Департамент образования Администрации города Тюмени
МАОУ СОШ № 25 г. Тюмени

Рассмотрено:
МО учителей естественно-научного цикла
Руководитель МО
Ясиновских Н. Н.
_____
Протокол № 1
от 28 августа 2023 г

Согласовано:
Заместитель директора по УВР
Ясиновских Н.Н.
_____
«28» августа 2023г

Утверждаю:
Директор Дубонос С.М.
_____
Приказ № 178-02
от «31» августа 2023г.

РАБОЧАЯ ПРОГРАММА
элективного курса
«Информационная безопасность»
для обучающихся 10-11 классов
среднего общего образования

Составители:
Куприянова Н.А.
Лебедева М.В.

Тюмень, 2023

Рабочая программа элективного курса «Информационная безопасность» на уровне среднего общего образования составлена на основе требований к результатам освоения ФОП СОО, утвержденной приказом Министерства просвещения РФ от 18.05.2023 № 371; планируемым результатам обучения в соответствии с обновленным ФГОС СОО, утвержденным приказом Министерства просвещения РФ от 12.08. 2022 г. №732; Федеральной рабочей программой по информатике, а также с учётом федеральной рабочей программы воспитания, Концепции преподавания математики и информатики в Российской Федерации (утверждённой распоряжением Правительства Российской Федерации от 9 апреля 2016 г. № 637-р).

Рабочая программа по данному элективному курсу представляет собой методически оформленную конкретизацию требований, обновленных ФГОС СОО и раскрывает их реализацию через конкретное предметное содержание.

Рабочая программа по элективному курсу «Информационная безопасность» в 10-11 классах является составной частью основной образовательной программы среднего общего образования МАОУ СОШ № 25 города Тюмени.

Составлена на основе

- Рабочей программы курса «Информационная безопасность» Для 10-11 классов Авторы составители: Четверов Алексей Владимирович, ГБОУ Школа №1409, специалист по детской онлайн безопасности «Лаборатория Касперского» и Сиденко Андрей Григорьевич, руководитель направления по детской онлайн безопасности «Лаборатория Касперского»

Профессиональных стандартов

- 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).
- 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).
- 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).
- 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).
- 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)

Элективный курс «ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ» является частью образовательной программыдля ИТ-классов средней школы и для классов других профилей.

Курс носит междисциплинарный характер и может быть фактически разнесен между часами,отведенными на элективные

дисциплины и внеурочную деятельность. Предлагаемая программа соответствует положениям федерального государственного образовательногостандарта среднего общего образования.

Программа курса отражает способы формирования универсальных учебных действий,составляющих основу для профессионального самоопределения, саморазвития и непрерывного образования, выработки коммуникативных качеств, целостности общекультурного, личностного и познавательного развития учащихся.

ПОЯСНИТЕЛЬНАЯ ЗАПИСКА

Программа соответствует требованиям к структуре программ, заявленным в ФГОС, ивключает следующие разделы:

- Пояснительная записка, в которой уточняются общие цели образования с учетом специфики курса.
- Общая характеристика курса, содержащая ценностные ориентиры образования по технологическому профилю.
- Место данного курса в учебном плане.
- Результаты освоения курса (личностные, метапредметные и предметные), соответствующие глобальным целям образования по технологическому профилю и принципу развивающего обучения, лежащему в основе предлагаемой программы. Содержание курса по направлению «Информационная безопасность» в 10 и 11 классах.
- Тематическое планирование, которое дает представление об основных видах учебной деятельности в процессе освоения курса в 10-11 классах основной школы.
- Рекомендации по учебно-методическому и материально-техническому обеспечению образовательного процесса.
- Планируемые результаты освоения программы. Принципы и подходы к формированию программы Стандарт второго поколения (ФГОС) в сравнении со стандартом первого поколения

предполагает деятельностный подход к обучению, где главная цель: развитие личности учащегося. Система образования отказывается от традиционного представления результатов обучения в виде знаний, умений и навыков. Формулировки стандарта указывают реальные виды деятельности, которыми следует овладеть к концу обучения, т. е. обучающиеся должны уметь учиться, самостоятельно добывать знания, анализировать, отбирать нужную информацию, уметь контактировать в различных по возрастному составу группах. Информационная безопасность - междисциплинарный комплекс знаний и умений. Для того чтобы обучающийся достиг приемлемого уровня знаний и умений в сфере информационной безопасности, он должен владеть знаниями и

