Муниципальное автономное общеобразовательное учреждение города Новосибирска
«Лицей №22 «Надежда Сибири»
Главный корпус на Советской: г. Новосибирск, ул. Советская, 63, тел. 222-35-15,
e-mail: l_22@edu54.ru
Корпус 99 на Чаплыгина: г. Новосибирск, ул. Чаплыгина, 59, тел. 223-74-15

РАССМОТРЕНО на заседании инженерной кафедры протокол № 1 от 25.08.2025 Кириленко К.А. *ФИО руководителя кафедры*	СОГЛАСОВАНО Заместитель директора Н.А.Данилова от 29.08.2025

РАБОЧАЯ ПРОГРАММА

Информатика. Информационная безопасность

10 «ИП» , 11 «ИП» класса

(уровень среднего общего образования)

Разработчик:

Кириленко Ксения Алексеевна

2025

Рабочая программа по учебному предмету «Информатика. Информационная безопасность» (предметная область «Математика и информатика») (далее соответственно – программа по информационной безопасности) составлена на основе Федеральной рабочей программы по информатике и является авторской, включает пояснительную записку, содержание обучения, планируемые результаты освоения программы по информационной безопасности

Пояснительная записка отражает общие цели и задачи изучения искусственного интеллекта, место в структуре учебного плана, а также подходы к отбору содержания, к определению планируемых результатов.

Содержание обучения раскрывает содержательные линии, которые предлагаются для обязательного изучения в 10 и 11 классе на уровне среднего общего образования.

Планируемые результаты освоения программы по моделированию физических процессов включают личностные, метапредметные результаты за период обучения в 10 и 11 классе на уровне среднего общего образования, а также предметные достижения обучающегося.

1. Пояснительная записка

Информационная безопасность представляет собой критически важную дисциплину в современном цифровом обществе, объединяющую технические знания, правовые нормы и управленческие подходы для защиты данных, систем и инфраструктуры от внутренних и внешних угроз. Изучение основ информационной безопасности в школе открывает учащимся возможность не просто использовать цифровые технологии, а понимать принципы их защищенного функционирования, развивая глубокое осознание рисков цифровой среды и практические навыки противодействия им, востребованные на рынке труда.

Функциональная значимость предмета для школьников заключается в освоении комплексного инструментария для обеспечения кибербезопасности на различных уровнях, включая такие фундаментальные концепции, как конфиденциальность, целостность и доступность данных (триада CIA), криптографические методы защиты информации, принципы аутентификации и авторизации, а также основы сетевой безопасности. Эти знания переводят абстрактные представления о киберугрозах в конкретные и прикладные навыки защиты, позволяя решать практические задачи — от обеспечения безопасности личных аккаунтов и данных до понимания принципов защиты корпоративных сетей и критической информационной инфраструктуры.

Знание принципов информационной безопасности и умение их применять важно для каждого школьника, стремящегося стать грамотным и ответственным цифровым гражданином. Понимание того, как злоумышленники осуществляют атаки (социальная инженерия, фишинг, malware), как работают механизмы защиты (шифрование, брандмауэры, антивирусы) и как выстраивать политики безопасности, помогает учащимся развивать критическое, аналитическое и прогностическое мышление, а также способность к построению многоуровневых систем защиты.

Дисциплина информационной безопасности, выполняя свои основные функции, позволяет учащимся абстрагироваться от узкотехнического подхода и сосредоточиться на комплексном видении проблемы, рассматривая ее в триаде "технологии — люди — процессы". Она предоставляет системный каркас для анализа угроз, оценки уязвимостей и выбора контрмер, что дает возможность сосредоточиться на управлении рисками, разработке политик безопасности и формировании культуры безопасного поведения, что является ключевым этапом в любой профессиональной деятельности, связанной с IT.

