

ДЕПАРТАМЕНТ ПО СОЦИАЛЬНЫМ ВОПРОСАМ
Заводоуковская средняя общеобразовательная школа № 3,
филиал Муниципального автономного
общеобразовательного учреждения
Заводоуковского муниципального округа
«Заводоуковская средняя общеобразовательная школа № 2»
(СОШ № 3, филиал МАОУ «СОШ № 2»)

РАССМОТРЕНА
на заседании ШМО
учителей математики и
информатики
протокол № 7
от 24.08.2026
/Поляк М.А./ *Пл-*

СОГЛАСОВАНА
заместитель директора
филиала
Мингалева А.А.
/Мингалева А.А./
от 28.08.2026

УТВЕРЖДЕНА
приказом директора школы
от 29.08.2026
№ 141-О

РАБОЧАЯ ПРОГРАММА
учебного курса
«Информационная безопасность»
Уровень среднего общего образования

Составитель:
Барышева О.В.
учитель математики

ПОЯСНИТЕЛЬНАЯ ЗАПИСКА

Рабочая программа учебного курса «Информационная безопасность» разработана в соответствии с ФГОС СОО, утв. приказом Минобрнауки РФ от 17.05.2012 № 413 с изм. от 12.08.2022 № 732, с учётом ФОП СОО, утверждённой приказом Министерства просвещения РФ от 18.05.2023 № 371 (с обновлением от 12.07.2023 № 74228), приказа Минпросвещения России от 09.10.2024 № 704 «О внесении изменений в некоторые приказы Министерства просвещения Российской Федерации, касающиеся федеральных образовательных программ начального общего образования, основного общего образования и среднего общего образования»; в соответствии с Положением о рабочих программах учебных предметов, учебных курсов (в том числе курсов внеурочной деятельности), учебных модулей, разрабатываемых на основе обновленных ФГОС и в соответствии с требованиями Федеральных образовательных программ начального общего, основного общего, среднего общего образования.

ОБЩАЯ ХАРАКТЕРИСТИКА УЧЕБНОГО КУРСА «ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ»

Курс «Информационная безопасность» является важной составляющей работы с обучающимися, активно использующими различные сетевые формы общения (социальные сети, игры, пр.) с целью мотивации ответственного отношения к обеспечению своей личной безопасности, безопасности своей семьи и своих друзей.

Правовая грамотность приобретает новый ракурс в связи с процессом информатизации всех сфер деятельности человека, включая и школьное образование. Роль информации в данном процессе достаточно велика, и, по мнению ведущих специалистов в области информационной безопасности, она на сегодняшний день занимает уровень главного ресурса развития человеческой цивилизации. Более того, информация наряду с веществом и энергией стала основой всего научного знания и жизни человека. В этой связи вопросы, касающиеся информационной безопасности, являются составной частью правовой культуры и совершенно очевидно, что они должны занимать значительное место в содержании школьного курса информатики.

Программа курса «Информационной безопасности» ориентирована на учащихся, проявляющих интерес к различным аспектам защиты информации, желающих углубленно изучить правовые аспекты информационной безопасности, и рассчитана на учеников, имеющих подготовку по информатике в объеме, соответствующем требованиям стандарта среднего общего образования по информатике и информационным технологиям.

Курс включает в себя как теорию, так и практику. Теория дает знания о предмете

безопасности, проблемах ее обеспечения и принципах их решения. В результате практических занятий формируются умения оформления информационных объектов с целью обеспечения их безопасного состояния.

Особый характер тематики обучения требует дискуссионной формы организации занятий, когда ученики вовлекаются в круг проблем, смело высказывают свои мнения и суждения по каждому вопросу. Практическая работа осуществляется учеником на персональном компьютере, где в отдельной папке он формирует файлы-документы и производит над ними соответствующие действия.

Содержание обучения, формы занятий, проектная деятельность предусматривают развитие межпредметных связей - опору на знания других разделов информатики, истории, обществознания, естествознания и др.

ЦЕЛИ ИЗУЧЕНИЯ УЧЕБНОГО КУРСА «ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ»

Дать понятие информационной безопасности, целей и задач информационной безопасности, структуры предмета информационной безопасности и ее обеспечения; представление о защите информации, ее формах, структуре, функциях и задачах; сформировать у учащихся представление об основных проблемах информационной безопасности, принципах и подходах к их решению; сформировать у учащихся компетенций в следующих областях:

- обеспечение информационной безопасности;
- правовые аспекты информационной безопасности;
- криптография;
- сетевая безопасность;
- безопасность личного информационного пространства.

