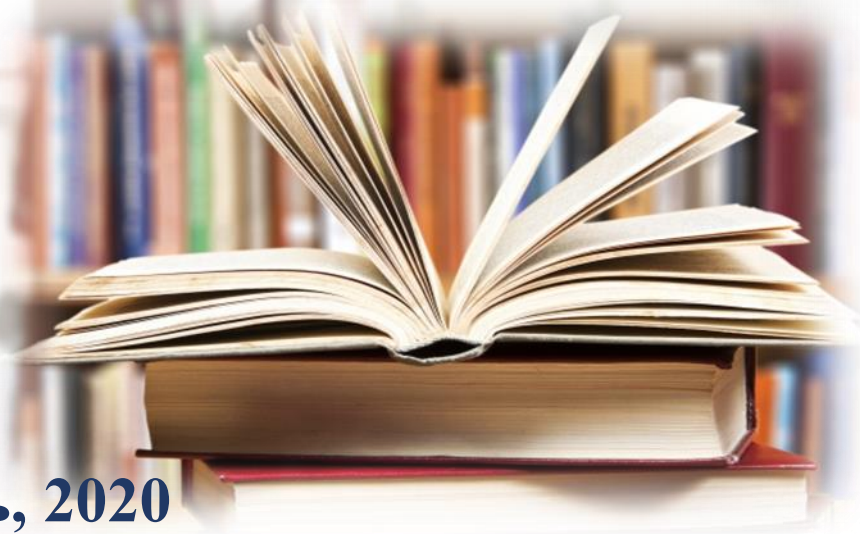




**Сектор информационно-библиотечного обслуживания IT и радиотехнического
профиля. Читальный зал №3**

Выставка электронных изданий «Криптография»