умениями в следующих сферах: математика, информатика, инфокоммуникационные технологии и системы, физика, программирование, технические средства защиты информации, криптография, основы вирусологии. Раннее начало изучения практической области информационной безопасности по отношению к теоретическим знаниям, получаемым в рамках таких дисциплин, как информатика, математика, введение в информационную безопасность, позволяют сформировать более высокий интерес к освоению этих теоретических дисциплин и показывают учащемуся практическое значение теоретических знаний. Состав участников образовательного процесса

Программа среднего общего образования рассчитана на реализацию в 10 - 11 классах общеобразовательных учреждений и учреждений с углубленным изучением отдельных предметов, и нацелена на возрастную категорию учащихся 15 – 18 лет.

Общая характеристикаучебного курса

Представленная программа направления «Информационная безопасность» (10-11 класс)» предназначена для практического освоения учащимися:

- защиты личного информационного пространства;
- обслуживание информационно-коммуникационной системы;
- обслуживание сетевых устройств информационно-коммуникационной системы;
- обслуживание серверных операционных систем информационно-коммуникационнойсистемы;
- обеспечение защиты средств связи сетей электросвязи от несанкционированногодоступа к ним;
- обслуживание средств защиты информации в компьютерных системах и сетях;
- обслуживания систем защиты информации в автоматизированных системах;
- обеспечение защиты информации в автоматизированных системах в процессе ихэксплуатации;
- оценивание уровня безопасности компьютерных систем и сетей;
- администрирование средств защиты информации в компьютерных системах и сетях.

Программа рассчитана на 2 года (10-11 класс), и состоит из 18 тем: основы информационной безопасности; направления обеспечения информационной безопасности; защита информации; основы теории чисел; криптография; стеганография; основы операционных систем; законодательство в сфере информационной безопасности; вредоносные программы; программно-технические средства защиты информации; вычислительные сети; социальная инженерия; анализ безопасности веб-проектов; процессы, связанные с обеспечением защиты данных; обеспечение безопасности вычислительных сетей; эшелонированная

оборона; интернет вещей.

При этом обучение можно условно разделить на 4 модуля:

Модуль 1. Введение в информационную безопасность. Посвящен введению в информационную безопасность, изучению направлений обеспечения информационной безопасности, способам защиты информации с использованием различных шифров и алгоритмов, методам сокрытия факта передачи информации в цифровых объектах и связанных с этими процессами угрозами.

Модуль 2. Элементы информационной безопасности в вычислительных сетях. Посвящен способам защиты информации при передаче по открытым каналам связи, угрозам информационной безопасности и способам защиты от них в вычислительных сетях.

Модуль 3. Элементы информационной безопасности программного обеспечения. Посвящен основам и администрированию операционных систем семейств Windows и Linux, языку Асемблер, законодательству Российской федерации в сфере защиты информации и авторского права, основам вирусологии и вредоносных программ.

Модуль 4. Элементы защиты информации в вычислительных системах. Посвящен Программно-техническим средствам защиты информации, процессам связанных с обеспечением информационной безопасности вычислительных систем.

Цели и задачи реализации основной
образовательной программы основного общегообразования по курсу

Элективный курс по профилю «Информационная безопасность» специально разработан для формирования у будущих специалистов компетенций в области обеспечения информационной безопасности, правовых аспектов информационной безопасности, кибербезопасности, а также получения базовых знаний по криптографии и элементам сетевой безопасности, обеспечения информационной безопасности личного пространства.

Цели курса

- Сформировать у будущих специалистов компетенций в 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 курса

- создать условия для формирования умений, необходимых для различных форм безопасной коммуникации (электронная почта, чаты, блоги, форумы, социальные сети и др.) с различными целями и ответственного отношения к взаимодействию в современной информационно-телекоммуникационной среде;
- дать представление о видах и способах распространения вредоносных кодов, способов защиты личных устройств;
- познакомить со способами защиты от противоправных посягательств в Интернете, защиты личных данных;
- познакомить со стандартами информационного взаимодействия систем;
- познакомить с конструкциями типичных элементов линий передачи информации;
- сформировать умения задавать базовые параметры, в том числе параметры защиты от несанкционированного доступа к операционным системам, а так же настройки конфигурации операционных систем сетевых устройств;
- познакомить с архитектурой, устройством и функционированием вычислительных систем;
- сформировать знания в области обеспечения защиты информации в вычислительных сетях и системах;
- сформировать знания в области типовых и программно-аппаратных средств защиты информации в операционных системах.

