Захист інформації.

Безпека

Інформація грає важливу роль в забезпеченні всіх сторін життєдіяльності суспільства і особливо важлива інформація завжди підлягала захисту від розголошення. Розвиток нових інформаційних технологій супроводжується такими негативними явищами, як промислове шпигунство, комп'ютерні злочини і несанкціонований доступ до конфіденційної інформації. Виникли нові поняття «кібертероризм», «інформаційна війна» і т. п. Тому захист інформації є найважливішим державним завданням у будь-якій державі. Захист інформації повиннен забезпечувати запобігання шкоди в результаті втрати (розкрадання, спотворення, підробки) інформації в будь-якому її вигляді.

Довгий, С.О., Сучасні телекомунікації: Мережі, технології, безпека, економіка, регулювання [Текст]: Монографія / С.О. Довгий, П.П. Воробієнко, К.Д. Гуляєв; За загальною ред. С.О. Довгого. – 2-е видання (доповнене). – К.: Азимут-Україна, 2013. – 608 с.

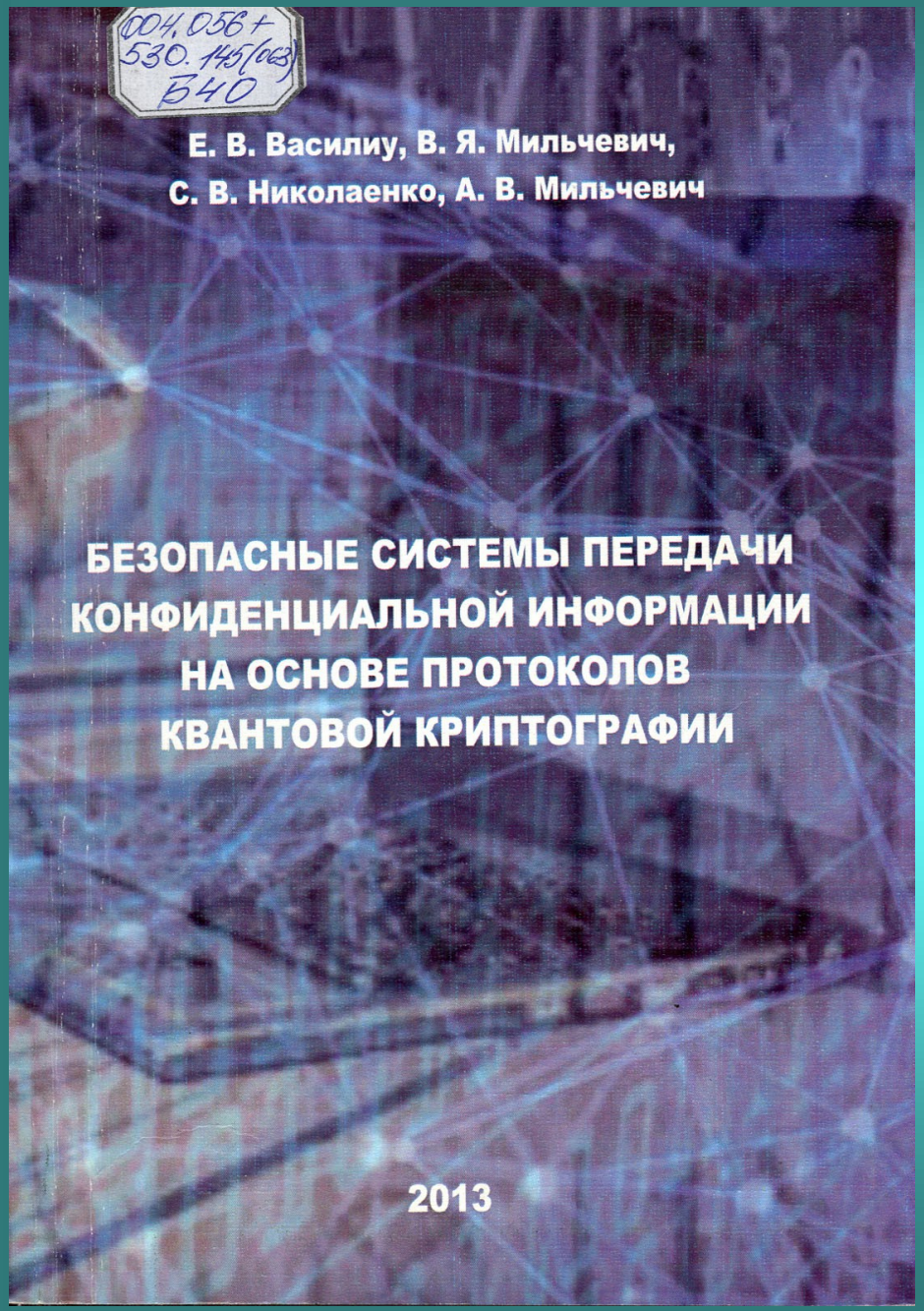
У монографії комплексно розкрито питання розвитку телекомунікаційних мереж наступних поколінь, що містить технологічні, організаційні та регуляторні аспекти створення та впровадження новітніх технологій.

В книзі представлено комплексний огляд сучасного стану загальної теорії телекомунікацій, технологій захисту інформації та фільтрації контенту, технологій мінімізації обсягів службового навантаження тощо та наведено науково-методичні основи низки принципово нових високоефективних телекомунікаційних технологій побудови конвергентних мультимедійних мереж наступних поколінь.

Защита информации в телекоммуникационных системах: учебное пособие для вузов / Г.Ф. Конахович, В.П. Климчук, С.М. Паук, В.Г. Потапов; гл. ред. Ю.А. Шпак. – К.: "МК-Пресс", 2005. – 288 с.

В книге рассмотрены основные проблемы защиты информации, возникающие в ведомственных системах связи и передачи данных, радиотехнических системах и системах связи общего пользования. Проведен достаточно полный анализ каналов утечки информации, методов и способов несанкционированного получения информации, средств защиты информации. Проанализированы особенности функционирования ведомственных телекоммуникационных систем. Отдельные главы посвящены криптографии и шифрованию, а также методам закрытия речевых сигналов.

Книга будет полезна специалистам в области телекоммуникации и защиты информации, а также студентам соответствующих специальностей.



Безопасные системы передачи конфиденциальной информации на основе протоколов квантовой криптографии [Текст]: монография / Е.В. Василиу, В.Я. Мильчевич, С.В. Николаенко, А.В. Мильчевич. – Харьков: Цифровая типография; Краснодар, 2013. – 168 с.

В монографии представлены результаты исследований в области одного из новых направлений квантовой криптографии – квантовых протоколов прямой безопасной связи, которые позволяют передавать конфиденциальную информацию по открытым квантовым каналам связи напрямую, то есть без ее шифрования либо сокрытия.

Англо-русский словарь по телекоммуникациям и информационной безопасности [Текст] = English-Russian Dictionary of Telecommunications and Data Security / П.П. Воробиенко, Г.П. Кузнецова, В.П. Веретенникова, И.И. Стоянова. – Одесса: ОНАС им. А.С. Попова, 2012. – 212 с.

Англо-русский словарь по телекоммуникациям и информационной безопасности содержит более 6000 терминов и охватывает темы:

- виды электросвязи;