Обучение информационной безопасности направлено на развитие интеллектуальных и технических способностей учащихся, включая умение идентифицировать и классифицировать угрозы, проводить анализ рисков, применять базовые методы криптографии, настраивать параметры безопасности операционных систем и сетевых устройств и реагировать на инциденты. Это способствует развитию правового сознания, этичного подхода к использованию цифровых технологий, навыков расследования инцидентов и работы с нормативной документацией, что является crucial для успешной адаптации в цифровом мире и дальнейшей карьеры в качестве специалиста по безопасности, аудитора или руководителя.

Содержание программы по информационной безопасности ориентировано также на развитие функциональной грамотности учащихся, включая умение оценивать достоверность информации и источников, противостоять манипуляциям в сети, защищать свою цифровую репутацию, применять полученные знания для обеспечения личной и профессиональной безопасности в повседневной жизни, расширяя тем самым свои возможности для уверенной и ответственной деятельности в цифровом пространстве.

Цели и задачи изучения учебного предмета «Информационная безопасность».

Изучение предмета «Информационная безопасность» направлено на достижение следующих целей:

- Формирование системного понимания комплексного подхода к защите информации как основы устойчивого функционирования любого современного субъекта (личности, организации, государства), связывающего теоретические знания о природе угроз и уязвимостей с практическими навыками реализации защитных механизмов и политик.
- Развитие компетенций в области выявления, анализа и нейтрализации киберугроз, включающих проведение аудита защищенности, применение криптографических методов, настройку систем контроля доступа и противодействие современным атакам, с использованием как теоретических моделей, так и практического инструментария (например, Wireshark, Nmap, hashcat).
- Стимулирование интереса к исследовательской и проектной деятельности в сфере кибербезопасности через решение практических кейсов, участие в CTF-

соревнованиях (Capture The Flag) и разработку моделей систем защиты для учебных проектов.

Задачи изучения предмета:

- Развивать аналитическое и прогностическое мышление через процесс идентификации активов, оценки рисков, моделирования угроз и выбора адекватных мер защиты для конкретной информационной системы.
- Формировать навыки обеспечения безопасности на всех этапах жизненного цикла IT-продукта: от безопасной разработки (DevSecOps) и тестирования на проникновение (pen-testing) до расследования инцидентов и восстановления работоспособности после атаки.
- Воспитывать культуру безопасного поведения в цифровой среде, понимая важность использования надежных паролей, многфакторной аутентификации, шифрования данных и критической оценки информации на предмет фишинга и социальной инженерии.
- Развивать умение самостоятельно учиться: работать с отечественными и международными стандартами безопасности (например, ГОСТ Р ИСО/МЭК 27000, NIST CSF), анализировать актуальные угрозы по данным CERT-центров, искать решения и обмениваться знаниями в профессиональных сообществах и на специализированных платформах (Hack The Box, Cybrary).

Особенности классов

Рабочая программа по предмету «Информатика. Информационная безопасность» для 10-го «ИП» и 11-го «ИП» класса предназначена для углубленного изучения учащимися информационно-технологического профиля». На изучение данного модуля отведено 33 часа в 10-ом классе и 30 часов в 11-ом классе.

Место предмета в учебном плане лицея

Учебный план на изучение «Информатика. Информационная безопасность» в 10 «ИП» и 11 «ИП» классах среднего общего образования отводит 1 учебный час в неделю (всего 33 часа в 10 классе и 30 часов в 11 классе) за счёт части, формируемой участниками образовательных отношений.

Учебный год	Количество часов	
	10 «ИП»	11 «ИП»
2025/2026	33	30

К тематическому планированию применяется модульный принцип построения образовательной программы, что позволяет выстраивать индивидуальную образовательную парадигму и обеспечивать саморазвитие при индивидуальном темпе работы с учебным материалом, контроль и самоконтроль знаний.

Используемые образовательные технологии, в том числе дистанционные

Обучение искусственному интеллекту может осуществляться с использованием дистанционных образовательных технологий (далее ДОТ), которое предполагает как самостоятельное прохождение учебного материала учеником, так и с помощью сопровождения учителя. При применении ДОТ используются платформы: лицейская платформа дистанционного обучения Moodle, ФГИС «Моя школа», ГИС «Электронная школа» Новосибирской области.