Планируемые результаты изучения курса

Личностные

- сформированность основ саморазвития и самовоспитания в соответствии с общечеловеческими ценностями и идеалами гражданского общества; готовность и способность к самостоятельной, творческой и ответственной деятельности;
- толерантное сознание и поведение в поликультурном мире, готовность и способность вести диалог с другими людьми, достигать в нем взаимопонимания, находить общие цели и сотрудничать для их достижения, способность противостоять идеологии экстремизма, национализма, ксенофобии, дискриминации по социальным, религиозным, расовым, национальным признакам и другим негативным социальным явлениям;
- навыки сотрудничества со сверстниками, детьми младшего возраста, взрослыми в образовательной, общественно полезной, учебно-исследовательской, проектной и других видахдеятельности;

- нравственное сознание и поведение на основе усвоения общечеловеческих ценностей;
- 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;
- осознанный выбор будущей профессии и возможностей реализации собственных жизненных планов; отношение к профессиональной деятельности как возможности участия в решении личных, общественных, государственных, общенациональных проблем;
- принятие и реализацию ценностей здорового и безопасного образа жизни правил индивидуального и коллективного безопасного поведения в информационно- телекоммуникационной среде.

Предметные

Выпускник научится:

- безопасно использовать средства коммуникации;
- безопасно использовать ресурсы интернета;
- идентифицировать типичные инциденты;
- задавать базовые параметры, в том числе параметры защиты от несанкционированногодоступа к операционным системам;
- настраивать и управлять сетевыми устройствами;
- использовать процедуры восстановления данных;
- определять точки восстановления данных;
- производить мониторинг администрируемых сетевых устройств информационно-коммуникационных систем;
- применять внешние программно-аппаратные средства для контроляпроизводительности сетевой инфраструктуры;
- устанавливать и настраивать параметры сетевых протоколов, реализованных втелекоммуникационном оборудовании;
- применять программно-аппаратные средства защиты информации в операционныхсистемах;
- применять антивирусные средства защиты информации в операционных системах;
- анализировать компьютерную систему с целью определения уровня защищенности;
- использовать типовые криптографические средства защиты информации;

- классифицировать и оценивать угрозы информационной безопасности;
- изготавливать защищенное техническое средство или систему обработки информации.

Выпускник овладеет:

- основами правовых аспектов использования компьютерных программ и работы вИнтернете;
- представлениями о влиянии информационных технологий на жизнь человека вобществе;
- знаниями об "операционных системах" и основных функциях операционных систем;
- знаниями об общих принципах разработки и функционирования интернет-приложений;
- представлениями о компьютерных сетях и их роли в современном мире;
- приемами безопасной организации своего личного пространства данных сиспользованием индивидуальных накопителей данных, интернет-сервисов и т.п.
- навыками и умениями безопасного и целесообразного поведения при работе скомпьютерными программами и в Интернете;
- основными навыками и умениями использования компьютерных устройств.

Выпускник получит возможность овладеть:

- навыками инженерного мышления;
- навыками работы с реальными программно-аппаратными комплексами;
- навыками оценивания уровня безопасности компьютерных систем; навыкамиобеспечения информационной безопасности личного пространства;
- различными источниками информации, включая Интернет-ресурсы и другие базыданных для решения коммуникативных задач в области безопасности жизнедеятельности.

Метапредметные

- умение 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;
- умение продуктивно общаться и взаимодействовать в процессе совместной деятельности, учитывать позиции других участников

деятельности, эффективно разрешатьконфликты;