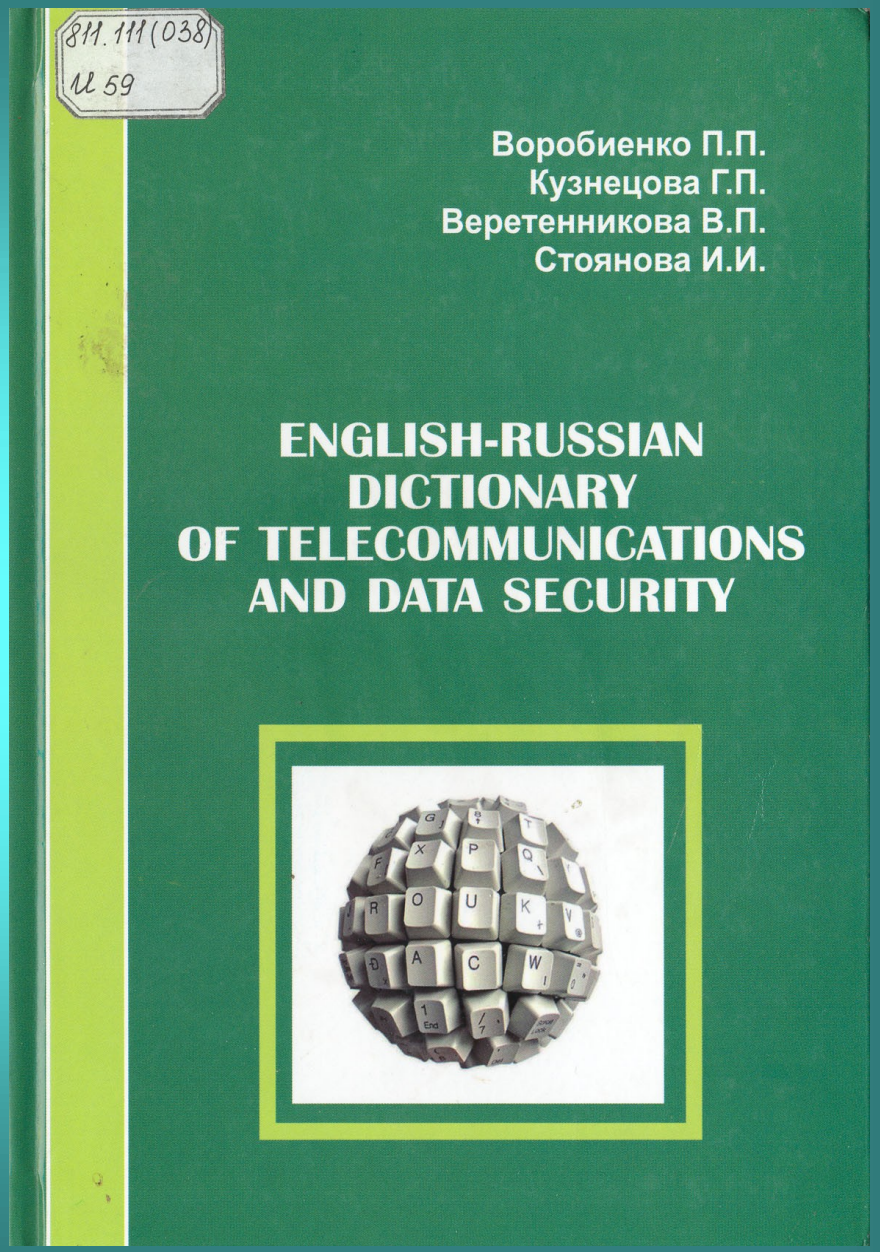
- информационная безопасность;

- предоставление телекоммуникационных услуг;

- современные технологии.

Словарь состоит из двух частей: англо-русского словаря и словаря английских сокращений.

Для специалистов в области телекоммуникаций и информационной безопасности, переводчиков, преподавателей и студентов.



Поповский, В.В., Защита информации в телекоммуникационных системах: учебник / В.В. Поповский, А.В. Персиков. – Х.: ООО "Компания СМИТ", 2006.

Т. 1. – 238 с.

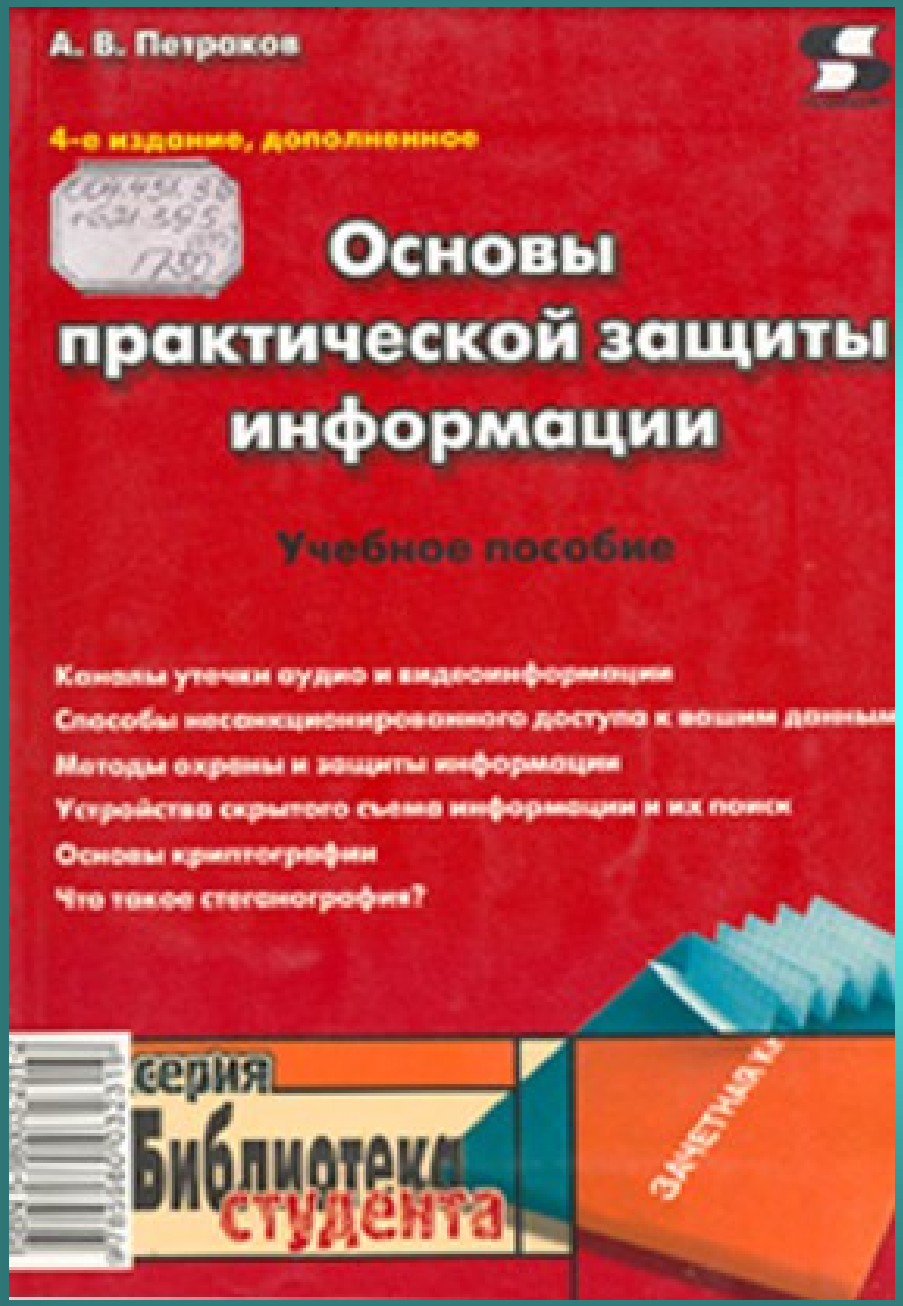
В данном учебнике изложен курс информационной безопасности для специалистов в области «Телекоммуникации», в том числе вопросы защиты интеллектуальной собственности, криптографической защиты информации, защищенных протоколов обмена данными в сетях общего использования, защиты мобильных, а также операционных систем и сетей. Подробно рассмотрены стенографические методы защиты информации и перспективные разработки в сфере защиты информации.

Поповский, В.В., Защита информации в телекоммуникационных системах: учебник / В.В. Поповский, А.В. Персиков. – Х.: ООО "Компания СМИТ", 2006.

Т. 2. – 292 с.

Во втором томе подробно рассмотрены основные процедуры работы с защищенными системами, основы построения операционных систем, в том числе Windows, Linux, приведены общие сведения о брандмауэрах, подняты вопросы технической защиты информации, изложены методы и средства защиты информации, понятия и суть криптографии и стеганографии, а также перспективные разработки в сфере защиты информации.

Для студентов, магистров и аспирантов, а также научных сотрудников, работающих в области «Телекоммуникации».