При реализации рабочей программы могут быть использованы материалы для подготовки к профилям олимпиады КД НТИ и стандартов Всероссийского чемпионатного движения по профессиональному мастерству «Профессионалы».

Информация о промежуточной аттестации

Промежуточная аттестация осуществляется по окончании учебного модуля с целью проверки степени и качества усвоения материала по результатам изучения тематических модулей и проводится в форме аттестационных работ.

Текущий контроль осуществляются с целью проверки степени и качества усвоения материала в ходе его изучения в следующих формах: самостоятельных и проверочных работ.

Текущий контроль и промежуточная аттестация осуществляются в соответствии с «Положением об осуществлении текущего контроля успеваемости и промежуточной аттестации обучающихся, их формах, периодичности и порядке проведения муниципального автономного общеобразовательного учреждения города Новосибирска «Лицей № 22 «Надежда Сибири» (протокол педагогического совета №1 от 29.08.2023).

Итоговая аттестация проводится в соответствии с законодательством РФ.

Промежуточная аттестация по предмету «Информационная безопасность» в 10 «ИП» классе

№ модульной	**Название модуля**	**Количество часов в модуле**	**Номер урока ПА**	**Форма ПА**
МР № 1	Информационная безопасность	33	33	Практическая работа

Промежуточная аттестация по предмету «Информационная безопасность» в 11 «ИП» классе

№ модульной	**Название модуля**	**Количество часов в модуле**	**Номер урока ПА**	**Форма ПА**
МР № 1	Информационная безопасность	30	30	Практическая работа

2. Содержание учебного предмета

10 класс

Модуль 1 «Информационная безопасность»

Вводное занятие. Какие области ИБ и виды соревнований существуют? Введение в Linux. Часть I. Введение в Linux. Часть II. Как работают веб-сервисы. TCP/UDP, HTTP. Google dorking. Как работает поисковая система. LFI, Command injection. RCE (Remote Code Execution). Проведение соревнований. Часть I. Проведение соревнований. Часть II. Изучение баз данных. SQL. SQL-инъекции. Принципы ИБ. Значение данных и философия. Способы создания backdoor'ов в Linux. KillChain. Проведение полноценной атаки на примере машины с HTB. Образование и особенности обучения в сфере ИБ.

11 класс

Модуль 1 «Информационная безопасность»

Вводное занятие. Какие области ИБ и виды соревнований существуют? Введение в Linux. Часть I. Введение в Linux. Часть II. Как работают веб-сервисы. TCP/UDP, HTTP. Google dorking. Как работает поисковая система. LFI, Command injection. RCE (Remote Code Execution). Проведение соревнований. Часть I. Проведение соревнований. Часть II. Изучение баз данных. SQL. SQL-инъекции. Принципы ИБ. Значение данных и философия. Способы создания backdoor'ов в Linux. KillChain. Проведение полноценной атаки на примере машины с HTB. Образование и особенности обучения в сфере ИБ.

Планируемые образовательные результаты освоения учебного предмета Искусственный интеллект

Личностные результаты

1. сформированность мировоззрения, соответствующего современному уровню развития науки и техники;
2. готовность и способность к образованию, в том числе самообразованию, на протяжении всей жизни; сознательное отношение к непрерывному образованию как условию успешной профессиональной и общественной деятельности;
3. навыки сотрудничества со сверстниками, детьми младшего возраста, взрослыми в образовательной, учебно-исследовательской, проектной и других видах деятельности;
4. эстетическое отношение к миру, включая эстетику научного и технического творчества;

Метапредметные результаты:

1.2.5	Анализировать полученные в ходе решения задачи результаты, критически оценивать их достоверность, прогнозировать изменение в новых условиях
1.2.6	Уметь переносить знания в познавательную и практическую области жизнедеятельности; уметь интегрировать знания из разных предметных областей; осуществлять целенаправленный поиск переноса средств и способов действия в профессиональную среду
1.2.7	Способность и готовность к самостоятельному поиску методов решения практических задач, применению различных методов познания; ставить и формулировать собственные задачи в образовательной деятельности и жизненных ситуациях; ставить проблемы и задачи, допускающие альтернативные решения; выдвигать новые идеи, предлагать оригинальные подходы и решения; разрабатывать план решения проблемы с учетом анализа имеющихся материальных и нематериальных ресурсов
1.3	Работа с информацией
1.3.1	Владеть навыками получения информации из источников разных типов, самостоятельно осуществлять поиск, анализ, систематизацию и интерпретацию информации различных видов и форм представления
1.3.2	Создавать тексты в различных форматах с учетом назначения информации и целевой аудитории, выбирая оптимальную форму представления и визуализации
1.3.3	Оценивать достоверность, легитимность информации, ее соответствие правовым и морально-этическим нормам
1.3.4	Использовать средства информационных и коммуникационных технологий в решении когнитивных, коммуникативных и организационных задач с соблюдением требований эргономики, техники безопасности, гигиены, ресурсосбережения, правовых и этических норм, норм информационной безопасности
1.3.5	Владеть навыками распознавания и защиты информации, информационной безопасности личности
2	Коммуникативные УУД
2.1	Общение
2.1.1	Осуществлять коммуникации во всех сферах жизни; владеть различными способами общения и взаимодействия
2.1.2	Развернуто и логично излагать свою точку зрения с использованием языковых средств
2.1.3	Аргументированно вести диалог
3	
3.1	Самоорганизация
3.1.1	Самостоятельно осуществлять познавательную деятельность, выявлять проблемы, ставить и формулировать собственные задачи в образовательной деятельности и жизненных ситуациях; давать оценку новым ситуациям
3.1.2	Самостоятельно составлять план решения проблемы с учетом имеющихся ресурсов, собственных возможностей и предпочтений; делать осознанный выбор, аргументировать его, брать ответственность за решение; оценивать приобретенный опыт; способствовать формированию и проявлению широкой эрудиции в разных областях знаний
3.2	Самоконтроль

3.2.1	Давать оценку новым ситуациям, вносить коррективы в деятельность, оценивать соответствие результатов целям
3.2.2	Владеть навыками познавательной рефлексии как осознания совершаемых действий и мыслительных процессов, их результатов и оснований; использовать приемы рефлексии для оценки ситуации, выбора верного решения; уметь оценивать риски и своевременно принимать решения по их снижению
3.3	Эмоциональный интеллект, предполагающий сформированность: саморегулирования, включающего самоконтроль, умение принимать ответственность за свое поведение, способность адаптироваться к эмоциональным изменениям и проявлять гибкость, быть открытым новому; внутренней мотивации, включающей стремление к достижению цели и успеху, оптимизм, инициативность, умение действовать, исходя из своих возможностей

Выпускник научится:

1. самостоятельно определять цели деятельности и составлять планы деятельности; самостоятельно осуществлять, контролировать и корректировать деятельность; использовать все возможные ресурсы для достижения поставленных целей и реализации планов деятельности; выбирать успешные стратегии в различных ситуациях;

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

3. владеть навыками познавательной, учебно-исследовательской и проектной деятельности, навыками разрешения проблем;

4. использовать средства информационных и коммуникационных технологий в решении когнитивных, коммуникативных и организационных задач с соблюдением требований эргономики, техники безопасности, гигиены, ресурсосбережения, правовых и этических норм, норм информационной безопасности.

Выпускник получит возможность научиться:

1. быть готовым и способным к самостоятельной информационно-познавательной деятельности, включая умение ориентироваться в различных источниках информации, критически оценивать и интерпретировать информацию, получаемую из различных источников;

2. быть способным и готовым к самостоятельному поиску методов решения практических задач, применению различных методов познания.