- владение навыками познавательной, учебно-исследовательской и проектной деятельности, навыками разрешения проблем; способность и готовность к самостоятельному поиску методов решения практических задач, применению различных методов познания;
- готовность и способность к самостоятельной информационно-познавательной деятельности, владение навыками получения необходимой информации из словарей разных типов, умение ориентироваться в различных источниках информации, критически оценивать и интерпретировать информацию, получаемую из различных источников;
- умение использовать средства информационных и коммуникационных технологий (далее - ИКТ) в решении когнитивных, коммуникативных и организационных задач с соблюдением требований эргономики, техники безопасности, гигиены, ресурсосбережения, правовых и этических норм, норм информационной безопасности;
- умение определять назначение и функции различных социальных институтов;
- умение самостоятельно оценивать и принимать решения, определяющие стратегию поведения, с учетом гражданских и нравственных ценностей;
- владение языковыми средствами - умение ясно, логично и точно излагать свою точку зрения, использовать адекватные языковые средства;
- владение навыками познавательной рефлексии как осознания совершаемых действий и мыслительных процессов, их результатов и оснований, границ своего знания и незнания, новыхпознавательных задач и средств их достижения.

СОДЕРЖАНИЕ КУРСА Рабочей программой предусмотрен следующий тематический план, который представлен втаблице 1.
Таблица 1. Тематический план.

№ п/п	Модуль	Наименование раздела	Количество часов
10 класс -34 часа			
1.	Введение в информационную безопасность	Основы Информационнойбезопасности.	3
2.		Направления обеспечения информационной безопасности	3
3.		Защита информации методамисимметричного шифрования	4
4.		Стеганография	6
5.	Элементы информационной безопасности в вычислительных сетях	Криптография	9
6.		Вычислительные сети	9
11 класс – 33 часа			
7.	Элементы информационной безопасности программного обеспечения.	Основы операционных систем	3
8.		Законодательство в сфере информационной безопасности	3
9.		Вредоносные программы	4
10.	Элементы защиты информации в вычислительных системах	Программно-технические средствазащиты информации	3
11		Социальная инженерия	2
12.		Анализ безопасности веб-проектов	4

13.		Процессы, связанные с обеспечениемзащиты данных	2
14.		Обеспечение безопасностивычислительных сетей	4
15.		Эшелонированная оборона	3
16.		Интернет вещей	5

Краткое содержание разделов

Раздел 1. Основы Информационной безопасности. Что представляет собой кибербезопасность и почему потребность в специалистах по кибербезопасности продолжает расти. Что такое организационные данные и почему их важно защищать? Кто такие киберпреступники и что им нужно. Рассматриваются примеры атак, нарушений безопасности, а так же цели защиты. Разбор некоторых примеров атак на информационные системы.

Раздел 2. Направления обеспечения информационной безопасности. Технические каналы утечки информации: технический, электромагнитный, оптический. Средствазащиты от технических угроз. Экономическая модель защиты информации.

Раздел 3. Защита информации методами симметричного шифрования. Симметричные шифры: шифры древней спарты, шифр Брайля, атбаш, Цезаря, Гросфельда, Виженера, вертикальной перестановки, афинный шифр, шифр Хилла, Плейфера, Вернама. Представление информации в формате BASE64

Раздел 4. Стеганография. Исторический обзор стеганографических систем. Описание стеганографических систем. Основные угрозы и типы нарушителей безопасности стеганографических систем. Типы атак на различные стеганографические системы.

Раздел 5. Основы теории чисел. Целые числа, простые числа, позиционные системы счисления. Сравнения по модулю. Уравнения в целых числах. Теория множеств, множества и функции, комбинаторика, вероятность и случайность. **Криптография.** Криптоанализ симметричных шифров. Статистическая устойчивость шифротекстов. Односторонние функции. Передачи зашифрованных сообщений и ключей шифрования по открытым каналам связи. Хеш функции. **Вычислительные сети.** Виды сетей, топология сетей,

компоненты сетей. Сетевая модель OSI. Введение в Packet Tracer и создание виртуальных сетей. Защита вычислительных сетей от внешних и внутренних угроз. Виртуальные частные и анонимные сети.

Раздел 6. Основы операционных систем. Архитектура вычислительных машин. Язык Ассемблер. Основы администрирования Операционных систем Windows и Linux. Установкаи настройка специальных операционных систем

Раздел 7. Законодательство в сфере информационной безопасности. Авторское право и лицензии. Коммерческая тайна и способы ее защиты. Персональные данные и правила обращения с ними.

Раздел 8. Вредоносные программы. Классификация вредоносных программ: Троянская программа, Вирус, Червь, программы шпионы, рекламные программы.

Раздел 9. Программно-технические средства защиты информации. Антивирусные программы и принципы их работы.

