Муниципальное общеобразовательное учреждение
«Средняя общеобразовательная школа п. Белоярский
Новобурасского района Саратовской области
имени Бабушкина А.М»

«Принято»
Руководитель МО

_____/ Лозе Е.Н /
подпись ФИО
Протокол № 1 от
«28»августа 2023г.

«Согласовано»
Заместитель
руководителя по ВР МОУ
«СОШ п.Белоярский
имени Бабушкина А.М.»
_____/Максимова С.В./
подпись ФИО
«28»_08_2023_г.

«Утверждаю»
Руководитель МОУ «СОШ
п.Белоярский имени
Бабушкина А.М.»
_____/Юркина С.А./
подпись ФИО
Приказ №82
от «28»_08_2023г.

РАБОЧАЯ ПРОГРАММА

Внеурочной деятельности «Информационная безопасность»
(указать учебный предмет, курс или модуля, название в/д)
для обучающихся 10 класса

Рассмотрено на заседании
педагогического совета
протокол № 1
от «28» августа 2023 г.

Пояснительная записка

Программа разработана наоснове:

- федерального государственного образовательного стандарта основного общего образования по предметным образовательным областям «Математика и информатика», «Физическая культура и основы безопасности жизнедеятельности»;
- Учебного плана внеурочной деятельности МОУ «СОШ п.Бедоярский имени Бабушкина А.М.»;

Основными **целями** изучения курса «Информационная безопасность» являются:

• обеспечение условий для профилактики негативных тенденций в информационной культуре учащихся, повышениязащищенности детей от информационных рисков и угроз;

• формирование навыков своевременного распознавания онлайн-рисков (технического, контентного, коммуникационного, потребительского характера и риска интернет-зависимости).

Задачи программы:

1. 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);
2. создать условия для формирования умений, необходимых для различных форм коммуникации (электронная почта, чаты, блоги, форумы, социальные сети и др.) с различными целями и ответственного отношения к взаимодействию в современной информационно-телекоммуникационной среде;
3. 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.;
4. 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;
5. сформировать навыки по профилактике и коррекции зависимого поведения школьников, связанного с компьютерными технологиями и Интернетом.

Реализация программы воспитания

1. Способствовать выработке сознательного и бережного отношения к вопросамсобственной информационной безопасности;
2. Способствовать формированию и развитию нравственных, этических,патриотических качеств личности.
3. Стимулировать поведение и деятельность, направленные на соблюдение информационной безопасности.

Общая характеристика учебного курса

Курс внеурочной деятельности «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.

Программа учебного курса рассчитана на 34 учебных часов

На изучение курса внеурочной деятельности «Информационная безопасность» отводится по 1 часу в неделю в 10 классе.

Личностные, метапредметные и предметные результаты освоения учебного курса

Предметные:

Выпускник 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.Выпускник овладеет:
- приемами безопасной организации своего личного пространства данных с использованием индивидуальных накопителейданных, интернет-сервисов и т.п.

Выпускник получит возможность овладеть:

- основами соблюдения норм информационной этики и права;
- основами самоконтроля, самооценки, принятия решений и осуществления осознанного выбора в учебной и познавательнойдеятельности 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.

Метапредметные

Регулятивные универсальные учебные действия.

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 задачопределенного класса;
- оценивать свою деятельность, аргументируя причины достижения или отсутствия планируемого результата;
- находить достаточные средства для выполнения учебных действий в изменяющейся ситуации и/или приотсутствии 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.

Познавательные универсальные учебные действия

В результате освоения учебного курса обучающийся сможет:

- выделять явление из общего ряда других явлений;
- определять обстоятельства, которые предшествовали возникновению связи между явлениями, из этих обстоятельств выделятьопределяющие, 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.

Коммуникативные универсальные учебные действия.

В результате освоения учебного курса обучающийся сможет:

• строить позитивные отношения в процессе учебной и познавательной деятельности;

• критически относиться к собственному мнению, с достоинством признавать ошибочность своего мнения (если оно таково) икорректировать 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 спомощью средств ИКТ;

• выбирать, строить и использовать адекватную информационную модель для передачи своих мыслей средствами естественныхи 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 правилаинформационной безопасности.

Личностные

• 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 базеориентировки в мире профессий и профессиональных предпочтений, с учетом устойчивых познавательных интересов;

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

• сформированность понимания ценности безопасного образа жизни; интериоризация правил индивидуального и коллективногобезопасного поведения в информационно-телекоммуникационной среде.