Регулятивные универсальные учебные действия

1. самостоятельно определять цели, задавать параметры и критерии, по которым можно определить, что цель достигнута;

2. оценивать возможные последствия достижения поставленной цели в деятельности, собственной жизни и жизни окружающих людей, основываясь на соображениях этики и морали;

3. ставить и формулировать собственные задачи в образовательной деятельности и жизненных ситуациях;

4. оценивать ресурсы, в том числе время и другие нематериальные ресурсы, необходимые для достижения поставленной цели;

5. выбирать путь достижения цели, планировать решение поставленных задач, оптимизируя материальные и нематериальные затраты;

6. организовывать эффективный поиск ресурсов, необходимых для достижения поставленной цели;

7. сопоставлять полученный результат деятельности с поставленной заранее целью.

Познавательные универсальные учебные действия

1. искать и находить обобщенные способы решения задач, в том числе, осуществлять развернутый информационный поиск и ставить на его основе новые (учебные и познавательные) задачи;

2. критически оценивать и интерпретировать информацию с разных позиций, распознавать и фиксировать противоречия в информационных источниках;

3. использовать различные модельно-схематические средства для представления существенных связей и отношений, а также противоречий, выявленных в информационных источниках;

4. находить и приводить критические аргументы в отношении действий и суждений другого; спокойно и разумно относиться к критическим замечаниям в отношении собственного суждения, рассматривать их как ресурс собственного развития;

5. выходить за рамки учебного предмета и осуществлять целенаправленный поиск возможностей для широкого переноса средств и способов действия;

6. выстраивать индивидуальную образовательную траекторию, учитывая ограничения со стороны других участников и ресурсные ограничения;

7. менять и удерживать разные позиции в познавательной деятельности.

Коммуникативные универсальные учебные действия

1. осуществлять деловую коммуникацию как со сверстниками, так и со взрослыми (как внутри образовательной организации, так и за ее пределами), подбирать партнеров для деловой коммуникации исходя из соображений результативности взаимодействия, а не личных симпатий;

2. при осуществлении групповой работы быть как руководителем, так и членом команды в разных ролях (генератор идей, критик, исполнитель, выступающий, эксперт и т.д.);

3. координировать и выполнять работу в условиях реального, виртуального и комбинированного взаимодействия;

4. развернуто, логично и точно излагать свою точку зрения с использованием адекватных (устных и письменных) языковых средств;

5. распознавать конфликтогенные ситуации и предотвращать конфликты до их активной фазы, выстраивать деловую и образовательную коммуникацию, избегая личностных оценочных суждений.

Предметные результаты

Выпускник будет демонстрировать:

1) систематизация знаний, относящихся к *математическим объектам информатики*; умение строить математические объекты информатики, в том числе логические формулы;

2) сформированность базовых навыков и умений по соблюдению требований *техники безопасности*, гигиены и ресурсосбережения при работе со средствами информатизации;

3) владение опытом построения и использования *компьютерно-математических моделей*, проведения экспериментов и статистической обработки данных с помощью компьютера, интерпретации результатов, получаемых в ходе моделирования реальных процессов; умение оценивать числовые параметры моделируемых объектов и процессов; сформированность представлений о необходимости *анализа соответствия модели* и моделируемого объекта (процесса);

4) сформированность представлений о способах хранения и простейшей обработке данных; умение пользоваться *базами данных* и справочными системами; владение основными сведениями о базах данных, их структуре, средствах создания и работы с ними;

Выпускник получит возможность продемонстрировать:

1. владение системой базовых знаний, отражающих *вклад информатики* в формирование современной научной картины мира;

2. владение навыками *алгоритмического мышления* и понимание необходимости формального описания алгоритмов.

ПРОВЕРЯЕМЫЕ НА ЕГЭ ПО ИНФОРМАТИКЕ ТРЕБОВАНИЯ К РЕЗУЛЬТАТАМ ОСВОЕНИЯ ОСНОВНОЙ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ СРЕДНЕГО ОБЩЕГО ОБРАЗОВАНИЯ