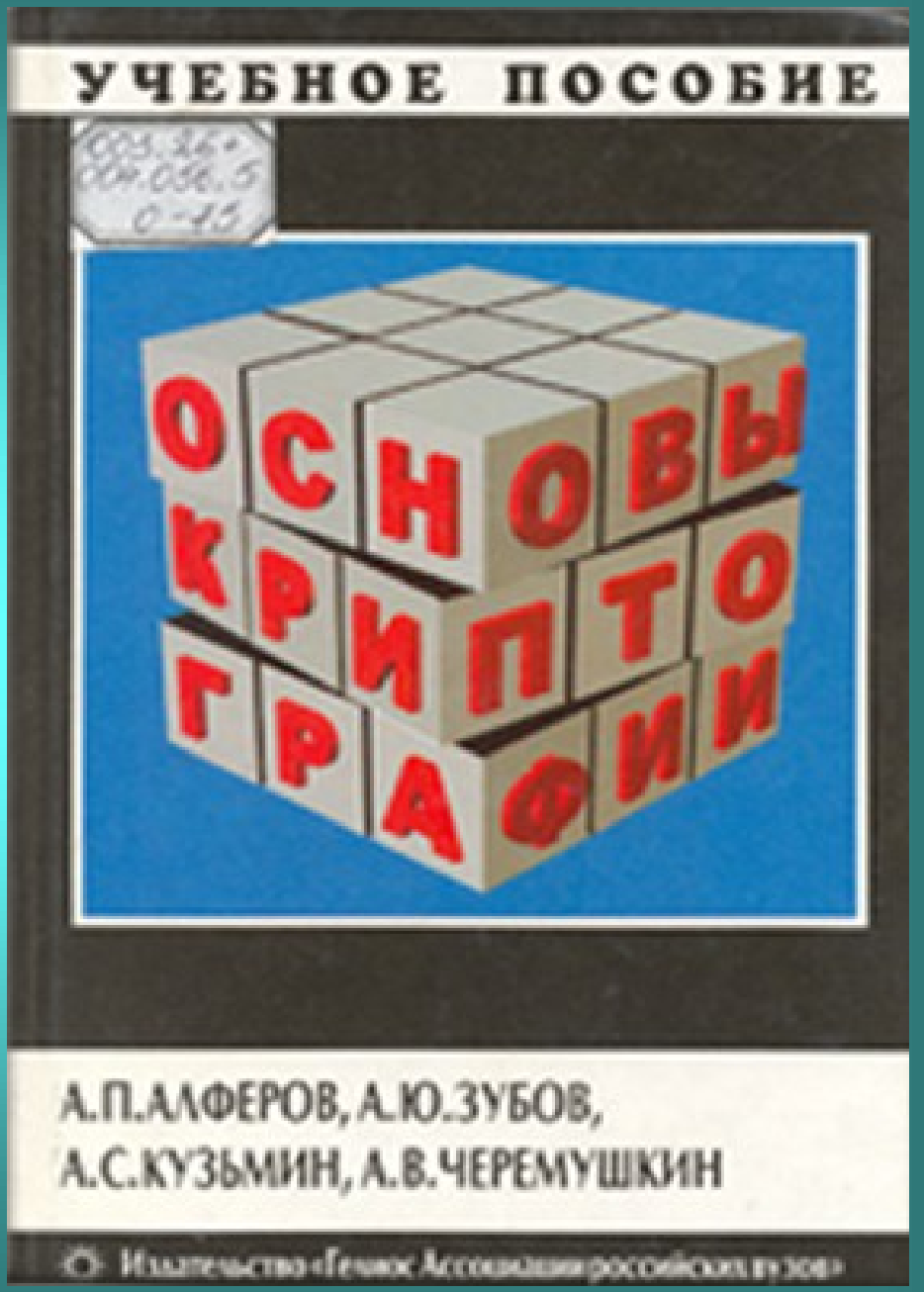
Петраков, А.В., Основы практической защиты информации: учебное пособие. – 4-е изд., доп. – М.: СОЛОН-Пресс, 2005. – 388 с.: илл.

В последние годы в учебные планы всех вузов и факультетов связи вошла новая дисциплина «Основы защиты информации». Настоящее учебное издание предназначено в помощь изучающим эту дисциплину как в университетах, колледжах и институтах повышения квалификации на специальностях 2009, 2010, 2011, 2012, 2102 (связи), так и на смежных специальностях при изучении дисциплин «Защита информации» или «Техническая защита информации».

Основы криптографии [Текст]: учебное пособие / А.П. Алферов, А.Ю. Зубов, А.С. Кузьмин, А.В. Черемушкин. – 2-е изд., испр.и доп. – М.: Гелиос АРВ, 2002. – 480 с.: ил.

Написано ведущими специалистами в области криптографии, имеющими многолетний опыт разработки криптографических средств защиты и преподавания дисциплин криптографического цикла в ведущих вузах страны.

Излагаются основные понятия и разделы, позволяющие получить представление о задачах и проблемах современной криптографии. В пособие вошли как традиционные вопросы классификации и оценки надежности шифров, так и системные вопросы использования криптографических методов защиты информации.

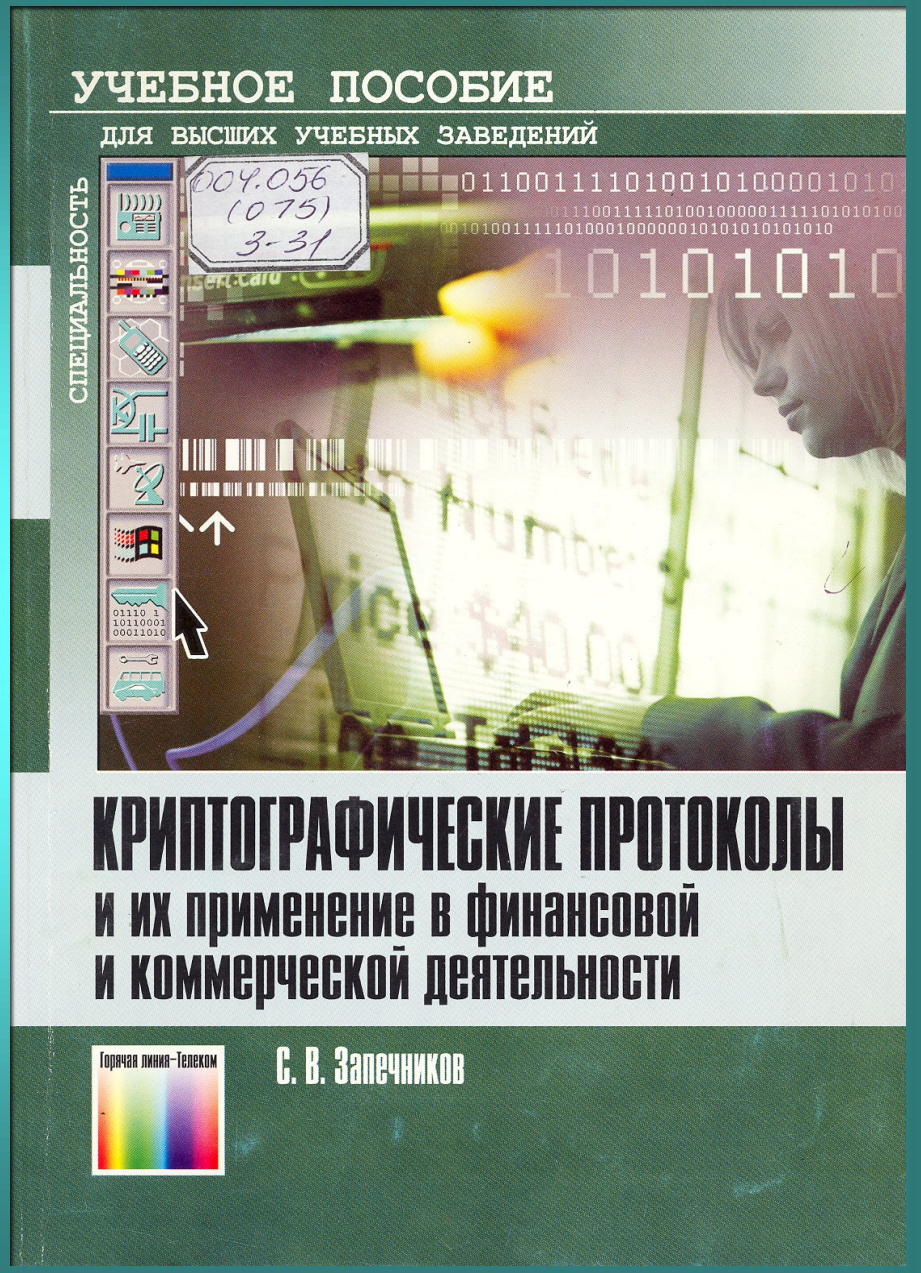


Технические средства и методы защиты информации [Текст]: учебное пособие для вузов / А.П. Зайцев, А.А. Шелупанов, Р.В. Мещеряков [и др.]; под ред. А.П. Зайцева и А.А. Шелупанова. – 4-е изд., испр. и доп. - М.: Горячая Линия-Телеком, 2009. – 616 с. : ил.

Рассмотрены технические средства и методы защиты информации от несанкционированного доступа. Описаны возможные технические каналы утечки информации. Основное внимание уделено рассмотрению принципов работы технических средств защиты информации. Отличительной особенностью книги является наличие лабораторных и практических занятий, которые позволяют студентам приобрести практические навыки работы с техническими средствами защиты информации.

Запечников, С.В., Криптографические протоколы и их применение в финансовой и коммерческой деятельности: учебное пособие для вузов. – М.: Горячая Линия-Телеком, 2007. – 320 с.

В систематизированном виде изложены основы теории криптографических протоколов и практики их применения в финансовой и коммерческой деятельности. Наряду с рассмотрением современных методов синтеза и анализа основных классов криптографических протоколов, основное внимание уделяется специальным их применением: защищенным каналам передачи информации, системам электронных платежей, защищенному электронному документообороту. Рассматриваются проблемы криптографической защиты многосторонних транзакций и коммерческих сделок, криптографических методов обеспечения государственно-правовых отношений, осуществляемых с использованием технических средств компьютерных систем.



Баричев, С.Г., Основы современной криптографии / С.Г. Баричев, В.В. Гончаров, Р.Е. Серов. – 2-е изд., перераб. и доп. – М.: Горячая Линия-Телеком, 2002. – 175 с.