Раздел 10. Социальная инженерия. Сбор информации и профайлинг. Доксинг. Методы социальной инженерии.

Раздел 11. Анализ безопасности веб-проектов. Техники аудита безопасности веб- проектов. Общие знания относительно рисков, сопровождающих современные интернет- приложения. Методики анализа безопасности клиент-серверных приложений. Методики анализа кода. Архитектурный анализ.

Раздел 12. Процессы, связанные с обеспечением защиты данных. Сертификаты. LDAP. RADIUS. Kerberos. Контроль доступа. Методы обеспечения процессов авторизации иучета.

Раздел 13. Обеспечение безопасности вычислительных сетей. Контроль сетевого трафика. Архитектура безопасной сети. Защита беспроводных сетей.

Раздел 14. Эшелонированная оборона. Безопасность системы и приложений, Основные правила для защиты операционных систем и отключение ненужных компонентов системы. Настройка локальных браундмаеров. Управление правилами приложений.

Раздел 15. Интернет вещей. Что такое интернет вещей. Безопасность трафика, генерируемого интернетом вещей. Безопасность интернет вещей. Интернет вещей в бизнесе и на предприятиях. Автоматизация посредством интернета вещей.

УЧЕБНО-МЕТОДИЧЕСКОЕ И МАТЕРИАЛЬНО-

ТЕХНИЧЕСКОЕОБЕСПЕЧЕНИЕ ОБРАЗОВАТЕЛЬНОГОПРОЦЕССА.

Программное обеспечение (в том числесистемное ПО)

1. Анализатор базовой безопасности Microsoft: Microsoft Baseline Security Analyzer(бесплатная);
2. Операционная система Winows 10 или Winows 11;
3. am.Requirements (распространяется свободно);
4. AnyLogic 8.75 Personal Learning Edition (бесплатная);
5. Arduino IDE 1.8.15 (распространяется свободно);
6. Astra linux common edition (распространяется свободно);
7. Cisco Packet Tracer (бесплатная);
8. CoppeliaSim V4.2.0 rev5 EDU (распространяется свободно);
9. Enigmail for Thunderbird 2.1.9 (распространяется свободно);
10. fping 5.0 (распространяется свободно);
11. Google Chrome (распространяется свободно);
12. Gpg4win 3.1.16 (распространяется свободно);
13. Kaspersky Security Cloud;
14. Kaspersky Total Security;
15. KasperskyOS Community Edition (бесплатная);
16. Microsoft Security Assessment tool (бесплатная);
17. Mosquitto 2.0.11 (распространяется свободно);

18. nmap 7.91 (распространяется свободно);
19. PyCharm community edition (бесплатная);
20. Tails 4.20 (распространяется свободно);
21. The Amnesic Incognito Live System (распространяется свободно);
22. Thunderbird 78.0 (распространяется свободно);
23. Ubuntu for Raspberry Pi (распространяется свободно);
24. Ubuntu Server 18.04.5 (распространяется свободно);
25. VirtualBox 6.1 (распространяется свободно);
26. Visual Studio Code (распространяется свободно);
27. Wireshark is 3.4.6. (распространяется свободно);

Список учебной и методической литературы, идругие источники:

1. Абросимов, Л. И. Базисные методы проектирования и анализа сетей ЭВМ : учебное пособие / Л. И. Абросимов. — Санкт-Петербург : Лань, 2021. — 212 с. — ISBN 978-5-8114-3538-8. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/169320 (дата обращения: 13.07.2021). — Режим доступа: для авториз.пользователей.
2. Бирюков, А.А. Информационная безопасность: защита и нападение [Электронный ресурс] / А.А. Бирюков. — Электрон. дан. — Москва : ДМК Пресс, 2017. — 434 с. — Режим доступа: https://e.lanbook.com/book/93278. — Загл. с экрана.
3. Введение в сетевые технологии - https://stepik.org/course/58678/info
4. Внуков, А. А. Защита информации : учебное пособие для бакалавриата и магистратуры / А. А. Внуков. — 2-е изд., испр. и доп. — М. : Издательство Юрайт, 2018. — 261 с. — (Серия : Бакалавр и магистр. Академический курс). — ISBN 978-5-534-01678-9. — Режим доступа : www.biblio-online.ru/book/73BEF88E-FC6D-494A-821C-D213E1A984E1.
5. Вьюненко, Л. Ф. Имитационное моделирование : учебник и практикум для академического бакалавриата / Л. Ф. Вьюненко, М. В. Михайлов, Т. Н. Первозванская ; под ред. Л. Ф. Вьюненко. — М. : Издательство Юрайт, 2016. — 283 с. — (Бакалавр. Академический курс). — ISBN 978-5- 9916-6428-8. [Электронный ресурс]— Режим доступа: https://www.biblioonline.ru/book/BEE05A5A-1AB0-4A08-ADB1-70BC357B6C20— Загл. с экрана.