Формы проведения занятий:

Формы организации деятельности: групповая, индивидуальная, индивидуально - групповая (3-5 человек). Занятия проводятся в комбинированной, теоретической и практической форме:

- теоретические занятия: основы безопасного поведения при работе с компьютерными программами, информацией в сети интернет, изучение терминов, беседы,лекции;
- практические занятия: работа с мобильными устройствами; закупки в интернет магазине; квесты; создание буклетов и мультимедийных презентаций.

Способы определения планируемых результатов – педагогическое наблюдение, тесты, педагогический анализ результатов анкетирования, тестирования, зачётов, взаимозачётов, опросов, выполнения обучающимися диагностических заданий, участия в мероприятиях, защиты проектов, решения задач поискового характера, активности обучающихся на занятиях и т.п. Для отслеживания результативности можно использовать: педагогический мониторинг, включающий контрольные задания и тесты, диагностикуличностного роста и продвижения, анкетирование, педагогические отзывы, ведение журнала учета или педагогического дневника, ведение оценочной системы; мониторинг образовательной деятельности детей, включающий самооценку обучающегося,

Формами подведения итогов реализации дополнительной общеобразовательной программы «Безопасность в сети Интернет» могут быть выставки буклетов, выполненных обучающимися; проведение квестов; выступления обучающихся по актуальным вопросам информационной безопасности с собственными мультимедийными презентациями на ученических мероприятиях.

Содержание программы

Основное содержание программы представлено разделами «Безопасность общения», «Безопасность устройств», «Безопасность информации».

Каждый раздел курса внеурочной деятельности завершается выполнением проектной работы по одной из тем, предложенныхна выбор учащихся и/или проверочного теста.

Раздел 1. «Безопасность общения»

Тема 1. Общение в социальных сетях и мессенджерах. 2 часа

Социальная сеть. История социальных сетей. Мессенджеры. Назначение социальных сетей и мессенджеров. Пользовательский контент.

Тема 2. С кем безопасно общаться в интернете. 1 час

Персональные данные как основной капитал личного пространства в цифровом мире. Правила добавления друзей в социальныхсетях. Профиль пользователя. Анонимные социальные сети.

Тема 3. Пароли для аккаунтов социальных сетей. 1час

Сложные пароли. Онлайн генераторы паролей. Правила хранения паролей. Использование функции браузера по запоминаниюпаролей.

Тема 4. Безопасный вход в аккаунты. 1 час

Виды аутентификации. Настройки безопасности аккаунта. Работа на чужом компьютере с точки зрения безопасности личногоаккаунта.

Тема 5. Настройки конфиденциальности в социальных сетях. 2 часа

Настройки приватности и конфиденциальности в разных социальных сетях. Приватность и конфиденциальность в мессенджерах.

Тема 6. Публикация информации в социальных сетях. 2 часа

Персональные данные. Публикация личной информации.

Тема 7. Кибербуллинг. 1 час

Определение кибербуллинга. Возможные причины кибербуллинга и как его избежать? Как не стать жертвой кибербуллинга.

Как помочь жертве кибербуллинга.

Тема 8. Публичные аккаунты. 2 часа

Настройки приватности публичных страниц. Правила ведения публичных страниц. Овершеринг.

Тема 9. Фишинг. 2 часа

Фишинг как мошеннический прием. Популярные варианты распространения фишинга. Отличие настоящих и фишинговыхсайтов. Как защититься от фишеров в социальных сетях и мессенджерах.

Раздел 2. «Безопасность устройств»

Тема 1. Что такое вредоносный код. 1 час

Виды вредоносных кодов. Возможности и деструктивные функции вредоносных кодов.

Тема 2. Распространение вредоносного кода. 1 час

Способы доставки вредоносных кодов. Исполняемые файлы и расширения вредоносных кодов. Вредоносная рассылка. Вредоносные скрипты. Способы выявления наличия вредоносных кодов на устройствах. Действия при обнаружениивредоносных кодов на устройствах.

Тема 3. Методы защиты от вредоносных программ. 2 часа

Способы защиты устройств от вредоносного кода. Антивирусные программы и их характеристики. Правила защиты от вредоносных кодов.

Тема 4. Распространение вредоносного кода для мобильных устройств. 2 часа

Расширение вредоносных кодов для мобильных устройств. Правила безопасности при установке приложений на мобильныеустройства.

Раздел 3 «Безопасность информации»

Тема 1. Социальная инженерия: распознать и избежать. 2 часа

Приемы социальной инженерии. Правила безопасности при виртуальных контактах.