В систематизированном виде рассмотрены вопросы создания симметричных и асимметричных криптографических систем защиты информации. Описаны алгоритмы электронных цифровых подписей, системы управления криптографическими ключами, имитозащита информации.

Для специалистов в области защиты информации, может быть полезна студентам вузов.

Основы информационной безопасности: учебное пособие / Е.Б. Белов, В.П. Лось, Р.В. Мещеряков, А.А. Шелупанов. – М.: Горячая Линия-Телеком, 2006. – 544 с.

Изложены вопросы теории и практики обеспечения информационной безопасности личности, общества и государства. Большое внимание уделено проблеме безопасности автоматизированных систем, включая вопросы определения модели нарушителя и требований к защите информации. Анализируются современные способы и средства защиты информации и архитектура систем защиты информации. В приложениях приведен справочный материал по ряду нормативных правовых документов и вариант рабочей программы по дисциплине «Основы информационной безопасности».

Для студентов высших учебных заведений, обучающихся по специальностям в области информационной безопасности, может быть полезной для широкого круга читателей, интересующихся вопросами обеспечения информационной безопасности.

Технологічні, організаційні та регуляторні засади побудови телекомунікаційних мереж сучасних та наступних поколінь [Текст]: монографія; Каф. комутаційних систем. – К.: Кафедра, 2014. – 288 с.

Комплексно розкрито питання розвитку телекомунікаційних мереж наступних поколінь, які включають технологічні, організаційні та регуляторні аспекти створення та впровадження новітніх технологій.

У виданні представлено принципово нові методи проектування телекомунікаційних мереж, що базуються на нових математичних моделях систем розподілу інформації та трафіку телекомунікаційних мереж, а також унікальні методики, які були успішно апробовані під час проектування багатьох телекомунікаційних мереж національного масштабу.

Джоханссон, Джеспер, Обеспечение безопасности. Ресурсы Windows Server 2008 [Текст]: руководство / пер. с англ. – М.: Русская редакция; СПб.: БХВ-Петербург, 2009. – 544 с.

Данное официальное руководство Microsoft содержит полное, углубленное описание планирования, развертывания и управления средствами обеспечения безопасности Windows Server 2008. В книге детально описаны новые инструменты безопасности Windows, объекты безопасности, сервисы безопасности, аутентификация пользователя и контроль доступа, стратегия сетевой безопасности и управление безопасной работой приложений, брандмауэр Windows, безопасность Active Directory, групповые политики, проведение аудита и управление обновлениями. На прилагаемом компакт-диске находятся полезные инструменты, готовые сценарии, шаблоны и другие полезные ресурсы.

Новые технологии электронного бизнеса и безопасности [Текст] / В.А. Быков, Л.К. Бабенко, О.Б. Макаревич та ін. - М.: Радио и связь, 2002. – 512 с.

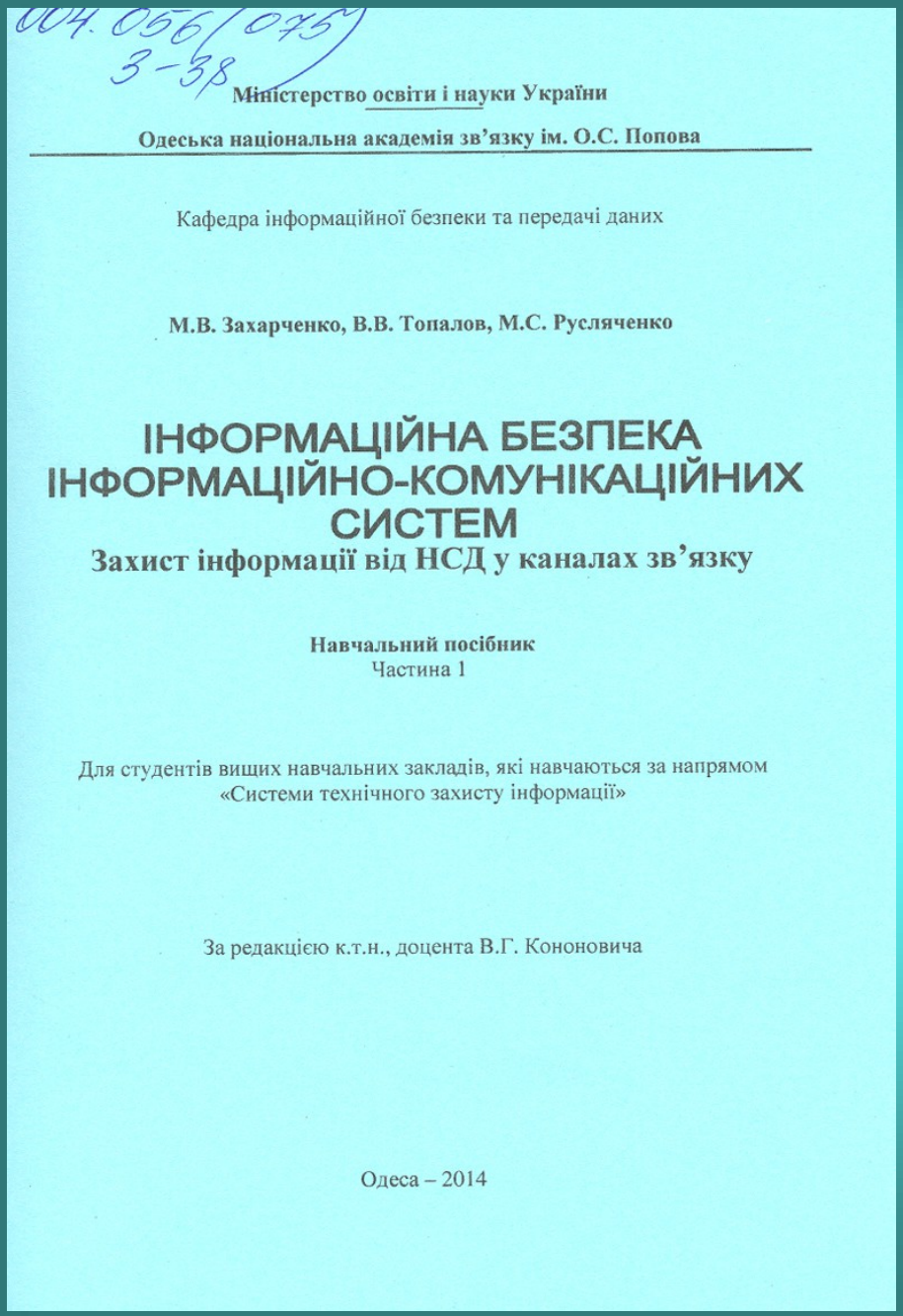
Электронный бизнес с использованием Internet – технологий сегодня является наиболее развивающейся и наиболее прибыльной сферой деятельности.

Книга рассчитана на широкий круг читателей, руководителей предприятий, предпринимателей и бизнесменов, интересующихся электронной коммерцией и безопасностью своей производственно-хозяйственной деятельности. Интерес к ней может быть проявлен студентами экономических и других Вузов, где читаются курсы по электронной коммерции и защите информации.

Асиметричні методи шифрування в телекомун. Мод. 2. – криптогр. методи захисту інформ. в телеком. системах та мережах [Текст]: навч. посібник / М.В. Захарченко, О.В. Онацький, Л.Г. Йона, Т.М. Шинкарук; каф. інформаційної безпеки та передачі даних. – Одеса: ОНАЗ ім. О.С. Попова, 2011. – 181 с.

Розглянуто математичні основи теорії чисел та основні вимоги до геш-функцій, забезпечуючих мінімізацію мережного трафіку та надлишковість відкритого тексту при криптографічному перетворенні, проведено аналіз сучасних способів організації секретного зв'язку без попереднього обміну ключами алгоритму електронно-цифрового підпису.

Теоретичний матеріал відповідає навчальним програмам «Захист інформації в телекомунікаційних системах та мережах», «Криптографія та стенографія» і супроводжується достатньою кількістю наведених типових прикладів, контрольних запитань та задач, забезпечуючих самоперевірку засвоєння матеріалу.



Захарченко, М.В., Інформаційна безпека інфомаційно-комунікаційних систем. Захист інформації від НСД у каналах зв'язку [Текст] Ч. 1: навчальний посібник / М.В. Захарченко, В.В. Топалов, М.С. Русляченко; за ред. В.Г. Кононовича; каф. інформаційної безпеки та передавання даних. – Одеса: ОНАЗ ім. О.С. Попова, 2014. – 228 с.

Представлені тематичні цикли лабораторного практикуму в галузі знань «Інформаційна безпека». Цикли лабораторного практикуму складені з навчально-методичних рекомендацій та посібників для виконання лабораторних робіт з напрямів підготовки «Системи технічного захисту інформації» та «Безпека інформаційно-комунікаційних систем», об'єднані завданням створення комплексних систем технічного захисту інформації в організаціях, підприємствах, установах та органах державної влади.