6. Гилязова, Р. Н. Информационная безопасность. Лабораторный практикум : учебное пособие / Р. Н. Гилязова. — Санкт-Петербург : Лань, 2020. — 44 с. — ISBN 978-5-8114-4294-2. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/130179 (дата обращения: 13.07.2021). — Режим доступа: для авториз.пользователей.

7. Грибунин В.Г., Оков И.Н., Туринцев И.В. Цифровая стеганография - М.: Солон-Пресс, 2017. — 262 с. — ISBN 978-5-91359-173-9.

8. Давидюк Н.В. Обеспечение безопасности абонентского телетрафика путём конфигурирования и настройки маршрутизатора (на примере MikroTik RouterBOARD) - Практикум. — СПб.: Интермедия, 2020. — 68 с. — ISBN 978-5-4383-0195-0

9. Ермакова, А. Ю. Криптографические методы защиты информации : учебно-методическое пособие / А. Ю. Ермакова. — Москва : РТУ МИРЭА, 2021. — 172 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/176563 (дата обращения:13.07.2021). — Режим доступа: для авториз. пользователей.

10. Журавлев, А. Е. Инфокоммуникационные системы: протоколы, интерфейсы и сети. Практикум : учебное пособие для спо / А. Е. Журавлев. — Санкт-Петербург : Лань, 2020. — 192 с. — ISBN 978-5-8114-5633-8. — Текст : электронный // Лань : электронно-библиотечная система.
— URL: https://e.lanbook.com/book/152624 (дата обращения: 13.07.2021). — Режим доступа: дляавториз. пользователей.

11. Журавлев, А. Е. Инфокоммуникационные системы. Аппаратное обеспечение : учебник для вузов / А. Е. Журавлев, А. В. Макшанов, А. В. Иванищев. — 2-е изд., стер. — Санкт-Петербург : Лань, 2021. — 392 с. — ISBN 978-5-8114-8514-7. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/176657 (дата обращения: 13.07.2021). Режим доступа: для авториз. пользователей.

12. Журавлев, А. Е. Инфокоммуникационные системы. Программное обеспечение : учебник для вузов / А. Е. Журавлев, А. В. Макшанов, А. В. Иванищев. — 2-е изд., стер. — Санкт-Петербург
: Лань, 2021. — 376 с. — ISBN 978-5-8114-8515-4. — Текст : электронный // Лань : электронно- библиотечная система. — URL: https://e.lanbook.com/book/176658 (дата обращения: 13.07.2021).
— Режим доступа: для авториз. пользователей.

13. Зайцев, А. П. Технические средства и методы защиты информации : учебник / А. П. Зайцев, Р. В. Мещеряков, А. А. Шелупанов. — 7-е изд., испр. — Москва : Горячая линия-Телеком, 2018. — 442 с. — ISBN 978-5-9912-0233-6. — Текст : электронный // Лань : электронно- библиотечная система. — URL: https://e.lanbook.com/book/111057 (дата обращения: 13.07.2021).
Режим доступа: для авториз. пользователей.

14. Кибербезопасность: что нужно знать о новом виде защиты? - https://stepik.org/course/69690/syllabus

15. Кобылянский, В. Г. Операционные системы, среды и оболочки : учебное пособие для вузов / В. Г. Кобылянский. — 3-е изд., стер. — Санкт-Петербург : Лань, 2021. — 120 с. — ISBN 978-5-8114-8187-3. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/173109 (дата обращения: 13.07.2021). — Режим доступа: для авториз.пользователей.

