**СЕВАСТОПОЛЬСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ**
**НАУЧНАЯ БИБЛИОТЕКА**
**ИНФОРМАЦИОННО - БИБЛИОГРАФИЧЕСКИЙ ОТДЕЛ**

**УДК 004.056:005.922.1**

# Информационная безопасность

Рекомендательный библиографический список

Севастополь 2016

Информационная безопасность : рекомендательный библиографический список / Севастопольск. государствен. ун-т; Научн. библ-ка; Информ.-библиографическ. отд. ; [Сост. Пряхина Л. В.]. — Севастополь, 2016. — 40с.

Рекомендательный библиографический список содержит 190 библиографических описаний книг(в том числе электронных изданий ЭБС «Znanium»), статей из периодических изданий, отчетов о НИР. В приведенных документах рассмотрены вопросы преподавания информационной безопасности, существующие подходы к защите информации в коммуникационных системах мониторинга, использующих Web-средства. Проведен анализ программных средств, используемых для обеспечения безопасности информации, циркулирующей в рассматриваемых системах мониторинга, представлены предложения по перспективным направлениям аппаратной реализации средств защиты информации. Рассматриваются задачи принятия решений о составе системы физической защиты потенциально опасных объектов. Определяется этап задачи, использующий знания экспертов — концептуальное проектирование, включающий анализ защищенности объекта, разработку практических рекомендаций по созданию системы физической защиты, выбор варианта и состава инженерно-технических средств охраны.

Библиографические описания выполнены по ГОСТ 7.1-2003 и расположены в алфавитном порядке авторов и заглавий, частично аннотированы.
Данные источники будут интересны для студентов, аспирантов, преподавателей и специалистов в области информационной безопасности.

1. **Абрамов, Т. А.** Программная система динамической идентификации пользователей систем дистанционного обучения [Текст] / Т. А. Абрамов // Информационные технологии и информационная безопасность в науке, технике и образовании "ИНФОТЕХ-2009" : материалы конф. / Севастоп. нац. техн. ун-т, С.-Петерб. гос. ун-т аэрокосм. приборостроения, Ин-т проблем информатики, Люблин. техн. ун-т. — Севастополь : Изд-во Севастоп. нац. техн. ун-та, 2009. — С. 247—248 : рис. — Библиогр. в конце ст.(1). (Шифр в БД 004(06)/И 741-994438)Предлагается использование средств постоянного мониторинга действий пользователя, основанных на анализе клавиатурного почерка обучаемого - динамики набора информации на клавиатуре.
2. **Авдошин, С. М.** Междисциплинарный подход к изучению информационной безопасности на основе анализа конкретных ситуаций / С. М. Авдошин, А. А. Савельева // Информационные технологии : Научно-технический и научно-производственный журнал. — 2012. — **N 5.** — С. 58—62 : табл. — Библиогр. в конце ст. Предлагается подход к преподаванию информационной безопасности, основанный на использовании метода кейс-стади для проведения практических занятий. Обосновывается целесообразность применения метода кейс-стади на примере его использования в рамках курсов "Организация и технология защиты информации" и "Технологии обеспечения информационной безопасности", читаемых студентам магистратуры и бакалавриата отделения программной инженерии НИУ "ВШЭ" с 2008 г. Данная работа восполняет отсутствие методических рекомендаций по использованию метода кейс-стади при преподавании в высших учебных заведениях дисциплин, связанных с защитой информации.
3. **Агапов, А. В.** Обработка и обеспечение безопасности электронных данных [Электронный ресурс] : учеб. пособие / А. В. Агапов, Т. В. Алексеева, А. В. Васильев и др.; под ред. Д. В. Денисова. — М.: МФПУ Синергия, 2012. — Электрон. данные. — Режим доступа : http://znanium.com/bookread2.php?book=451354; по паролю.
Учебное пособие предназначено для подготовки к сдаче государственного экзамена по специальностям «Информационные системы и технологии» (специализации «Безопасность информационных систем» и «Информационные системы электронной коммерции») и «Программное обеспечение вычислительной техники и автоматизированных систем» (специализация «Цифровая обработка данных»).
4. **Акулов, О. А.** Информатика : базовый курс : учебник для студентов высших учебных заведений, бакалавров, магистров, обучающихся по направлению "Информатика и вычислительная техника" / О. А. Акулов, Н. В. Медведев. — 8-е издание, стереотипное. — Москва : Омега — Л, 2013. — 574

с. : ил. ; 22 см. — (Высшее техническое образование). — Библиография: с. 573—574.
(Шифр 004(075.8)/А 441-024049508)
Экземпляры: всего:1 — (1)

5. **Артеменко, М. А.** Обеспечение безопасности данных в коммуникационных системах мониторинга, использующих Web-ГИС / М. А. Артеменко, И. П. Шумейко, Е. В. Шарга // Збірник наукових праць СНУЯЕ та П. — 2014. — **Вып. 1(49).** —С. 173—179. — Библиогр. в конце ст. Библ-ка ИЯЭиП.

Рассмотрены существующие подходы к защите информации в коммуникационных системах мониторинга, использующих Web-средства. Проведен анализ программных средств, используемых для обеспечения безопасности информации, циркулирующей в рассматриваемых системах мониторинга.

6. **Архангельский, А. В.** Опыт аппаратной реализации функциональных модулей средств защиты информации на интегральных схемах программируемой логики / А. В. Архангельский, Н. Ю. Торопченов // Программные продукты и системы. — 2013. — **N 2.** — С. 108—113. — Библиогр. в конце ст.