обеспечение условий для профилактики негативных тенденций в развитии информационной культуры учащихся, повышения защищённости детей от информационных рисков и угроз; формирование навыков своевременного распознавания онлайн-рисков (технического, контентного, коммуникационного, потребительского характера).

Задачи изучения курса:

- Сформировать общекультурные навыки работы с информацией (умения, связанные с поиском, пониманием, организацией, архивированием цифровой информации и ее критическим осмыслением, а также с созданием информационных объектов с использованием цифровых ресурсов (текстовых, изобразительных, аудио и видео);

- создать условия для формирования умений, необходимых для различных форм коммуникации (электронная почта, чаты, блоги, форумы, социальные сети и др.) с различными целями и ответственное отношения к взаимодействию в современной информационно-телекоммуникационной среде;
- сформировать знания, позволяющие эффективно и безопасно использовать технические и программные средства для решения различных задач, в том числе использования компьютерных сетей, облачных сервисов и т.п.;
- сформировать знания, умения, мотивацию и ответственность, позволяющие решать с помощью цифровых устройств и интернета различные повседневные задачи, связанные с конкретными жизненными ситуациями, предполагающими удовлетворение различных потребностей;
- сформировать навыки по профилактике и коррекции зависимого поведения школьников, связанного с компьютерными технологиями и Интернетом.

Воспитательный потенциал учебного предмета «Основы предпринимательской деятельности» реализуется через:

- использование воспитательных возможностей содержания учебного предмета для создания благоприятных условий для развития социально значимых отношений школьников и прежде всего ценностных отношений через демонстрацию обучающимся примеров ответственного, гражданского поведения, проявления человеколюбия и добросердечности, через подбор соответствующих текстов для чтения, задач для решения, проблемных ситуаций для обсуждения в классе;
- применение на уроке адекватных особым потребностям обучающихся и их реальным возможностям форм организации: дидактических материалов, стимулирующих познавательную мотивацию обучающихся;
- привлечение внимания обучающихся к ценностному аспекту изучаемых на уроках явлений, организация их работы с получаемой на уроке социально значимой информацией - инициирование ее обсуждения, высказывания обучающимися своего мнения по ее поводу, выработки своего к ней отношения;
- использование на уроке адекватных коммуникативных и коммуникационных (цифровых) технологий;
- организация взаимопомощи обучающихся друг другу в рамках урочной деятельности.

МЕСТО УЧЕБНОГО КУРСА «ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ» В УЧЕБНОМ ПЛАНЕ

Программа курса «Информационная безопасность» предназначена для реализации
Учебный курс «Информационная безопасность» составлен на основе требований

к предметным результатам освоения основной образовательной программы, представленной в федеральном государственном образовательном стандарте основного общего образования, и рассчитан на общую учебную нагрузку в объеме 34 часа (1 ч в неделю в течение одного года).

УЧЕБНО - МЕТОДИЧЕСКИЙ КОМПЛЕКТ УЧЕБНОГО КУРСА «ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ»

Для педагога:

1. Федеральный закон от 29.12.2012 года № 273 – ФЗ «Об образовании в Российской Федерации»;
2. Примерная программа основного общего образования по информатике и информационным технологиям Федерального государственного образовательного стандарта среднего общего образования;
3. Профессиональный стандарт:
 - 3.1. 06.026 «Системный администратор информационно-коммуникационных систем», утв. приказом Министерства труда и социальной защиты Российской Федерации от 29 сентября 2020 года N 680 (зарегистрирован Министерством юстиции Российской Федерации 26 октября 2020 года, регистрационный № 60580).
 - 3.2. 06.030 «Специалист по защите информации в телекоммуникационных системах и сетях», утв. приказом Министерства труда и социальной защиты Российской Федерации от 3 ноября 2016 г. № 608н (зарегистрирован Министерством юстиции Российской Федерации 25 ноября 2016 г., регистрационный № 44449).
 - 3.3. 06.032 «Специалист по безопасности компьютерных систем и сетей», утв. приказом Министерства труда и социальной защиты Российской Федерации от 1 ноября 2016 г. № 598н (зарегистрирован Министерством юстиции Российской Федерации 28 ноября 2016 г., регистрационный № 44464), (с изменениями и дополнениями).
 - 3.4. 06.030 «Специалист по защите информации в телекоммуникационных системах и сетях», утв. приказом Министерства труда и социальной защиты Российской Федерации от 3 ноября 2016 г. № 608н (зарегистрирован Министерством юстиции Российской Федерации 25 ноября 2016 г., регистрационный № 44449).
 - 3.5. 06.032 «Специалист по безопасности компьютерных систем и сетей», утв. приказом Министерства труда и социальной защиты Российской Федерации от 1 ноября 2016 г. № 598н (зарегистрирован Министерством юстиции Российской Федерации 28 ноября 2016 г., регистрационный № 44464), (с изменениями и дополнениями).
 - 3.6. 06.033 «Специалист по защите информации в автоматизированных системах», утв. приказом Министерства труда и социальной защиты Российской Федерации от 15