Голев, Д.В., Методики оцінки інформаційної захищеності телекомунікацій [Текст]: навч. посібник / Д.В. Голев, В.Г. Кононович, С.В. Хомич; за ред. чл.-кор. МАЗ В.Г. Кононовича; каф. інформаційної безпеки та передавання даних. – Одеса: ОНАЗ ім. О.С. Попова, 2013. – 218 с.

У навчальному посібнику розглянуто основні положення, теоретичні основи та практичні аспекти методик оцінки інформаційної захищеності. Пояснюються моделі та принципи оцінки ефективності технічного захисту інформації. Описані теорія та методи інструментальної оцінки у дослідженні систем безпеки інформаційних технологій. Розглядаються основні цілі, задачі та порядок проведення атестації комплексів технічного захисту інформації в інфокомунікаціях.

Розглядаються методичні основи оцінки ефективності захисту інформаційних ресурсів.

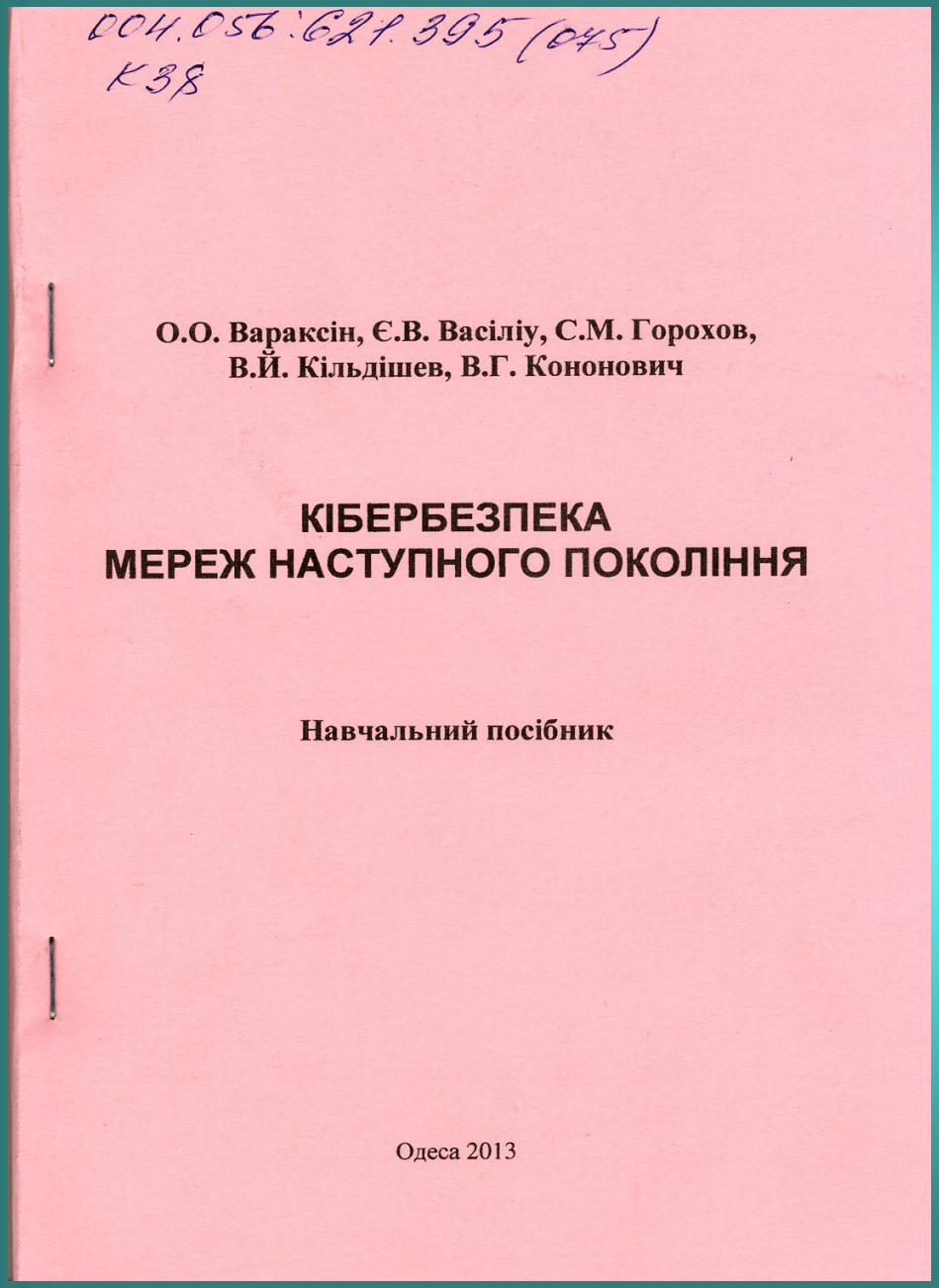
Голев Д.В., Кононович В.Г., Хомич С.В.

МЕТОДИКИ ОЦІНКИ ІНФОРМАЦІЙНОЇ ЗАХИЩЕНОСТІ ТЕЛЕКОМУНІКАЦІЙ

Навчальний посібник
галузі знань 1601, 1701 «Інформаційна безпека»
за спеціальністю 7.17010201, 8.17010201 – Системи технічного захисту інформації, автоматизації її обробки

За ред. чл.-кор. МАЗ В.Г. Кононовича

Одеса 2013

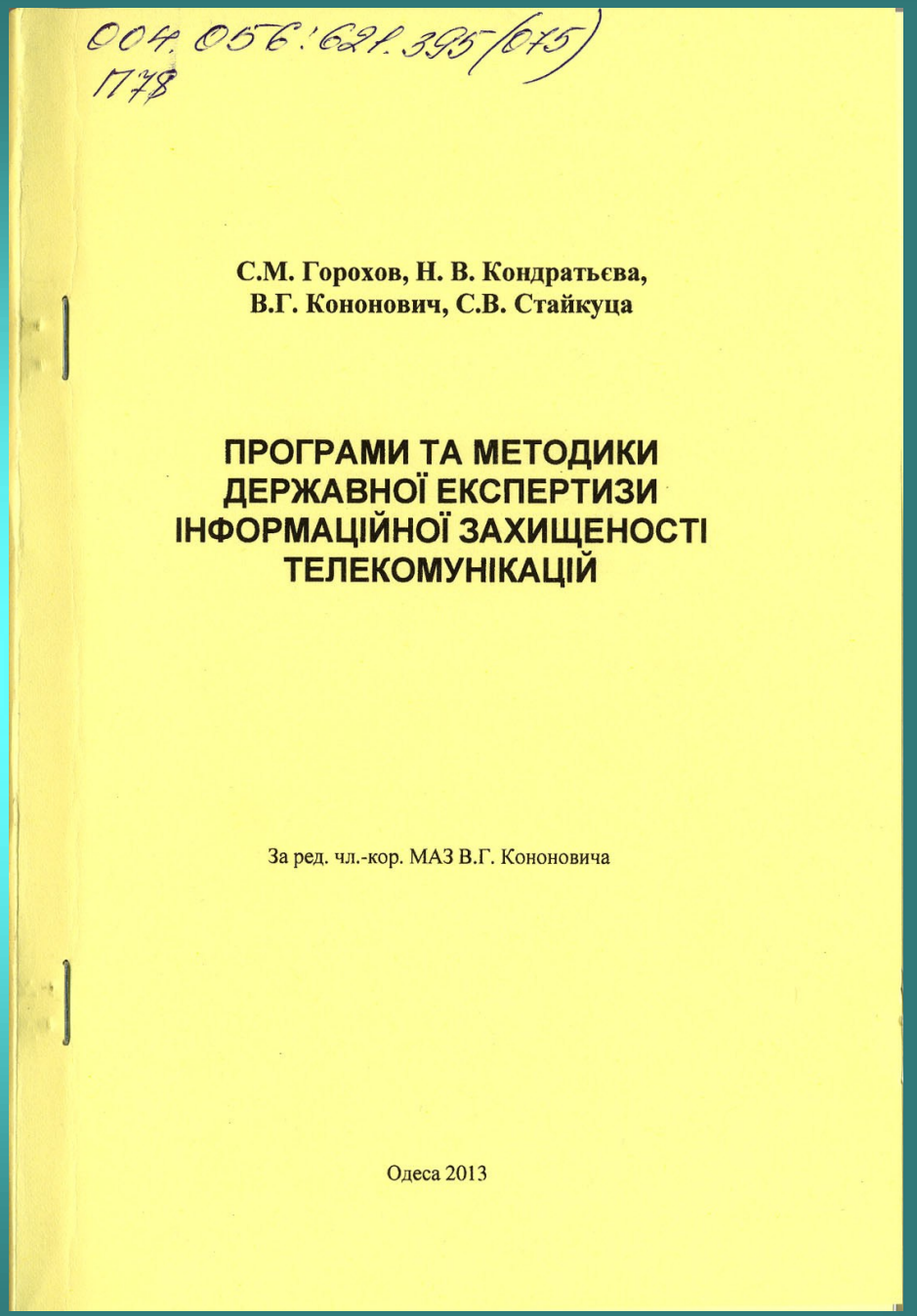


Кібербезпека мереж наступного покоління [Текст]: навчальний посібник / О.О. Вараксін, Є.В. Василіу, С.М. Горохов та ін.; каф. інформаційної безпеки та передавання даних. – Одеса: ОНАЗ ім. О.С. Попова, 2013. – 240 с.