Тема 2. Ложная информация в Интернете. 2 часа

Цифровое пространство как площадка самопрезентации, экспериментирования и освоения различных социальных ролей. Фейковые новости. Поддельные страницы.

Тема 3. Безопасность при использовании платежных карт в Интернете. 2 часа

Транзакции и связанные с ними риски. Правила совершения онлайн покупок. Безопасность банковских сервисов.

Тема 4. Беспроводная технология связи. 2 часа

Уязвимость Wi-Fi-соединений. Публичные и непубличные сети. Правила работы в публичных сетях.

Тема 5. Резервное копирование данных. 2 часа

Безопасность личной информации. Создание резервных копий на различных устройствах.

Тема 6. Основы государственной политики в области формирования культуры информационной безопасности. 4 часа

Доктрина национальной информационной безопасности. Обеспечение свободы и равенства доступа к информации знаниям.

Основные направления государственной политики в области формирования культуры информационной безопасности.

Тематическое планирование
курса внеурочной деятельности «Информационная безопасность» в 10 классе

№ п/п	Тема	Кол-во часов	Электронные учебно-методические материалы	Основное содержание	Характеристика основных видов учебной деятельности обучающихся
Тема 1. «Безопасность общения»					
1	Общение в социальных сетях имессенджерах	2	CompSchool. Школа компьютерной грамотности [Электронный ресурс]. - Режим доступа: http: //compschool.ru/categorv /internet	Социальная сеть. История социальных сетей. Мессенджеры. Назначение социальных сетей и мессенджеров. Пользовательский контент.	Выполняет базовые операции при использовании мессенджеров и социальных сетей. Создает свой образ в сети Интернет. Изучает историю и социальную значимость личных аккаунтов в сети Интернет.
2	С кем безопасно общаться в интернете	1	CompSchool. Школа компьютерной грамотности [Электронный ресурс]. - Режим доступа: http: //compschool.ru/categorv /internet	Персональные данные как основной капитал личного пространства в цифровом мире. Правиладобавления друзей в социальных сетях. Профиль пользователя. Анонимные социальные сети.	Руководствуется в общении социальными ценностями и установками коллектива и общества в целом. Изучает правила сетевого общения.
3	Пароли для аккаунтов социальныхсетей	1	http://lbz.ru/metodist/authors/ib/	Сложные пароли. Онлайн генераторыпаролей. Правила хранения паролей. Использование функции браузера по запоминаниюпаролей.	Изучает основные понятия регистрационной информации и шифрования. Умеет их применить.
4	Безопасный вход в аккаунты	1	http://lbz.ru/metodist/authors/ib/	Виды аутентификации. Настройки безопасности аккаунта. Работа на чужом компьютере сточки зрения безопасности личного аккаунта.	Объясняет причины использования безопасного входа при работе на чужом устройстве. Демонстрирует устойчивый навык безопасного входа.

5	Настройки конфиденциальности в социальных сетях	2	http://lbz.ru/metodist/authors/ib/	Настройки приватности и конфиденциальностив разных социальных сетях. Приватность и конфиденциальность в мессенджерах.	Раскрывает причины установки закрытого профиля. Меняет основные настройки приватности в личном профиле.
6	Публикация информации в социальных сетях	2	https://intuit.ru/studies/courses/10/10/info	Персональные данные. Публикация личнойинформации.	Осуществляет поиск и использует информацию, необходимую для выполнения поставленных задач.
7	Кибербуллинг	1	https://intuit.ru/studies/courses/10/10/info	Определение кибербуллинга. Возможные причины кибербуллинга и как его избежать? Как не стать жертвой кибербуллинга. Как помочь жертвекибербуллинга.	Реагирует на опасные ситуации, распознает провокации и попытки манипуляции со стороны виртуальных собеседников.
8	Публичные аккаунты	2	https://intuit.ru/studies/courses/10/10/info	Настройки приватности публичных страниц. Правила ведения публичных страниц. Овершеринг.	Решает экспериментальные задачи. Самостоятельно создает источники информации разного типа и для разных аудиторий, соблюдая правила информационной безопасности.
9	Фишинг	2	https://intuit.ru/studies/courses/10/10/info	Фишинг как мошеннический прием. Популярныевариантыраспространения фишинга. Отличие настоящих и фишинговых сайтов. Как защититься от фишеров в социальных сетяхи мессенджерах.	Анализ проблемных ситуаций. Разработка кейсов с примерами из личной жизни/жизни знакомых. Разработка и распространение чек-листа (памятки) по противодействию фишингу.
Тема 2. «Безопасность устройств»					
1	Что такое вредоносныйкод?	1	http://lbz.ru/metodist/authors/ib/	Виды вредоносных кодов. Возможности и Деструктивные функции вредоносных кодов.	Соблюдает технику безопасности при эксплуатации компьютерных систем. Использует инструментальные программные средства и сервисы адекватно задаче.
2	Распространение вредоносного кода	1	http://lbz.ru/metodist/authors/ib/	Способы доставки вредоносных кодов. Исполняемые файлы и расширения вредоносных кодов. Вредоносная рассылка.	Выявляет и анализирует (при помощи чек-листа) возможные угрозы информационной безопасности объектов.