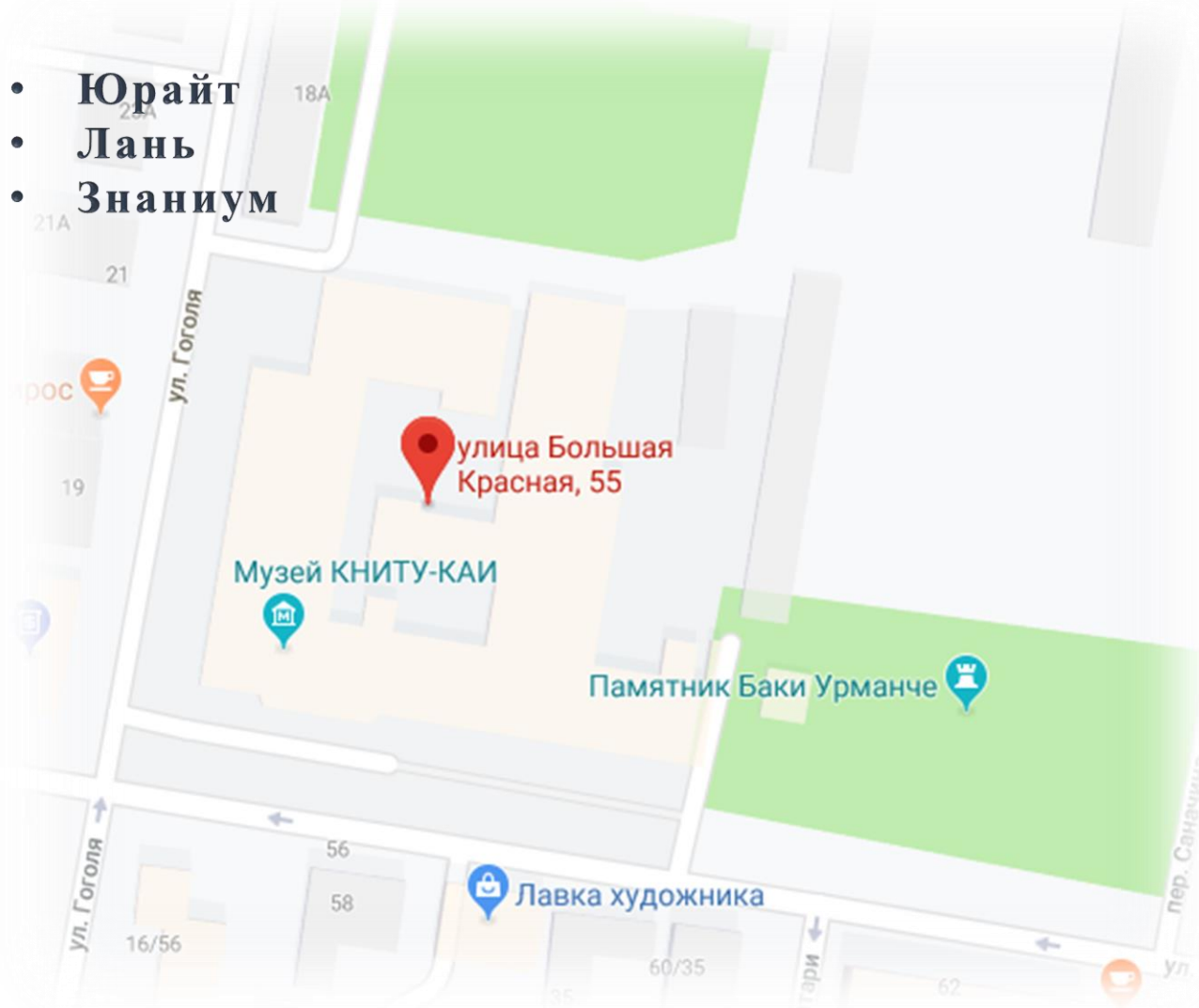


Декабрь, 2020

Уважаемые читатели!

Приглашаем Вас ознакомиться с электронными изданиями, доступными для читателей НТБ им. Н.Г. Четаева КНИТУ-КАИ в ЭБС:

- Юрайт
- Лань
- Знаниум



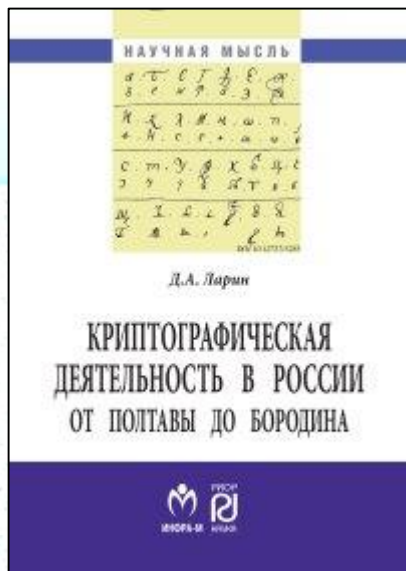


Баранова, Е. К. Информационная безопасность. История специальных методов криптографической деятельности: Учебное пособие / Баранова Е.К., Бабаш А.В., Ларин Д.А. - Москва :ИЦ РИОР, НИЦ ИНФРА-М, 2019. - 236 с.:. - ISBN 978-5-369-01788-3. - Текст : электронный. - URL: <https://znanium.com/catalog/product/987215> (дата обращения: 03.12.2020). – Режим доступа: по подписке.

Аннотация: Учебное пособие посвящено истории тайных операций в криптографической деятельности и взлому криптосистем на протяжении XIX—XX веков. Разбираются вопросы рождения и становления российского криптоанализа, особое внимание уделено виднейшим специалистам в этой сфере и их противостоянию взломщикам шифров. Книга создана на основе множества исторических документов и публикаций авторов по истории криптографии, в ней описан криптографический подход к защите информации и исторические предпосылки в данной области. Представленные в учебном пособии материалы будут полезны бакалаврам и магистрам высших учебных заведений, изучающим курсы «Криптографические методы защиты информации», «Информационная безопасность» и «Управление информационной безопасностью», а также всем интересующимся вопросами истории криптографии и защиты информации.

Доступ по ссылке: <https://znanium.com/catalog/document?pid=987215>





Ларин, Д. А. Криптографическая деятельность в России от Полтавы до Бородина : монография / Д.А. Ларин. — Москва : ИИОП : ИИИИИ-М, 2019. — 282 с. — (Научная мысль). — <https://doi.org/10.12737/5285>. - ISBN 978-5-369-01384-7. - Текст : электронный. - URL: <https://znanium.com/catalog/product/1010795> (дата обращения: 03.12.2020). – Режим доступа: по подписке.