сентября 2016 г. № 522н (зарегистрирован Министерством юстиции Российской Федерации 28 сентября 2016 г., регистрационный № 43857).

3.7. 06.034 «Специалист по технической защите информации», утв. приказом Министерства труда и социальной защиты Российской Федерации от 1 ноября 2016 г. № 599н (зарегистрирован Министерством юстиции Российской Федерации 25 ноября 2016 года, регистрационный № 44443).

3.8. 06.030 «Специалист по защите информации в телекоммуникационных системах и сетях», утв. приказом Министерства труда и социальной защиты Российской Федерации от 3 ноября 2016 г. № 608н (зарегистрирован Министерством юстиции Российской Федерации 25 ноября 2016 г., регистрационный № 44449).

3.9. 06.032 «Специалист по безопасности компьютерных систем и сетей», утв. приказом Министерства труда и социальной защиты Российской Федерации от 1 ноября 2016 г. № 598н (зарегистрирован Министерством юстиции Российской Федерации 28 ноября 2016 г., регистрационный № 44464), (с изменениями и дополнениями).

3.10. 06.033 «Специалист по защите информации в автоматизированных системах», утв. приказом Министерства труда и социальной защиты Российской Федерации от 15 сентября 2016 г. № 522н (зарегистрирован Министерством юстиции Российской Федерации 28 сентября 2016 г., регистрационный № 43857).

3.11. 06.034 «Специалист по технической защите информации», утв. приказом Министерства труда и социальной защиты Российской Федерации от 1 ноября 2016 г. № 599н (зарегистрирован Министерством юстиции Российской Федерации 25 ноября 2016 года, регистрационный № 44443).

ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОСВОЕНИЯ ПРОГРАММЫ ПО НА УРОВНЕ СРЕДНЕГО ОБЩЕГО ОБРАЗОВАНИЯ

Личностные:

Выработать у обучающегося осознанное, уважительное и доброжелательное отношение к окружающим людям в реальном и виртуальном мире, их позициям, взглядам, готовность вести диалог с другими людьми, обоснованно осуществлять выбор виртуальных собеседников;

готовность и способность к осознанному выбору и построению дальнейшей индивидуальной траектории образования на базе ориентировки в мире профессий и профессиональных предпочтений, с учетом устойчивых познавательных интересов;

понимание социальных норм, правил поведения, ролей и форм социальной жизни в группах и сообществах;

сформированность понимания ценности безопасного образа жизни;

интериоризация правил индивидуального и коллективного безопасного поведения в информационно- телекоммуникационной среде.

Метапредметные:

В результате освоения учебного курса обучающийся сможет идентифицировать собственные проблемы и определять главную проблему; выдвигать версии решения проблемы, формулировать гипотезы, предвосхищать конечный результат; ставить цель деятельности на основе определенной проблемы и существующих возможностей; выбирать из предложенных вариантов и самостоятельно искать средства/ресурсы для решения задачи/достижения цели; составлять план решения проблемы (выполнения проекта, проведения исследования); описывать свой опыт, оформляя его для передачи другим людям в виде технологии решения практических задач определенного класса; оценивать свою деятельность, аргументируя причины достижения или отсутствия планируемого результата; находить достаточные средства для выполнения учебных действий в изменяющейся ситуации и/или при отсутствии планируемого результата; работая по своему плану, вносить коррективы в текущую деятельность на основе анализа изменений ситуации для получения запланированных характеристик продукта/результата; принимать решение в учебной ситуации и нести за него ответственность; выделять явление из общего ряда других явлений; определять обстоятельства, которые предшествовали возникновению связи между явлениями, из этих обстоятельств выделять определяющие, способные быть причиной данного явления, выявлять причины и следствия явлений; строить рассуждение от общих закономерностей к частным явлениям и от частных явлений к общим закономерностям; излагать полученную информацию, интерпретируя ее в контексте решаемой задачи; самостоятельно указывать на информацию, нуждающуюся в проверке, предлагать и применять способ проверки достоверности информации; критически оценивать содержание и форму текста; определять необходимые ключевые поисковые слова и запросы; строить позитивные отношения в процессе учебной и познавательной деятельности; критически относиться к собственному мнению, с достоинством признавать ошибочность своего мнения (если оно таково) и корректировать его; договариваться о правилах и вопросах для обсуждения в соответствии с поставленной перед группой задачей; делать оценочный вывод о достижении цели коммуникации непосредственно после завершения коммуникативного контакта и обосновывать его. целенаправленно искать и использовать информационные ресурсы, необходимые для решения учебных и практических задач с помощью средств ИКТ; выбирать, строить и использовать адекватную информационную модель для передачи своих мыслей средствами естественных и формальных языков в соответствии с