У навчальному посібнику розглянуто основні положення, поняття й визначення, теоретичні засади та практичні аспекти кібербезпеки мереж наступних поколінь. Описано можливості протоколу SIP і технічні вимоги до систем захисту інформації. Розглядаються основні цілі, задачі та функції організаційного, правового, технічного, методичного та програмно-апаратного забезпечення кібербезпеки, джерела загроз і засоби їх впливу на об'єкти кібербезпеки, особливості побудови інфокомунікацій та архітектури системи кібербезпеки інфокомунікацій відповідно до вимог безпеки інформаційних ресурсів і кіберсередовища.

Програми та методики державної експертизи інформаційної захищеності телекомунікацій [Текст]: навчальний посібник / С.М. Горохов, Н.В. Кондратьєва, В.Г. Кононович, С.В. Стайкуца; каф. інформаційної безпеки та передавання данних; за ред. чл.-кор. МАЗ В.Г. Кононовича. – Одеса: ОНАЗ ім. О.С. Попова, 2013. – 252 с.

У навчальному посібнику розглянуто основні положення, теоретичні засади та практичні аспекти методик оцінки інформаційної захищеності. Пояснюються моделі та принципи оцінки ефективності захисту від несанкціонованого доступу. Розглядаються методи оцінки забезпечення гарантій безпеки. Описані теорія та методи експертних оцінок у дослідженні систем безпеки інформаційних технологій. Розглядаються основні цілі, задачі та порядок проведення державної експертизи комплексних систем технічного захисту інформації в інфокомунікаціях.



С. М. Горохов, В. Г. Кононович, С.В. Стайкуца,
Т. М. Лемеха, Ю.В. Копитін

ІНФОРМАЦІЙНА БЕЗПЕКА ЦИФРОВИХ ПРОГРАМНО-КЕРОВАНИХ АТС

Навчальний посібник

Для студентів вищих навчальних закладів, які навчаються за напрямом «Системи захисту інформаційних та інформаційно-комунікаційних систем»

За ред. члена-кореспондента МАЗ, кандидата технічних наук, доцента В.Г. Кононовича

Одеса 2013

Інформаційна безпека цифрових програмно-керованих АТС [Текст]: навчальний посібник / С.М. Горохов, В.Г. Кононович, С.В. Стайкуца та ін.; за ред. чл.-кор. МАЗ В.Г. Кононовича; каф. інформаційної безпеки та передавання данних. – Одеса: ОНАЗ ім. О.С. Попова, 2013. – 244 с.

Представлені основні положення, поняття й визначення з проектування систем технічного захисту інформації програмно-керованих автоматичних телефонних станцій, зокрема, органів державної влади, організаційного, правового, технічного, методичного та програмно-апаратного забезпечення на етапах створення, введення в дію та технічної експлуатації комплексних систем технічного захисту інформації. Викладаються методи техніко-економічного обґрунтування ефективності інформаційної безпеки.

Онацкий, А.В., Ассиметричные методы шифрования. Мод. 2. Криптографические методы защиты информации в телекоммуникационных системах и сетях [Текст]: учебное пособие / А.В. Онацкий, Л.Г. Йона; под ред. Н.В. Захарченко; каф. информ. безоп. и передачи данных. – Одесса: ОНАС им. А.С. Попова, 2010. – 147 с.

Изложены основные подходы и методы современной криптографии для решения задач, возникающих при обработке, хранении и передаче информации в системах телекоммуникаций.

Рассмотрены методы шифрования с открытыми ключами, цифровой подписи, основные криптографические протоколы и хэш-функции, криптосистемы на эллиптических кривых. Изложение теоретического материала ведется с использованием математического аппарата из теории чисел. Подробно описаны алгоритмы, лежащие в основе международных стандартов. Приведены упражнения, необходимые при проведении практических занятий.

Министерство транспорта и связи Украины
Государственная администрация связи
Одесская национальная академия связи им. А. С. Попова

А. В. Онацкий, Л. Г. Йона

**Защита информации
в телекоммуникационных системах и сетях**

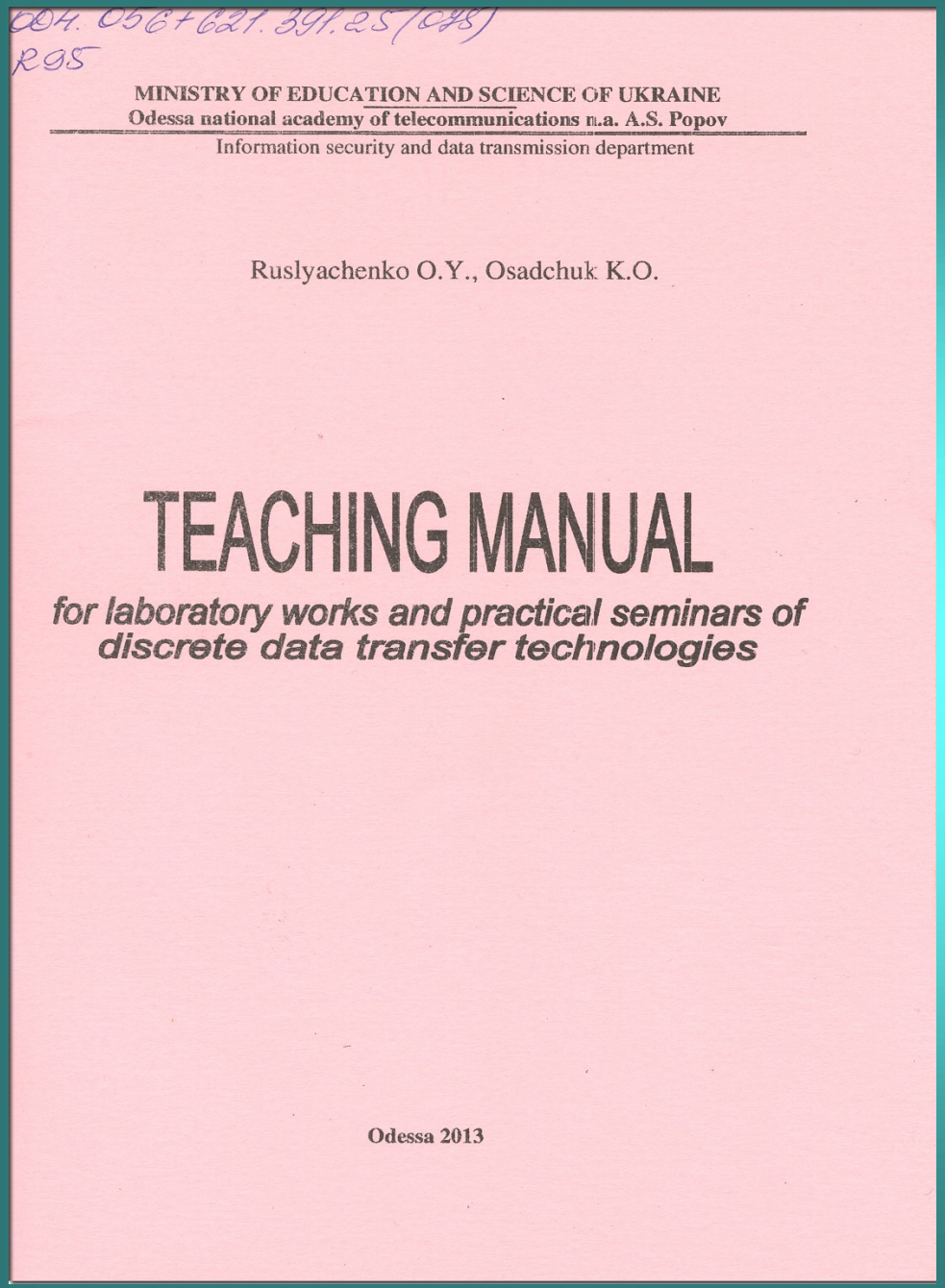
*Модуль 2 Криптографические методы защиты информации
в телекоммуникационных системах и сетях*

АСИММЕТРИЧНЫЕ МЕТОДЫ ШИФРОВАНИЯ

Учебное пособие
по направлениям подготовки студентов
6.050903 Телекоммуникаций
6.170102 Системы технической защиты информации
6.050901 Радиотехника