Аннотация: Монография посвящена истории российской криптографии в период от начала правления императора Петра I до окончания Наполеоновских войн. В этот период криптографическая деятельность стала неотъемлемой частью системы государственного управления России. Книга предназначена для специалистов, работающих в области защиты информации, преподавателей, студентов, аспирантов, а также для всех, кто интересуется отечественной историей. Монография может быть использована в учебном процессе по ряду дисциплин, касающихся защиты информации.

Доступ по ссылке: <https://znanium.com/catalog/document?pid=1010795>





Романьков, В. А. Введение в криптографию. Курс лекций / В.А. Романьков. — 2-е изд., испр. и доп. — Москва : ФОРУМ : ИНФРА-М, 2019. — 240 с. — (Высшее образование: Бакалавриат). - ISBN 978-5-00091-493-9. - Текст : электронный. - URL: <https://znanium.com/catalog/product/1018899> (дата обращения: 03.12.2020). – Режим доступа: по подписке.

Аннотация: В курсе лекций изложены математические основы современной криптографии, описан ряд криптографических схем и протоколов, имеющих важное теоретическое значение и широкое практическое применение. Лекции сопровождаются примерами и задачами. Адресован студентам, впервые изучающим криптографию. Может также оказаться полезным специалистам в данной области.

Доступ по ссылке: <https://znanium.com/catalog/document?pid=1018899>





Тропин, М. П. Основы прикладной алгебры : учебное пособие / М. П. Тропин. — 2-е изд., стер. — Санкт-Петербург : Лань, 2020. — 288 с. — ISBN 978-5-8114-5327-6. — Текст : электронный // Лань : электронно-библиотечная система. — URL: <https://e.lanbook.com/book/139282> (дата обращения: 03.12.2020). — Режим доступа: для авториз. пользователей.

Аннотация: В пособие вошли такие разделы, как целые числа, элементы общей алгебры, общая теория многочленов, расширения полей, конечные поля, многочлены над конечными полями, эллиптические кривые. Эти разделы играют важную роль в приложениях. Уровень сложности изложения невысокий, однако предполагается, что читатель имеет математическую подготовку. В конце каждой главы предлагаются задачи для самостоятельного решения. Они направлены на освоение основных понятий и базовых алгоритмов. Учебное пособие предназначено для студентов, обучающихся по направлениям «Математика и механика», «Компьютерные и информационные науки», «Информационная безопасность», «Образование и педагогические науки», другим направлениям и специальностям математического и технического профиля. Учебное пособие может быть использовано как для преподавания прикладной алгебры как самостоятельной дисциплины, так и как основа для различных курсов по алгебре, теории кодирования и криптографии.

Доступ по ссылке: <https://e.lanbook.com/book/139282>





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: 03.12.2020). — Режим доступа: для авториз. пользователей.

Аннотация: Основная цель пособия — подготовить математическую базу для чтения дисциплин, связанных с криптографическими методами защиты информации, в которых находят применение многие разделы алгебры и теории чисел. Особое внимание в пособии уделяется наиболее востребованным в криптографии вопросам делимости и сравнимости целых чисел, а также конечным алгебраическим объектам — конечным группам, кольцам и полям; многочленам и матрицам над конечными кольцами и полями и др. Кроме этого, пособие содержит дополнительные сведения из алгебры и теории чисел, необходимые для развития весьма актуальной в настоящее время криптографии на эллиптических кривых над конечными полями, а также содержит примеры применения алгебры и теории чисел в криптографии. Понятия и многие факты широко иллюстрируются примерами. В конце всех разделов приводятся контрольные вопросы и задания. Пособие предназначено обучающимся по направлениям бакалавриата и специалитета «Информационная безопасность». Оно может быть использовано обучающимися по направлению бакалавриата «Педагогическое образование» (профиль «Математическое образование»), так как охватывает содержание большинства разделов дисциплины «Алгебра и теория чисел».