условиями коммуникации; использовать компьютерные технологии (включая выбор адекватных задаче инструментальных программно-аппаратных средств и сервисов) для решения информационных и коммуникационных учебных задач, в том числе: вычисление, написание писем, сочинений, докладов, рефератов, создание презентаций и др.; использовать информацию с учетом этических и правовых норм; создавать информационные ресурсы разного типа и для разных аудиторий, соблюдать информационную гигиену и правила информационной безопасности.

Предметные:

Обучающийся научится анализировать доменные имена компьютеров и адреса документов в интернете; безопасно использовать средства коммуникации, безопасно вести и применять способы самозащиты при попытке мошенничества, безопасно использовать ресурсы интернета.

Овладеет приемами безопасной организации своего личного пространства данных с использованием индивидуальных накопителей данных, интернет-сервисов и т.п.

Получит возможность овладеть основами соблюдения норм информационной этики и права; основами самоконтроля, самооценки, принятия решений и осуществления осознанного выбора в учебной и познавательной деятельности при формировании современной культуры безопасности жизнедеятельности; использовать для решения коммуникативных задач в области безопасности жизнедеятельности различные источники информации, включая Интернет-ресурсы и другие базы данных.

СОДЕРЖАНИЕ УЧЕБНОГО КУРСА «ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ»

РАЗДЕЛ 1. Безопасность информации (Углубленный уровень) — 12 часов

1. Правовые аспекты информационной безопасности (2 ч).

- Федеральные законы: 149-ФЗ «Об информации, информационных технологиях и о защите информации», 152-ФЗ «О персональных данных», 187-ФЗ «О безопасности критической информационной инфраструктуры».
- Ответственность за правонарушения в сфере ИБ (КоАП, УК РФ).
- Лицензирование деятельности по технической защите конфиденциальной информации.

2. Криптография и защита данных (3 ч).

- История криптографии. Шифры замены и перестановки.
- Симметричное и асимметричное шифрование. Электронная цифровая подпись (ЭЦП).

- Практическая работа: «Шифрование текста с использованием простых шифров» или «Работа с ЭЦП (на примере портала Госуслуг)».
- 3. Основы сетевой безопасности (3 ч).**
- Модель OSI и стек TCP/IP. Уязвимости протоколов.
 - Межсетевые экраны (Firewall) и системы обнаружения вторжений (IDS/IPS).
 - VPN: принципы работы, риски использования бесплатных сервисов.
- 4. Защита информации в корпоративных системах (2 ч).**
- Понятие коммерческой тайны. Режим коммерческой тайны.
 - DLP-системы (предотвращение утечек данных).
 - Промышленный шпионаж и кибердиверсии.
- 5. Выполнение и защита проектов (2 ч).**
- Проекты: «Модель безопасной сети школы», «Анализ утечек данных в крупных компаниях», «Разработка политики информационной безопасности для малого бизнеса».

РАЗДЕЛ 2. Безопасность устройств (Углубленный уровень) — 12 часов

- 1. Анализ вредоносного ПО и методы его исследования (3 ч).**
- Классификация: вирусы, черви, трояны, шпионы, шифровальщики (Ransomware).
 - Песочницы (Sandbox) для анализа ПО.
 - Практическая работа: «Анализ подозрительного файла в виртуальной среде (на примере онлайн-сервисов)».
- 2. Безопасность операционных систем (3 ч).**
- Разграничение прав доступа. Учетные записи пользователей и администратора.
 - Настройка политик безопасности в Windows/Linux.
 - Обновление ПО как критический элемент безопасности. Управление уязвимостями.
- 3. Безопасность интернета вещей (IoT) и мобильных устройств (2 ч).**
- Умные дома, носимые устройства: риски взлома.
 - Безопасность Android и iOS: различия в архитектуре, root-права и джейлбрейк.
 - Практическая работа: «Настройка безопасного смартфона».
- 4. Основы кибергигиены и цифровой forensic (2 ч).**
- Сбор цифровых доказательств. Восстановление удаленных данных.
 - Логи и журналы событий: как найти следы атаки.