Под редакцией проф. Н. В. Захарченко

Одесса – 2010



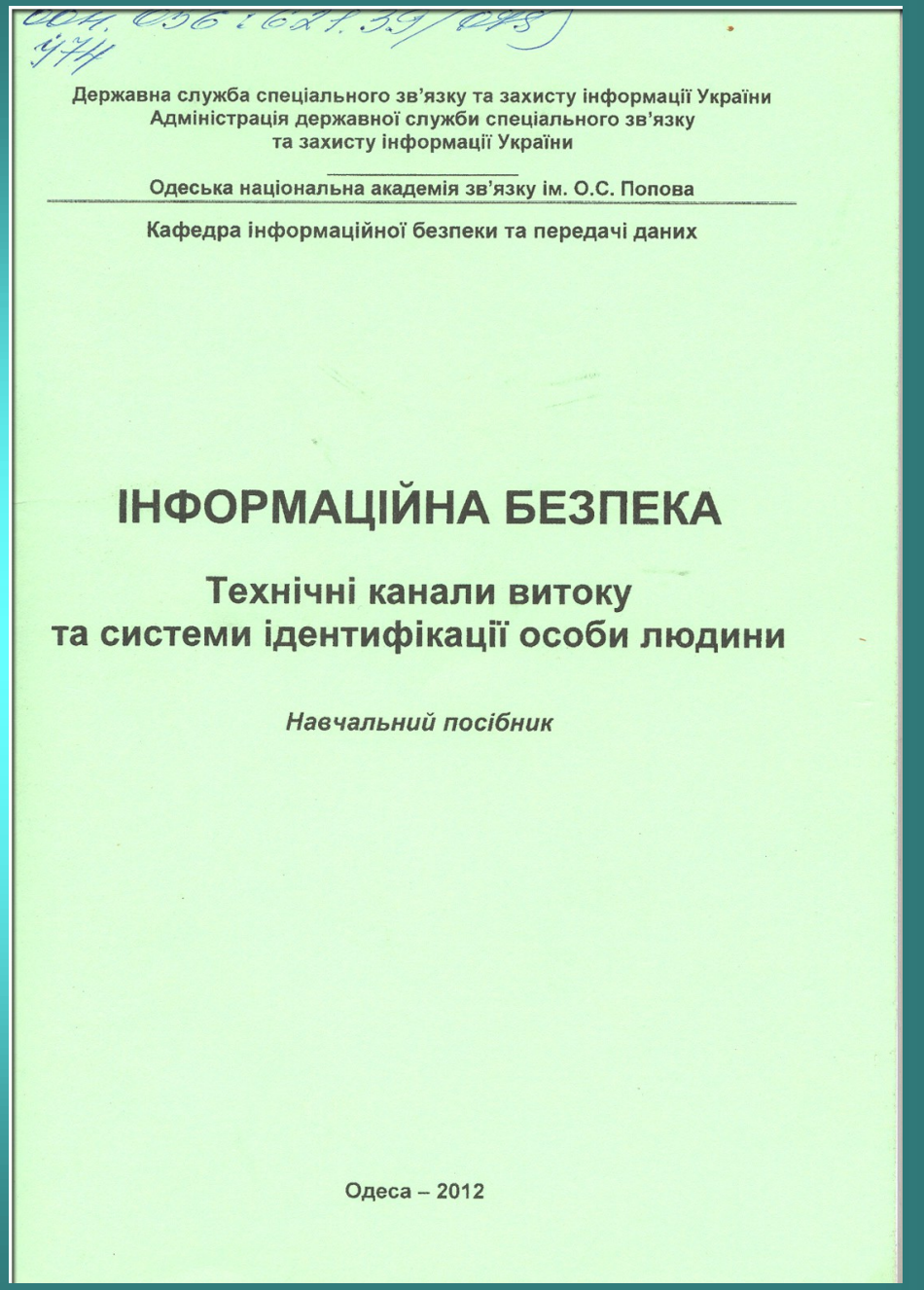
Ruslyachenko, O.Y.

Discrete data transfer technologies [Text] Module 3: Teaching manual for laboratory works and practical seminars / O.Y. Ruslyachenko, K.O. Osadchuk; Information security and data transmission department. - Odessa: ONAT by the name of A.S. Popov, 2013. – 60 c .

Навчальний посібник містить конспект лекцій та методичні вказівки до проведення лабораторних та практичних занять для модуля 3 з дисципліни Технології передачі дискретних повідомлень англійською мовою.

Інформаційна безпека. Технічні канали витоку та системи ідентифікації особи людини [Текст]: навчальний посібник / М.В. Захарченко, Д.В. Голев, О.Ю. Русляченко [та ін.]; за ред. В.Г. Кононовича; Каф. інформ. безпеки та передачі даних. – Одеса: ОНАЗ ім. О.С. Попова, 2012. – 188 с.

Представлені тематичні цикли лабораторного практикуму в галузі знань «Інформаційна безпека». Цикли лабораторного практикуму складені з навчально-методичних рекомендацій та посібників для виконання лабораторних робіт з напрямів підготовки «Системи технічного захисту інформації» та «Безпека інформаційно-комунікаційних систем», об'єднані завданням створення комплексних систем технічного захисту інформації в організаціях, підприємствах, установах та органах державної влади.



Державна служба спеціального зв'язку та захисту інформації України
Адміністрація державної служби спеціального зв'язку
та захисту інформації України

Одеська національна академія зв'язку ім. О.С. Попова

Кафедра інформаційної безпеки та передачі даних

ІНФОРМАЦІЙНА БЕЗПЕКА

Технічні канали витоку та системи ідентифікації особи людини

Навчальний посібник

Одеса – 2012

Міністерство освіти і науки України
Міністерство транспорту та зв'язку України
Одеська національна академія зв'язку ім. О.С. Попова

Тардаскіна Т.М., Кононович В.Г.

МЕНЕДЖМЕНТ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ В ГАЛУЗІ ЗВ'ЯЗКУ

Рекомендовано Міністерством освіти і науки України як навчальний посібник для студентів вищих навчальних закладів

Одеса
2011

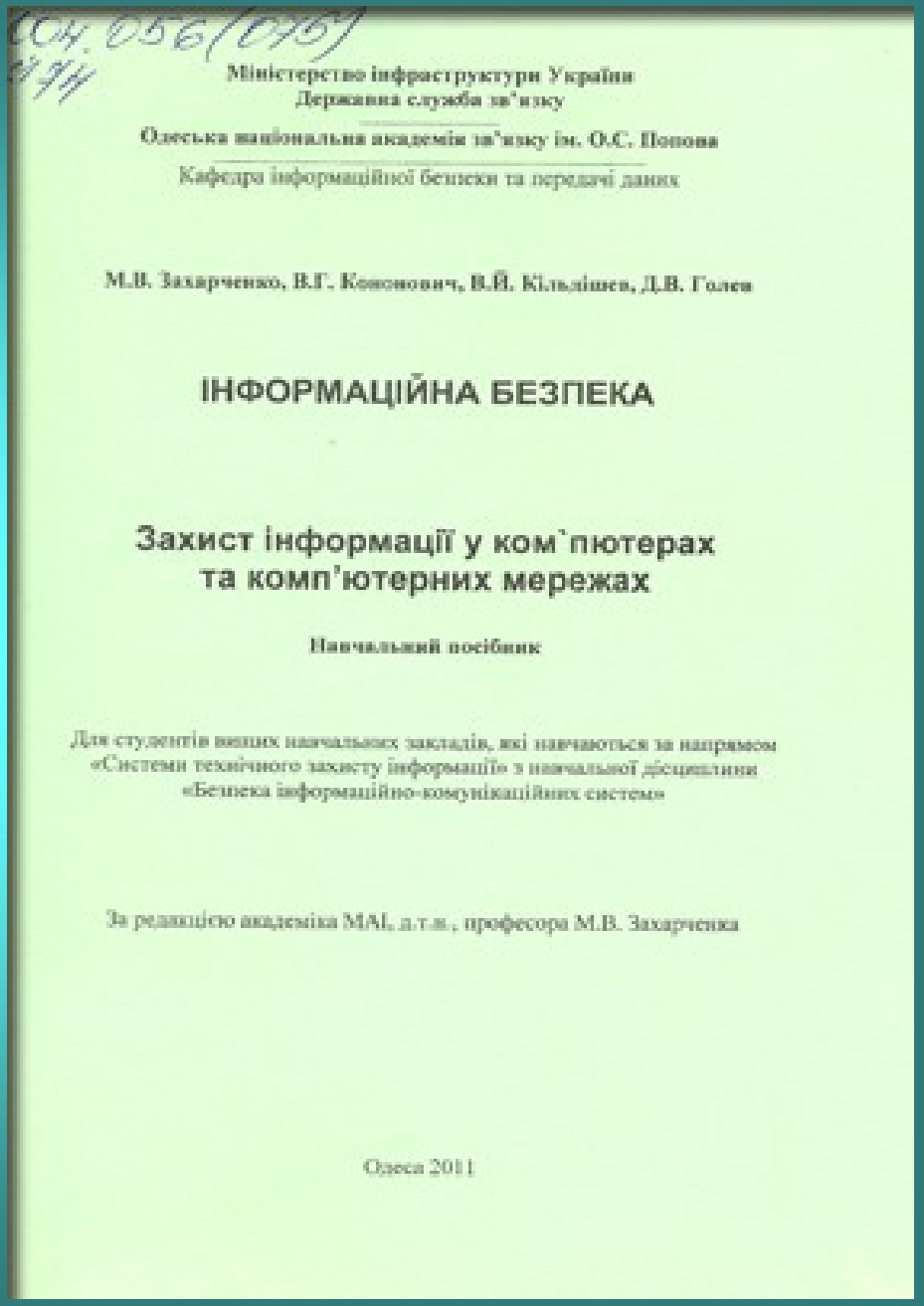
Тардаскіна, Т.М., Менеджмент інформаційної безпеки в галузі зв'язку [Текст] / Каф. економіки підприємства та корпорат. управл.: навчальний посібник / Т.М. Тардаскіна, В.Г. Кононович; за заг. ред. М.В. Захарченка. – Одеса: ОНАЗ ім.О.С. Попова, 2011. – 272 с.