16. Краковский, Ю. М. Методы защиты информации : учебное пособие для вузов / Ю. М. Краковский. — 3-е изд., перераб. — Санкт-Петербург : Лань, 2021. — 236 с. — ISBN 978-5-8114- 5632-1. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/156401 (дата обращения: 13.07.2021). — Режим доступа: для авториз.пользователей.

17. Кутузов, О. И. Инфокоммуникационные системы и сети : учебник для вузов / О. И. Кутузов, Т. М. Татарникова, В. В. Цехановский. — 2-е изд., стер. — Санкт-Петербург : Лань, 2021. — 244 с. — ISBN 978-5-8114-8051-7. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/171410 (дата обращения: 13.07.2021). — Режим доступа: дляавториз. пользователей.

18. Лившиц И.И. Нормативно-методическое обеспечение информационной безопасности - Учебно-методическое пособие. – СПб: Университет ИТМО, 2021. – 68 с.

19. Маркина Т.А. Основные механизмы защиты в ОС MS Windows. Методические рекомендации по выполнению лабораторных работ - СПб.: Университет ИТМО, 2020. — 34 с.

20. Мартынов, Л. М. Алгебра и теория чисел для криптографии : учебное пособие / Л. М. Мартынов. — Санкт-Петербург : Лань, 2020. — 456 с. — ISBN 978-5-8114-4424-3. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/140740 (дата обращения: 13.07.2021). — Режим доступа: для авториз.пользователей.

21. Математика в кибербезопасности - https://stepik.org/course/62247/syllabus

22. Молдовян А.А., Молдовян Д.Н., Левина А.Б. Молдовян А.А., Молдовян Д.Н., Левина А.Б. Протоколы аутентификации с нулевым разглашением секрета. – СПб: Университет ИТМО, 2016. http://books.ifmo.ru/file/pdf/1887.pdf

23. Нестеров, С. А. Основы информационной безопасности : учебник для вузов / С. А. Нестеров. — Санкт-Петербург : Лань, 2021. — 324 с. — ISBN 978-5-8114-6738-9. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/165837 (дата обращения: 13.07.2021). — Режим доступа: для авториз.пользователей.

24. Никифоров, С. Н. Методы защиты информации. Защита от внешних вторжений : учебное пособие для спо / С. Н. Никифоров. — 2-е изд., стер. — Санкт-Петербург : Лань, 2021. — 96 с. — ISBN 978-5-8114-7906-1. — Текст : электронный // Лань : электронно-библиотечная система. —

URL: https://e.lanbook.com/book/167185 (дата обращения: 13.07.2021). — Режим доступа: для авториз. пользователей.

25. Никифоров, С. Н. Методы защиты информации. Защищенные сети : учебное пособие / С. Н. Никифоров. — Санкт-Петербург : Лань, 2021. — 96 с. — ISBN 978-5-8114-3099-4. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/169311 (дата обращения: 13.07.2021). — Режим доступа: для авториз.пользователей.

26. Никифоров, С. Н. Методы защиты информации. Пароли, скрытие, шифрование : учебное пособие для спо / С. Н. Никифоров. — 2-е изд., стер. — Санкт-Петербург : Лань, 2021. — 124 с.

— ISBN 978-5-8114-8256-6. — Текст : электронный // Лань : электронно-библиотечная система.

— URL: https://e.lanbook.com/book/173803 (дата обращения: 13.07.2021). — Режим доступа: дляавториз. пользователей.

27. Никифоров, С. Н. Методы защиты информации. Шифрование данных : учебное пособие

/ С. Н. Никифоров. — 2-е изд., стер. — Санкт-Петербург : Лань, 2019. — 160 с. — ISBN 978-5- 8114-4042-9. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/114699 (дата обращения: 13.07.2021). — Режим доступа: для авториз. пользователей.

28. Новиков, В.К. Организационно-правовые основы информационной безопасности (защиты информации). Юридическая ответственность за правонарушения в области информационной безопасности (защиты информации) [Электронный ресурс] : учебное пособие

/ В.К. Новиков. — Электрон. дан. — Москва : Горячая линия-Телеком, 2017. — 176 с. — Режим доступа: https://e.lanbook.com/book/111084. — Загл. с экрана.