5. Выполнение и защита проектов (2 ч).

- Проекты: «Исследование уязвимости домашней Wi-Fi сети», «Разработка инструкции по безопасному использованию IoT-устройств в школе».

РАЗДЕЛ 3. Безопасность общения (Углубленный уровень) — 6 часов

1. Цифровая репутация и самопрезентация (2 ч).

- Понятие цифрового следа. Влияние цифрового следа на карьеру и образование.
- Управление репутацией: удаление данных, запросы на удаление, право на забвение.
- Практическая работа: «Аудит собственного цифрового следа».

2. Психология кибербуллинга и троллинга (2 ч).

- Кибербуллинг в подростковой среде и профессиональных коллективах.
- Методы противодействия и психологическая помощь.
- Роль модерации в сообществах.

3. Профессиональная этика в сети (2 ч).

- Нетикет (сетевой этикет) в деловой переписке.
- Безопасность при трудоустройстве онлайн: проверка работодателя, защита персональных данных при отклике на вакансии.

4. Итоговое обобщение (Зачет/Практикум) (1 ч).

- Комплексный тест по всем разделам 11 класса.
- Или итоговая практическая работа: «Разработка памятки по информационной безопасности для сотрудников организации».

ТЕМАТИЧЕСКОЕ ПЛАНИРОВАНИЕ

№	Тема	Кол-во часов	Практические работы
1	Правовые аспекты ИБ	2	Анализ кейсов правонарушений
2	Криптография	3	Шифрование текста, работа с ЭЦП
3	Сетевая безопасность	3	Настройка Firewall, анализ трафика
4	Защита в корпоративных системах	2	Разработка политики ИБ

ИТОГО: 34 часа

ПОУРОЧНОЕ ПЛАНИРОВАНИЕ

№ п/п	Наименование разделов и тем программы	Кол-во часов	Практические работы	Электронные (цифровые) образовательные ресурсы
Безопасность информации				
1.1	Правовые аспекты информационной безопасности. Федеральные законы 149-ФЗ, 152-ФЗ, 187- ФЗ	2	Анализ кейсов правонарушений в сфере ИБ	https://sbersova.ru/sections/protection/kurs-po-informacionnoy-bezopasnosti
1.2	Ответственность за правонарушения в сфере информационной безопасности	2	Работа с нормативными документами	https://sbersova.ru/sections/protection/kurs-po-informacionnoy-bezopasnosti
1.3	Криптография: история и основные понятия. Шифры замены и перестановки	2	Практическая работа «Шифрование текста»	https://sbersova.ru/sections/protection/kurs-po-informacionnoy-bezopasnosti
1.4	Симметричное и асимметричное шифрование. Электронная цифровая подпись (ЭЦП)	2	Практическая работа «Работа с ЭЦП»	https://sbersova.ru/sections/protection/kurs-po-informacionnoy-bezopasnosti
1.5	Основы сетевой безопасности. Модель OSI и стек TCP/IP	2	Анализ сетевых протоколов	https://sbersova.ru/sections/protection/kurs-po-informacionnoy-bezopasnosti
1.6	Межсетевые экраны и VPN: принципы работы и риски	2	Настройка VPN и Firewall	https://sbersova.ru/sections/protection/kurs-po-informacionnoy-bezopasnosti
Безопасность устройств				
2.1	Анализ вредоносного ПО: вирусы, черви, трояны, шифровальщики	2	Классификация вредоносных программ	https://sbersova.ru/sections/protection/kurs-po-informacionnoy-bezopasnosti