Доступ по ссылке: <https://e.lanbook.com/book/140740>





Борзунов, С. В. Алгебра и геометрия с примерами на Python : учебное пособие для вузов / С. В. Борзунов, С. Д. Кургалин. — Санкт-Петербург : Лань, 2020. — 444 с. — ISBN 978-5-8114-5489-1. — Текст : электронный // Лань : электронно-библиотечная система. — URL: <https://e.lanbook.com/book/149336> (дата обращения: 03.12.2020). — Режим доступа: для авториз. пользователей.

Аннотация: Учебное пособие является современным введением в линейную алгебру и аналитическую геометрию для студентов естественно-научных факультетов вузов. Базовые алгоритмы алгебры и геометрии представлены на языке программирования Python. Помимо разделов, традиционно включаемых в указанные курсы, дается теоретический материал и методы решения практических задач по теории эллиптических кривых, применяемой в криптографии, а также по основам квантовых вычислений. Содержание книги соответствует ФГОС по направлениям подготовки «Информационные системы и технологии», «Программная инженерия», «Информационная безопасность», «Математика и компьютерные науки». Предназначено для студентов и преподавателей университетов и технических вузов, в которых изучаются курсы алгебры и геометрии, и особенно, для факультетов, где ведется подготовка специалистов в области информационно-коммуникационных технологий.

Доступ по ссылке: <https://e.lanbook.com/book/149336>





Торстейнсон, П. Криптография и безопасность в технологии .NET / П. Торстейнсон, Г. А. Ганеш ; под редакцией С. М. Молякко ; перевод с английского В. Д. Хорева. — 4-е изд. — Москва : Лаборатория знаний, 2020. — 482 с. — ISBN 978-5-00101-700-4. — Текст : электронный // Лань : электронно-библиотечная система. — URL: <https://e.lanbook.com/book/151552> (дата обращения: 03.12.2020). — Режим доступа: для авториз. пользователей.

Аннотация: Подробно излагаются вопросы реализации на .NET-платформе симметричной и асимметричной криптографии, цифровых подписей, XML-криптографии, пользовательской безопасности и защиты кодов, ASP .NET-безопасности, безопасности Web-служб. Изложение построено на разборе примеров конкретных атак на системы безопасности, богато снабжено текстами отлаженных программ. Для программистов, занимающихся разработкой и настройкой систем безопасности на платформе .NET.

Доступ по ссылке: <https://e.lanbook.com/book/151552>





Лось, А. Б. Криптографические методы защиты информации для изучающих компьютерную безопасность : учебник для вузов / А. Б. Лось, А. Ю. Нестеренко, М. И. Рожков. — 2-е изд., испр. — Москва : Издательство Юрайт, 2020. — 473 с. — (Высшее образование). — ISBN 978-5-534-12474-3. — Текст : электронный // ЭБС Юрайт [сайт]. — URL: <https://urait.ru/bcode/450277> (дата обращения: 03.12.2020).

Аннотация: Изложен курс алгоритмической теории чисел и ее приложений к вопросам защиты информации. Основное внимание уделено строгому математическому обоснованию, эффективной реализации и анализу трудоемкости алгоритмов, используемых в криптографических приложениях. Приведено описание современных криптографических схем и протоколов, использующих изложенные теоретические сведения. Курс содержит в себе изложение, построенное по принципу «от простого к сложному», что позволит освоить рассматриваемый материал без существенного использования дополнительной литературы.

Доступ по ссылке: <https://urait.ru/bcode/450277>





Бабенко, Л. К. Криптографическая защита информации: симметричное шифрование : учебное пособие для вузов / Л. К. Бабенко, Е. А. Ищукова. — Москва : Издательство Юрайт, 2020. — 220 с. — (Высшее образование). — ISBN 978-5-9916-9244-1. — Текст : электронный // ЭБС Юрайт [сайт]. — URL: <https://urait.ru/bcode/452871> (дата обращения: 03.12.2020).