Код проверяемого требования	Проверяемые требования к предметным результатам освоения основной образовательной программы среднего общего образования
1.	*Знать (понимать)*
1.1	Понимание основных принципов устройства и функционирования современных стационарных и мобильных компьютеров; тенденций развития компьютерных технологий; владение навыками работы с операционными системами и основными видами программного обеспечения для решения учебных задач по выбранной специализации
1.5	Знание функциональные возможности инструментальных средств среды разработки
1.6	Владение основными сведениями о базах данных, их структуре, средствах создания и работы с ними
2.	*Уметь*
2.2	Умение классифицировать основные задачи анализа данных (прогнозирование, классификация, кластеризация, анализ отклонений); понимать последовательность решения задач анализа данных: сбор первичных данных, очистка и оценка качества данных, выбор и (или) построение модели, пре-образование данных, визуализация данных, интерпретация результатов
2.11	Владение универсальным языком программирования высокого уровня (Паскаль, Python, Java, C++, C#), представлениями о базовых типах данных и структурах данных; умение использовать основные управляющие конструкции; умение осуществлять анализ предложенной программы: определять результаты работы программы при заданных исходных данных; определять, при каких исходных данных возможно получение указанных результатов; выявлять данные, которые могут привести к ошибке в работе программы; формулировать предложения по улучшению программного кода
2.12	Умение реализовывать на выбранном для изучения языке программирования высокого уровня (Паскаль, Python, Java, C++, C#) типовые алгоритмы обработки чисел, числовых последовательностей и массивов: представление числа в виде набора простых сомножителей; нахождение максимальной (минимальной) цифры натурального числа, записанного в системе счисления с основанием, не превышающим 10;

Код проверяемого требования	Проверяемые требования к предметным результатам освоения основной образовательной программы среднего общего образования
	вычисление обобщённых характеристик элементов массива или числовой последовательности (суммы, произведения среднего арифметического, минимального и максимального элементов, количества элементов, удовлетворяющих заданному условию); сортировку элементов массива; умение использовать в программах данные различных типов с учётом ограничений на диапазон их возможных значений, применять при решении задач структуры данных (списки, словари, стеки, очереди, деревья); применять стандартные и собственные подпрограммы для обработки числовых данных и символьных строк; использовать при разработке программ библиотеки подпрограмм; умение использовать средства отладки программ в среде программирования

ПЕРЕЧЕНЬ ЭЛЕМЕНТОВ СОДЕРЖАНИЯ, ПРОВЕРЯЕМЫХ НА ЕГЭ ПО ИНФОРМАТИКЕ

Код	Проверяемый элемент содержания
3	Алгоритмы и программирование
3.6	Язык программирования (Паскаль, Python, Java, C++, C#). Типы данных: целочисленные, вещественные, символьные, логические. Ветвления. Сложные условия. Циклы с условием. Циклы по переменной. Обработка данных, хранящихся в файлах. Текстовые и двоичные файлы. Файловые переменные (файловые указатели). Чтение из файла. Запись в файл. Разбиение задачи на подзадачи. Подпрограммы (процедуры и функции). Использование стандартной библиотеки языка программирования
3.9	Обработка символьных данных. Встроенные функции языка программирования для обработки символьных строк. Алгоритмы обработки символьных строк: подсчёт количества появлений символа в строке, разбиение строки на слова по пробельным символам, поиск подстроки внутри данной строки, замена найденной подстроки на другую строку. Генерация всех слов в некотором алфавите, удовлетворяющих заданным ограничениям. Преобразование числа в символьную строку и обратно
3.12	Словари (ассоциативные массивы, отображения). Хэш-таблицы. Построение алфавитно-частотного словаря для заданного текста
3.13	Стеки. Анализ правильности скобочного выражения. Вычисление арифметического выражения, записанного в постфиксной форме.