2.2	Методы исследования вредоносного ПО. Песочницы (Sandbox)	2	Анализ подозрительного файла в виртуальной среде	https://sbersova.ru/sections/protection/kurs-po-informacionnoy-bezopasnosti
2.3	Безопасность операционных систем. Разграничение прав доступа	2	Настройка политик безопасности Windows/Linux	https://sbersova.ru/sections/protection/kurs-po-informacionnoy-bezopasnosti
2.4	Управление уязвимостями и обновлениями ПО	2	Работа с центрами обновлений	https://sbersova.ru/sections/protection/kurs-po-informacionnoy-bezopasnosti
2.5	Безопасность интернета вещей (IoT) и мобильных устройств	2	Настройка безопасного смартфона	https://sbersova.ru/sections/protection/kurs-po-informacionnoy-bezopasnosti
2.6	Основы цифровой криминалистики (forensic). Логи и журналы событий	2	Поиск следов атаки в логах	https://sbersova.ru/sections/protection/kurs-po-informacionnoy-bezopasnosti
Безопасность общения				
3.1	Цифровая репутация и цифровой след. Управление репутацией	2	Аудит собственного цифрового следа	https://sbersova.ru/sections/protection/kurs-po-informacionnoy-bezopasnosti
3.2	Психология кибербуллинга и троллинга. Методы противодействия	2	Анализ ситуаций кибербуллинга	https://sbersova.ru/sections/protection/kurs-po-informacionnoy-bezopasnosti
3.3	Профессиональная этика в сети. Нетикет в деловой переписке	2	Составление делового письма	https://sbersova.ru/sections/protection/kurs-po-informacionnoy-bezopasnosti
3.4	Безопасность при трудоустройстве онлайн. Защита персональных данных	2	Проверка работодателя и вакансии	https://sbersova.ru/sections/protection/kurs-po-informacionnoy-bezopasnosti
Итоговое обобщение				

4.1	Разработка памятки по информационной безопасности для организации	1	Итоговая практическая работа	https://sbersova.ru/sections/protection/kurs-po-informacionnoy-bezopasnosti
4.2	Разработка памятки по информационной безопасности для организации	1	Итоговая практическая работа	https://sbersova.ru/sections/protection/kurs-po-informacionnoy-bezopasnosti

ПРОВЕРЯЕМЫЕ ТРЕБОВАНИЯ К РЕЗУЛЬТАТАМ ОСВОЕНИЯ ОСНОВНОЙ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

Код проверяемого результата	Проверяемые предметные результаты освоения основной образовательной программы среднего общего образования
1	По теме «Цифровая грамотность»
1.1	Наличие представлений о компьютерных сетях и их роли в современном мире; об общих принципах разработки и функционирования интернет-приложений
1.2	Умение организовывать личное информационное пространство с использованием различных средств цифровых технологий; понимание возможностей цифровых сервисов государственных услуг, цифровых образовательных сервисов; понимание возможностей и ограничений технологий искусственного интеллекта в различных областях; наличие представлений об использовании информационных технологий в различных профессиональных сферах
2	По теме «Теоретические основы информатики»
2.1	Владение теоретическим аппаратом, позволяющим определять кратчайший путь во взвешенном графе и количество путей между вершинами ориентированного ациклического графа
4	По теме «Информационные технологии»
4.1	Умение использовать компьютерно-математические модели для анализа объектов и процессов: формулировать цель моделирования, выполнять анализ результатов, полученных в ходе моделирования; оценивать адекватность модели моделируемому объекту или процессу; представлять результаты моделирования в наглядном виде

ПРОВЕРЯЕМЫЕ ЭЛЕМЕНТЫ СОДЕРЖАНИЯ

Код	Проверяемый элемент содержания
1	Цифровая грамотность
1.1	Принципы построения и аппаратные компоненты компьютерных сетей. Сетевые протоколы. Сеть Интернет. Адресация в сети Интернет. Система доменных имён
2	Теоретические основы информатики
2.1	Модели и моделирование. Цели моделирования. Соответствие модели моделируемому объекту или процессу. Формализация прикладных задач. Представление результатов моделирования в виде, удобном для восприятия человеком. Графическое представление данных (схемы, таблицы, графики)
4	Информационные технологии
4.1	Анализ данных. Основные задачи анализа данных: прогнозирование, классификация, кластеризация, анализ отклонений. Последовательность решения задач анализа данных: сбор первичных данных, очистка и оценка качества данных, выбор и (или) построение модели, преобразование данных, визуализация данных, интерпретация результатов
4.2	Анализ данных с помощью электронных таблиц. Вычисление суммы, среднего арифметического, наибольшего и наименьшего значений диапазона
4.3	Компьютерно-математические модели. Этапы компьютерно-математического моделирования: постановка задачи, разработка модели, тестирование модели, компьютерный эксперимент, анализ результатов моделирования