				Вредоносные скрипты. Способы выявления наличия вредоносных кодов на устройствах. Действия при обнаружении вредоносных кодов на устройствах.	
3	Методы защиты от вредоносных программ	2	http://lbz.ru/metodist/authors/ib/	Способы защиты устройств от вредоносногокода. Антивирусные программы и их характеристики. Правила защиты от вредоносных кодов.	Изучает виды антивирусных программ иправила их установки.
4	Распространение вредоносного кода для мобильных устройств	2	http://lbz.ru/metodist/authors/ib/	Расширение вредоносных кодов для мобильныхустройств. Правила безопасности при установке приложений на мобильные устройства.	Разрабатывает презентацию, инструкцию по обнаружению, алгоритм установки приложений на мобильные устройства для учащихся более младшего возраста.
Тема 3 «Безопасность информации»					
1	Социальная инженерия: распознать и избежать	2	http://lbz.ru/metodist/authors/ib/	Приемы социальной инженерии. Правила безопасности при виртуальных контактах.	Находит нужную информацию в базах данных, составляя запросы на поиск. Систематизирует получаемую информацию в процессе поиска.
2	Ложная информация в Интернете	2	http://lbz.ru/metodist/authors/ib/	Цифровое пространство как площадка самопрезентации, экспериментирования и освоения различных социальных ролей. Фейковые новости. Поддельные страницы.	Определяет возможные источники необходимых сведений, осуществляет поиск информации. Отбирает и сравнивает материал по нескольким источникам. Анализирует и оценивает достоверность информации.
3	Безопасность при использовании платежных карт в Интернете	2	https://intuit.ru/studies/courses/10/10/info	Транзакции и связанные с ними риски. Правила совершения онлайн покупок. Безопасность банковских сервисов.	Приводит примеры рисков, связанных с совершением онлайн покупок (умеет определить источник риска). Разрабатывает возможные варианты

					решения ситуаций, связанных с рисками использования платежных карт в Интернете.
4	Беспроводная технология связи	2	https://intuit.ru/studies/courses/10/10/info	Уязвимость Wi-Fi-соединений. Публичные и непубличные сети. Правила работы в публичных сетях.	Используя различную информацию, определяет понятия. Изучает особенности и стиль ведения личных и публичных аккаунтов.
5	Резервное копирование данных	2	https://intuit.ru/studies/courses/10/10/info	Безопасность личной информации. Создание резервных копий на различныхустройствах.	Создает резервные копии.
6	Основы Государственной политики в области формирования культуры информационной безопасности	4	https://intuit.ru/studies/courses/10/10/info	Доктрина национальной информационной безопасности. Обеспечение свободы и равенства доступа к информации изнаниям. Основные направления государственной политики в области формирования культуры информационной безопасности.	Умеет привести выдержки из законодательства РФ: - обеспечивающего конституционное правона поиск, получение и распространение информации; - отражающего правовые аспекты защиты киберпространства.
Итого:		**34 часа**			

Муниципальное общеобразовательное учреждение
«Средняя общеобразовательная школа п. Белоярский
Новобурасского района Саратовской области
имени Бабушкина А.М»

«Принято»	«Согласовано»	«Утверждаю»
Руководитель МО	Заместитель руководителя по ВР МОУ «СОШ п.Белоярский имени Бабушкина А.М.»	Руководитель МОУ «СОШ п.Белоярский имени Бабушкина А.М.»
_____/ Лозе Е.Н /	_____/Максимова С.В./	_____/Юркина С.А./
подпись ФИО	подпись ФИО	подпись ФИО
Протокол № 1 от «28»августа 2023г.	«28»_08_2023_г.	Приказ №82 от «28»_08_2023г.

КАЛЕНДАРНО-ТЕМАТИЧЕСКОЕ ПЛАНИРОВАНИЕ

по внеурочной деятельности «Информационная безопасность» в 10 классе
педагога дополнительного образования Центра образования цифрового и гуманитарного профилей «Точка роста» Дряпак Людмилы Николаевны, первой категории

Рассмотрено на заседании
педагогического совета
протокол № 1
от «28» августа 2023 г.