Код	Проверяемый элемент содержания
	Очереди. Использование очереди для временного хранения данных
3.15	Деревья. Реализация дерева с помощью ссылочных структур. Двоичные (бинарные) деревья. Построение дерева для заданного арифметического выражения. Рекурсивные алгоритмы обхода дерева. Использование стека и очереди для обхода дерева
3.17	Понятие об объектно-ориентированном программировании. Объекты и классы. Свойства и методы объектов. Объектно-ориентированный анализ. Разработка программ на основе объектно-ориентированного подхода. Инкапсуляция, наследование, полиморфизм

3. Тематическое планирование

10 класс

№ п/п	Наименование разделов и тем программы	Количество часов			Электронные (цифровые) образовательные ресурсы
		Всего	Контрольные работы	Практические работы	
Модуль №1 «Информационная безопасность» - 33 часа					
1.1	Информационная безопасность	31		2	https://www.lektorium.tv/info-security
1.2	Итоговый проект	1		1	

11 класс

№ п/п	Наименование разделов и тем программы	Количество часов			Электронные (цифровые) образовательные ресурсы
		Всего	Контрольные работы	Практические работы	
Модуль №1 «Информационная безопасность» - 30 часов					
1.1	Информационная безопасность	29		2	https://www.lektorium.tv/info-security
1.2	Итоговый проект	1		1	

5. Приложения к программе

ПОУРОЧНОЕ ПЛАНИРОВАНИЕ
10 класс

№ п/п	Наименование разделов и тем программы	Количество часов			Электронные (цифровые) образовательные ресурсы
		Всего	Контрольные работы	Практические работы	
Модуль 1. Информационная безопасность - 33 часа					
1.1	Вводное занятие. Какие области ИБ и виды соревнований существуют?	2			https://www.lektorium.tv/info-security
1.2	Введение в Linux. Часть I.	2			
1.3	Введение в Linux. Часть II.	2			
1.4	Как работают веб-сервисы. TCP/UDP, HTTP.	2			
1.5	Google dorking. Как работает поисковая система.	2			
1.6	LFI, Command injection.	2			
1.7	RCE (Remote Code Execution).	2			
1.8	Проведение соревнований. Часть I.	2		1	
1.9	Проведение	3		1	

	соревнований. Часть II.				
1.10	Изучение баз данных. SQL. SQL-инъекции.	2			
1.11	Принципы ИБ. Значение данных и философия.	2			
1.12	Способы создания backdoor'ов в Linux.	2			
1.13	Разбор домашнего задания.	2			
1.14	KillChain. Проведение полноценной атаки на примере машины с HTB.	4			
1.15	Образование и особенности обучения в сфере ИБ.	2			

11 класс

№ п/п	Наименование разделов и тем программы	Количество часов			Электронные (цифровые) образовательные ресурсы
		Всего	Контрольные работы	Практические работы	
Модуль 1. Информационная безопасность - 30 часов					
1.1	Вводное занятие. Какие области ИБ и	2			https://www.lektorium.tv/info-security

	виды соревнований существуют?				
1.2	Введение в Linux. Часть I.	2			
1.3	Введение в Linux. Часть II.	2			
1.4	Как работают веб-сервисы. TCP/UDP, HTTP.	2			
1.5	Google dorking. Как работает поисковая система.	2			
1.6	LFI, Command injection.	2			
1.7	RCE (Remote Code Execution).	2			
1.8	Проведение соревнований. Часть I.	2		1	
1.9	Проведение соревнований. Часть II.	2		1	
1.10	Изучение баз данных. SQL. SQL-инъекции.	2			
1.11	Принципы ИБ. Значение данных и философия.	2			
1.12	Способы создания backdoor'ов в Linux.	2			

1.13	Разбор домашнего задания.	2			
1.14	KillChain. Проведение полноценной атаки на примере машины с HTB.	2			
1.15	Образование и особенности обучения в сфере ИБ.	2			

КИМ
Модуль 1 «Информационная безопасность»

Практическая работа: «Операция “Кибер-расследование”»

Формат: Задание типа «Захвати флаг» (Capture The Flag) с последовательным прохождением этапов.

Сценарий: Вы — стажер в отделе кибербезопасности. К вашему руководителю поступило анонимное сообщение о потенциальной уязвимости во внутренней тестовой системе компании https://testcorp.local. Вам поручено провести проверку и оценить возможные риски.

Цель: Получить доступ к системе, обнаружить конфиденциальные данные и оставить отчет, доказав уязвимость. На каждом этапе вас ждет «флаг» — строка с кодом вида FLAG{...}, который необходимо найти и сдать.