29. Олифер, В.Г. Компьютерные сети принципы, технологии, протоколы / В.Г. Олифер, Н.А. Олифер. - М.: СПб: Питер, 2016. - 672

30. Операционные системы. Программное обеспечение : учебник. — Санкт-Петербург : Лань, 2020. — 248 с. — ISBN 978-5-8114-4290-4. — Текст : электронный // Лань : электронно- библиотечная система. — URL: https://e.lanbook.com/book/148222 (дата обращения: 13.07.2021).

— Режим доступа: для авториз. пользователей.

31. Петренко, В. И. Защита персональных данных в информационных системах. Практикум : учебное пособие для вузов / В. И. Петренко, И. В. Мандрица. — 3-е изд., стер. — Санкт-Петербург

: Лань, 2021. — 108 с. — ISBN 978-5-8114-8370-9. — Текст : электронный // Лань : электронно- библиотечная система. — URL: https://e.lanbook.com/book/175506 (дата обращения: 13.07.2021). Режим доступа: для авториз. пользователей.

32. Петренко, В. И. Защита персональных данных в информационных системах. Практикум : учебное пособие для спо / В. И. Петренко, И. В. Мандрица. — Санкт-Петербург : Лань, 2021. — 108 с. — ISBN 978-5-8114-6924-6. — Текст : электронный // Лань : электронно-библиотечная

система. — URL: https://e.lanbook.com/book/153678 (дата обращения: 13.07.2021). — Режим доступа: для авториз. пользователей.

33. Прохорова, О. В. Информационная безопасность и защита информации : учебник для вузов / О. В. Прохорова. — 3-е изд., стер. — Санкт-Петербург : Лань, 2021. — 124 с. — ISBN 978- 5-8114-7970-2. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/169817 (дата обращения: 13.07.2021). — Режим доступа: для авториз.пользователей.

34. Райтман М.А. Искусство легального анонимного и безопасного доступа к ресурсам Интернета. /Райтман М.А. Россия, БХВ-Петербург, 2017. ISBN 9785977537452 - 624 стр.

35. Сергеев, А. Н. Основы локальных компьютерных сетей : учебное пособие для спо / А. Н. Сергеев. — Санкт-Петербург : Лань, 2020. — 184 с. — ISBN 978-5-8114-6483-8. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/148024 (дата обращения: 13.07.2021). — Режим доступа: для авториз.пользователей.

36. Советов, Б. Я. Моделирование систем: учебник для академического бакалавриата / Б. Я. Советов, С. А. Яковлев. — 7-е изд. — М. : Издательство Юрайт, 2017. — 343 с. — (Бакалавр. Академический курс). — ISBN 978-5-9916-3898-2.

37. Староверова, Н. А. Операционные системы : учебник для спо / Н. А. Староверова. — Санкт-Петербург : Лань, 2021. — 412 с. — ISBN 978-5-8114-6385-5. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/162376 (дата обращения: 13.07.2021). — Режим доступа: для авториз. пользователей.

38. Тумбинская, М. В. Защита информации на предприятии : учебное пособие / М. В. Тумбинская, М. В. Петровский. — Санкт-Петербург : Лань, 2020. — 184 с. — ISBN 978-5-8114- 4291-1. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/130184 (дата обращения: 13.07.2021). — Режим доступа: для авториз.пользователей.

39. Федосеев В.А. Цифровые водяные знаки и стеганография - 2-е изд., испр. и дополн. — Самара: Самарский университет, 2019. — 144 с. — ISBN 978-5-7883-1370-2

40. Хасанов Р.И. Основы стеганографии - Оренбург: Оренбургский государственный университет, 2017. — 102 с.

41. Ярочкин, В. И. Информационная безопасность : учебник / В. И. Ярочкин. — 5-е изд. — Москва : Академический Проект, 2020. — 544 с. — ISBN 978-5-8291-3031-2. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/132242 (дата обращения: 13.07.2021). — Режим доступа: для авториз.пользователей.

42. Marion Nancy E., Twede Jason. Cybercrime: An Encyclopedia of Digital Crime - ABC-CLIO, LLC., 2020. — 485 p. — 978-1-4408-5735-5

ДОКУМЕНТ ПОДПИСАН
ЭЛЕКТРОННОЙ ПОДПИСЬЮ

СВЕДЕНИЯ О СЕРТИФИКАТЕ ЭП

Сертификат 327766045235508045123579633876966067016845890541

Владелец Дубонос Светлана Михайловна

Действителен С 28.09.2023 по 27.09.2024