2023- 2024 учебный год

Календарно-тематическое планирование

№ п/п	Тема урока	Кол-во часов	Дата		Коррекция
			план		
1	Общение в социальных сетях и мессенджерах	1	6.09		
2	Общение в социальных сетях и мессенджерах	1	13.09		
3	С кем безопасно общаться в интернете	1	20.09		
4	Пароли для аккаунтов социальных сетей	1	27.09		
5	Безопасный вход в аккаунты	1	4.10		
6	Настройки конфиденциальности в социальных сетях	1	11.10		
7	Настройки конфиденциальности в социальных сетях	1	18.10		
8	Публикация информации в социальных сетях	1	25.10		
9	Публикация информации в социальных сетях	1	8.11		
10	Кибербуллинг	1	15.11		
11	Публичные аккаунты	1	22.11		
12	Публичные аккаунты	1	29.11		
13	Фишинг	1	6.12		
14	Фишинг	1	13.12		
15	Что такое вредоносныйкод?	1	20.12		
16	Распространение вредоносного кода	1	27.12		
17	Методы защиты от вредоносных программ	1	10.01		
18	Методы защиты от вредоносных программ	1	17.01		
19	Распространение вредоносного кода для мобильных устройств	1	24.01		
20	Распространение вредоносного кода для мобильных устройств	1	31.01		
21	Социальная инженерия: распознать и избежать	1	7.02		
22	Социальная инженерия: распознать и избежать	1	14.02		
23	Ложная информация вИнтернете	1	21.02		
24	Ложная информация вИнтернете	1	28.02		

25	Безопасность прииспользовании платежных карт в Интернете	1	6.03		
26	Безопасность прииспользовании платежных карт в Интернете	1	13.03		
27	Беспроводная технология связи	1	20.03		
28	Беспроводная технология связи	1	3.04		
29	Резервное копирование данных	1	10.04		
30	Резервное копирование данных	1	17.04		
31	Основы Государственной политики в области формированиякультуры информационной безопасности	1	24.04		
32	Основы Государственной политики в области формированиякультуры информационной безопасности	1	8.05		
33	Основы Государственной политики в области формированиякультуры информационной безопасности	1	15.05		
34	Основы Государственной политики в области формированиякультуры информационной безопасности	1	22.05		

УЧЕБНО-МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ОБРАЗОВАТЕЛЬНОГО ПРОЦЕССА

ОБЯЗАТЕЛЬНЫЕ УЧЕБНЫЕ МАТЕРИАЛЫ ДЛЯ УЧЕНИКА

• Информационная безопасность. Учебники для 10-11 классов Авторы: Цветкова М.С. и др.

Общество с ограниченной ответственностью «БИНОМ. Лаборатория знаний» ;Акционерное общество «Издательство «Просвещение»

МЕТОДИЧЕСКИЕ МАТЕРИАЛЫ ДЛЯ УЧИТЕЛЯ

• Информационная безопасность. Учебники для 10-11 классов Авторы: Цветкова М.С. и др.

Общество с ограниченной ответственностью «БИНОМ. Лаборатория знаний» ;
Акционерное общество «Издательство «Просвещение»

Бирюков А.А. Информационная безопасность защита и нападение 2 е издание: Издательство: ДМК-Пресс., 2017, 434 с.

- Бирюков А.А. Информационная безопасность защита и нападение.: Издательство: ДМК-Пресс., 2018, 474 с.
- Колесниченко Денис. Анонимность и безопасность в интернете. От чайника к пользователю. Самоучитель Издательство: БХВ-Петербург, 2018, 240с.
- Мазаник Сергей. Безопасность компьютера. Защита от сбоев, вирусов и неисправностей: издательство: ЭКСМО, 2019, 256 с.
- Проскурин В.Г Защита в операционных системах: Издательство: Горячая линия-Телеком, 2019, 192 с.
- Савченко Е. Кто, как и зачем следит за вами через интернет: Москва - Третий Рим, 2019, 100 с.
- Яковлев В.А.Шпионские и антишпионские штучки: Техническая литература Издательство: Наука и Техника, 2018, 320 с.

ЦИФРОВЫЕ ОБРАЗОВАТЕЛЬНЫЕ РЕСУРСЫ И РЕСУРСЫ СЕТИ ИНТЕРНЕТ

https://bosova.ru/metodist/authors/informatika/3/eor10.php

https://intuit.ru/studies/courses/10/10/info

https://resh.edu.ru