Музагафаров А. Шифрованный мир. Азы криптографии и задачи по криптоанализу. — Ridero, 2022. — 156 с. — ISBN 978-5-00602725-1.
5. Хренников Б., Льяная Л., Гололобов Н. Кибербезопасность: учебное пособие для 8 класса. — Москва: Просвещение, 2022. — 96 с. — ISBN 978-5-09-098765-4.

Электронные информационные ресурсы:

1. Портал «КиберЗОЖ» <https://киберзож.рф>
2. Образовательная платформа по Python <https://pythonist.ru/>

Директор Центра компетенций
«Цифровая экономика»



Н.Ю. Сурова