Аннотация: Настоящее учебное пособие посвящено изучению основных аспектов современной криптографии, а именно ее большому разделу симметричным блочным шифрам. Большое количество наглядных примеров позволит освоить основные принципы применения криптографических алгоритмов. Вопросы для самоконтроля и задачи для самостоятельного решения будут способствовать закреплению изученного материала. Изученный материал позволит самостоятельно применять полученные знания на практике в области криптографии и в области криптоанализа.

Доступ по ссылке: <https://urait.ru/bcode/452871>





Фомичёв, В. М. Криптографические методы защиты информации в 2 ч. Часть 1. Математические аспекты : учебник для вузов / В. М. Фомичёв, Д. А. Мельников ; под редакцией В. М. Фомичёва. — Москва : Издательство Юрайт, 2020. — 209 с. — (Высшее образование). — ISBN 978-5-9916-7088-3. — Текст : электронный // ЭБС Юрайт [сайт]. — URL: <https://urait.ru/bcode/450820> (дата обращения: 03.12.2020).

Аннотация: Предлагаемый учебник является научным вкладом в противодействие современным угрозам информационной безопасности (ИБ) России. Авторы с большим опытом практической и преподавательской работы систематически изложили математические основы криптологии и основные криптографические методы защиты информации, показали их связь с задачами ИБ. Уникальность издания заключается в сочетании материала, связанного с защитой различных видов информации: текста, речи, изображений (факсимиле). Книга предназначена, в первую очередь, студентам и преподавателям по направлениям «Информационная безопасность», «Прикладная информатика» и «Информатика и вычислительная техника», а также других технических специальностей.

Доступ по ссылке: <https://urait.ru/bcode/450820>





Фомичёв, В. М. Криптографические методы защиты информации в 2 ч. Часть 2. Системные и прикладные аспекты : учебник для вузов / В. М. Фомичёв, Д. А. Мельников ; под редакцией В. М. Фомичёва. — Москва : Издательство Юрайт, 2020. — 245 с. — (Высшее образование). — ISBN 978-5-9916-7090-6. — Текст : электронный // ЭБС Юрайт [сайт]. — URL: <https://urait.ru/bcode/451486> (дата обращения: 03.12.2020).

Аннотация: Предлагаемый учебник является научным вкладом в противодействие современным угрозам информационной безопасности (ИБ) России. Авторы с большим опытом практической и преподавательской работы систематически изложили математические основы криптологии и основные криптографические методы защиты информации, показали их связь с задачами ИБ. Уникальность учебника заключается в сочетании материала, связанного с защитой различных видов информации: текста, речи, изображений (факсимиле). Издание предназначено, в первую очередь, студентам и преподавателям по направлениям «Информационная безопасность», «Прикладная информатика» и «Информатика и вычислительная техника», а также других технических специальностей.

Доступ по ссылке: <https://urait.ru/bcode/451486>





Васильева, И. Н. Криптографические методы защиты информации : учебник и практикум для вузов / И. Н. Васильева. — Москва : Издательство Юрайт, 2020. — 349 с. — (Высшее образование). — ISBN 978-5-534-02883-6. — Текст : электронный // ЭБС Юрайт [сайт]. — URL: <https://urait.ru/bcode/450998> (дата обращения: 03.12.2020).

Аннотация: Данный курс знакомит с основными принципами, подходами и методами современной криптографии. Наряду с историческими шифрами рассмотрены используемые в настоящее время криптосистемы с секретными и открытыми ключами, криптографические хэш-функции, методы электронной подписи, криптосистемы на эллиптических кривых. Освещены вопросы применения криптографических методов и средств защиты информации для обеспечения конфиденциальности, подтверждения целостности, аутентификации и решения других практических задач в современных информационных системах.

Доступ по ссылке: <https://urait.ru/bcode/450998>



СПАСИБО ЗА ВНИМАНИЕ!

Составители:



Назиева Лилия Нурулловна

Главный библиограф сектора информационно-библиотечного обслуживания IT профиля



Нечунаева Инесса Альбертовна

Заведующая сектором информационно-библиотечного обслуживания IT профиля

Адрес: ул. Большая Красная, д. 55, 7-е зд., КНИТУ-КАИ,
внутр. тел.: 75-13, ауд.423