Критерии оценки:

Найден 1-3 флага: Удовлетворительно. Понимание базовых принципов.
Найдено 4-7 флагов: Хорошо. Умение применять инструменты и логически мыслить.
Найдено 8+ флагов и написан отчет: Отлично. Системный подход, соответствующий этапам Kill Chain.
Этап 1: Разведка (Reconnaissance)

Задача: Используя технику Google Dorking, найдите скрытый тестовый раздел сайта testcorp.local.

Подсказка: Компания использует систему WordPress. Найдите документ для разработчиков, не предназначенный для индексации.
Инструменты: Поисковая система, операторы site:, inurl:, filetype:.

Флаг №1: Содержится в найденном PDF-документе.
Этап 2: Сканирование и анализ (Weaponization)

Задача: Цель найдена: https://testcorp.local/dev/docs.php. Проанализируйте параметры этого скрипта.

Подсказка: Скрипт принимает параметр file для отображения технической документации (например, ?file=network.pdf).
Инструменты: Браузер, curl.
Что искать: Попробуйте прочитать не только PDF-файлы. Используйте технику LFI (Local File Inclusion).

Флаг №2: Содержится в файле /etc/passwd на целевом сервере.
Этап 3: Поиск уязвимостей (Exploitation)

Задача 3.1: Обнаружьте, что скрипт docs.php также уязвим к RCE (Remote Code Execution) через уязвимость Command Injection.

Подсказка: Сервер объединяет содержимое файла с помощью команды cat. Попробуйте добавить свою команду через символы ; или |.
Пример: ?file=network.pdf; whoami
Инструменты: Burp Suite, curl.
Флаг №3: Выполните команду ls /home и найдите домашнюю директорию пользователя www-data. Флаг находится в файле flag.txt в этой директории.
Задача 3.2: Получите обратное соединение с сервером (Reverse Shell).

Инструменты: netcat, rlwrap.
Действие: Используя уязвимость RCE, заставьте сервер подключиться к вашей виртуальной машине на указанный порт.
Флаг №4: Найдите конфигурационный файл базы данных WordPress (wp-config.php) и извлеките из него пароль к БД. Этот пароль и является флагом.
Этап 4: Углубление доступа (Privilege Escalation)

Задача: Вы находитесь внутри системы как пользователь www-data. Изучите окружение и найдите способ повысить привилегии до root.

Подсказка 1: Проверьте, какие программы можно запускать от root с помощью команды sudo -l.
Подсказка 2: На сервере установлена старая версия текстового редактора, позволяющая запускать оболочку.
Инструменты: Команды Linux: sudo, find, linpeas.sh.

Флаг №5: Получив права root, найдите в системе файл root_flag.txt.
Этап 5: Работа с данными (Exfiltration)

Задача: Найдите базу данных WordPress и извлеките конфиденциальные данные.

Инструменты: Командная строка MySQL: mysql -u username -p database_name.
Действие: Подключитесь к БД, используя учетные данные из wp-config.php. Найдите таблицу wp_users и хэши паролей администратора.
Флаг №6: Хэш пароля пользователя admin.
Этап 6: Создание backdoor (Persistence)

Задача: Обеспечьте себе возможность вернуться в систему, даже если уязвимость будет закрыта.

Действие: Создайте скрытого пользователя с правами root и/или установите SSH-ключ для авторизации.
Инструменты: Команды useradd, ssh-keygen.
Флаг №7: Публичный ключ, который вы добавили в authorized_keys.
Этап 7: Анализ и отчетность (Reporting)

Финальное задание: Напишите краткий отчет о проведенной атаке по модели Kill Chain.

Цель: testcorp.local
Выявленные уязвимости: Перечислите все найденные уязвимости (LFI, RCE, пр.).
Методы атаки: Опишите кратко, как вы exploited каждую уязвимость.
Доказательства: Приложите все найденные флаги.
Рекомендации: Предложите по 1-2 способу исправления для каждой уязвимости.
Флаг №8 (Бонусный): Содержится в корректно составленном отчете, который необходимо отправить на проверку.