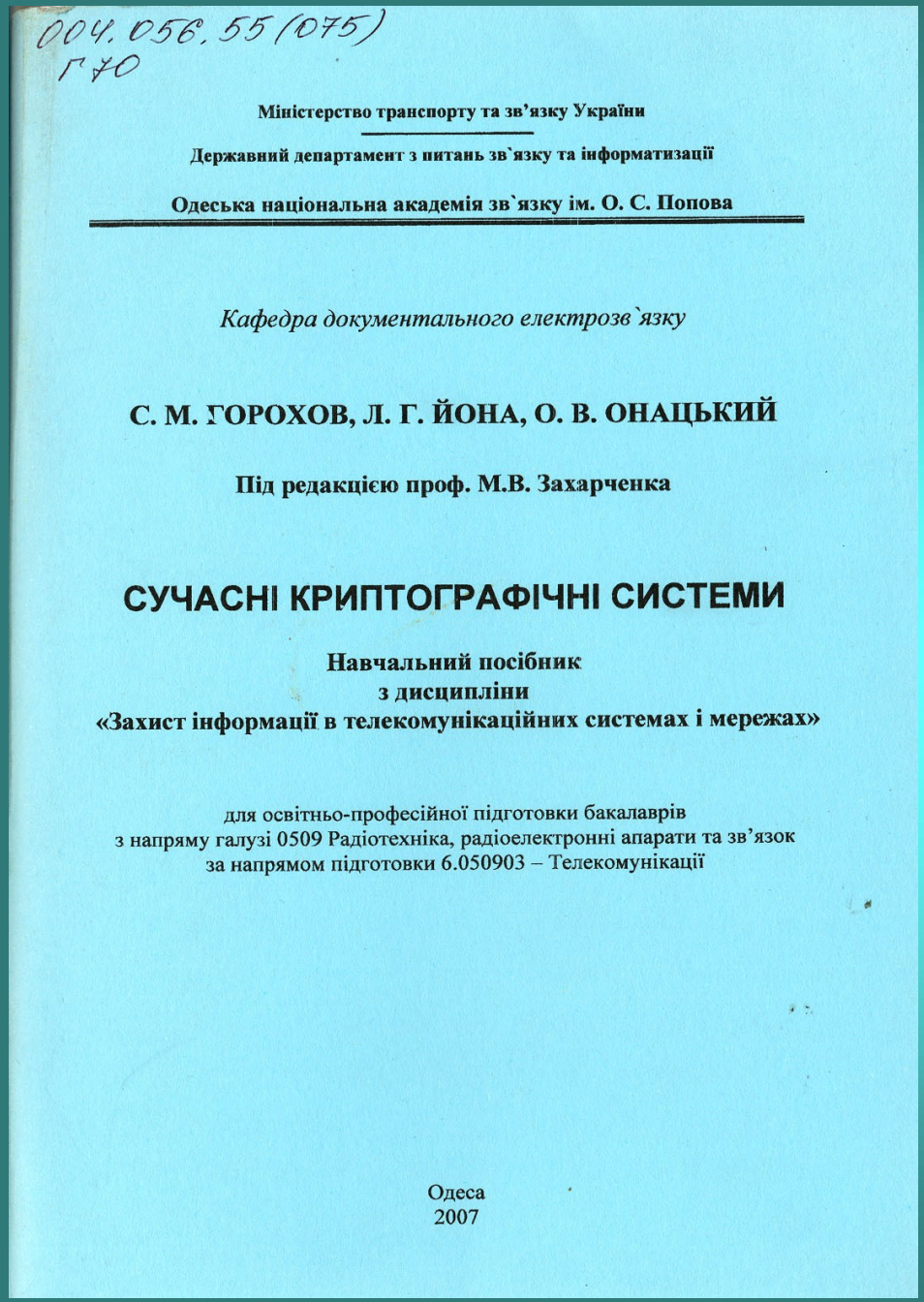
У навчальному посібнику розглянуті теоретичні засади й практичні аспекти менеджменту інформаційної безпеки в галузі зв'язку. Навчальний посібник містить теоретичну частину, контрольні питання, завдання для самостійної роботи та тести. У посібнику висвітлюються основні поняття та задачі менеджменту інформаційної безпеки в умовах формування інформаційного суспільства. Розглядаються основні цілі, задачі та функції забезпечення інформаційної безпеки, джерела загроз та засоби їх впливу на об'єкти інформаційної безпеки, особливості побудови архітектури телекомунікаційних мереж відповідно до вимог інформаційної безпеки. Детально вивчається технологічне управління інформаційною безпекою.

Інформаційна безпека. Захист інформації у комп'ютерах та комп'ютерних мережах [Текст]: навчальний посібник / М.В. Захарченко, В.Г. Кононович, В.Й. Кільдішев, Д.В. Голев; за ред. М.В. Захарченко; Каф. інформаційної безпеки та передачі даних. – Одеса: ОНАЗ ім. О.С. Попова, 2011. – 166 с.

Представлені тематичні цикли лабораторного практикуму в галузі знань «Інформаційна безпека». Цикли лабораторного практикуму складені з навчально-методичних рекомендацій та посібників для виконання лабораторних робіт з напряму підготовки «Системи технічного захисту інформації» й об'єднані завданням створення комплексних систем технічного захисту інформації на об'єктах інформаційної діяльності органів місцевої державної влади.

Навчальний посібник буде корисний студентам бакалаврату, магістрату та слухачам курсів підвищення кваліфікації у галузі знань інформаційної безпеки, для студентів старших курсів вищих навчальних закладів.





Горохов, С.М., Сучасні криптографічні системи: навчальний посібник / С.М. Горохов, Л.Г. Йона, О.В. Онацький; під ред. М.В. Захарченка; Каф. документального електрозв'язку. – Одеса: ОНАЗ ім. О.С. Попова, 2007. – 149 с.

Навчальний посібник призначено для студентів, котрі вивчають дисципліну «Захист інформації в телекомунікаційних системах і мережах». Містить систематичне викладення наукових основ від найпростіших прикладів та основних понять до сучасних криптографічних концепцій. Спрямовано на вивчення симетричних криптосистем. Розглянуто криптосистеми з відкритим ключем, а також питання убезпечення від несанкціонованого втручання в електронних системах.

Асиметричні методи шифрування в телекомун. Мод. 2. Криптогр. методи захисту інформ. в телеком. системах та мережах [Текст]: навч. посібник / М.В. Захарченко, О.В. Онацький, Л.Г. Йона, Т.М. Шинкарук; каф. інформаційної безпеки та передачі данних. – Одеса: ОНАЗ ім. О.С. Попова, 2011. – 181 с.

Розглянуто математичні основи теорії чисел та основні вимоги до хеш-функцій, забезпечуючих мінімізацію мережного трафіку та надлишковість відкритого тексту при криптографічному перетворенні, проведено аналіз сучасних способів організації секретного зв'язку без попереднього обміну ключами алгоритму електронно-цифрового підпису.

Міністерство інфраструктури України
Державна служба зв'язку
Одеська національна академія зв'язку ім. О. С. Попова

**М. В. Захарченко, О. В. Онацький,
Л. Г. Йона, Т. М. Шинкарчук**

АСИМЕТРИЧНІ МЕТОДИ ШИФРУВАННЯ В ТЕЛЕКОМУНІКАЦІЯХ

Модуль 2 – Криптографічні методи захисту інформації в телекомунікаційних системах та мережах

Навчальний посібник
за напрямами підготовки студентів
6.050903 – Телекомунікації
6.170101 – Безпека інформаційних і комунікаційних систем
6.170102 – Системи технічного захисту інформації
6.050901 – Радіотехніка
6.090504 – Мережі та системи поштового зв'язку

Одеса 2011