В статье рассматривается опыт аппаратной реализации основных функциональных систем средств защиты информации на ПЭВМ. Приводится краткий обзор технических характеристик интегральных схем программируемой логики фирмы Altera. Приведены варианты архитектурного построения функциональных модулей. Рассмотрены вариант аппаратной реализации криптозащищенной сети Ethernet и особенности аппаратной реализации криптографического алгоритма. Предлагаются авторские методы реализации блока подстановки условно-постоянных ключей, а также формирования пула случайных чисел на основе аналогового датчика случайных чисел. Представлены авторские предложения по перспективным направлениям аппаратной реализации средств защиты информации.

7. **Астахов, А. М.** Искусство управления информационными рисками / А. М. Астахов. — М. : ДМК Пресс, 2010. — 312 с. : ил. — Библиогр.: с. 238—239.
(Шифр 004.056.5 : 33/А 91-057164)
Экземпляры: всего:2 — ОКХ(1), НА(1)

8. **Бабак, В. П.** Теоретические основы защиты информации : учебник / В. П. Бабак, А. А. Ключников ; НАН Украины, Ин-т проблем безопасности АЭС. — Чернобыль : Ин-т проблем безопасности АЭС, 2012. — 776 с. — Библиогр.: с. 774—775.
Экземпляры: всего:1 — ЧЗ библ-ки ИЯЭиП (1)

В учебнике изложены основные понятия и методы защиты информации, базирующиеся на математическом аппарате преобразования и исследования информационных сигналов, технологиях измерения, передачи и обработки информации, сигналов и данных, на помехоустойчивом кодировании, использовании современных информационно-коммуникационных каналов передачи информации, на алгоритмах шифрования и дешифрования, стегано- и криптографии, цифровой подписи и т.п.

9. **Бабаш, А. В**. История защиты информации в зарубежных странах [Электронный ресурс]: Учебное пособие / А.В. Бабаш, Д.А. Ларин. — М.: РИОР: ИНФРА-М, 2013. — Электрон. данные. — Режим доступа : http://znanium.com/bookread2.php?book=492549; по паролю.
В учебном пособии дается краткое изложение истории криптографии с исторически известного в настоящее время момента возникновения криптографии (Древняя Греция, Рим). Авторы стремятся не только показать и разъяснить появлявшиеся в историко-хронологическом порядке криптографические идеи, конкретные способы шифрования, но и дать характеристику культуры конкретной исторической эпохи, в которой эти идеи и шифры появлялись. Предназначено для студентов высших учебных заведений, обучающихся по направлениям информационной безопасности и прикладной информатики.
10. **Бабаш, А. В.** Криптографические методы защиты информации. Т. 3: учеб.-метод. пособие / А.В. Бабаш. — 2-е изд. — М.: РИОР: ИНФРА-М, 2014. — (Высшее образование: Бакалавриат). — Электрон. данные. — Режим доступа : http://znanium.com/bookread2.php?book=432654; по паролю.
Пособие предназначено для студентов высших учебных заведений, обучающихся по специальности «Прикладная информатика (в экономике)». Оно также содержит методический материал для ряда инновационных курсов лекций по профилю «Информационная безопасность» и может быть использовано для блока дисциплин этого профиля. Ряд представленных результатов полезен специалистам и аспирантам, специализирующимся в указанной области.
11. **Баранова, Е. К.** Информационная безопасность и защита информации : учеб. пособие / Е. К. Баранова, А. В. Бабаш. — 2-е изд. — М. : РИОР : ИНФРА — М, 2014. — 255 с. : ил., табл. — (Высшее образование). — Библиогр. в конце гл.
(Шифр 004.7.056.5(075.8/Б 241-976101)
Экземпляры: всего:1 — ЧЗТ(1)
12. **Баранова, Е. К.** Информационная безопасность и защита информации: Учебное пособие/Баранова Е. К., Бабаш А. В., 3-е изд. — М.: РИОР : ИНФРА-М, 2016. — 322 с. — (Высшее образование); То же [Электронный ресурс]. — Электрон. данные. — Режим доступа : http://znanium.com/bookread2.php?book=495249; по паролю.
Учебное пособие посвящено рассмотрению базовых вопросов информационной безопасности и защиты информации и может быть рекомендовано бакалаврам и магистрам, изучающим курсы «Информационная безопасность» и «Управление информационной безопасностью», а также смежные с ними дисциплины. Книга может быть также полезна аспирантам и специалистам, интересующимся вопросами защиты информации.
13. **Башлы, П. Н.** Информационная безопасность и защита информации [Электронный ресурс] : Учебник / П. Н. Башлы, А. В. Бабаш, Е. К. Баранова. — М.: РИОР, 2013. — Электрон.

данные. — Режим доступа http://znanium.com/bookread2.php?book=405000; по паролю.

Учебник посвящен рассмотрению базовых вопросов информационной безопасности и защиты информации, представляет интерес для студентов высших учебных заведений. Книга может быть также полезна аспирантам и специалистам, интересующимся вопросами защиты информации.

14. **Безопасность** критических инфраструктур**:** математические и инженерные методы анализа и обеспечения = Safety of Critical Infrastructures: Mathematical and Engineering Methods of Analysis and Ensuring / М-во образования и науки, молодежи и спорта Украины, Нац. аэрокосм. ун-т им. Н. Е. Жуковского "Харьк. авиац. ин-т" ; ред. В. С. Харченко. — [Харьков] : [Изд-во Нац. аэрокосм. ун-та им. Н. Е. Жуковского "Харьк. авиац. ин-т"], 2011. — 641 с. : ил., табл. — (Проект TEMPUS-SAFEGUARD). — Список сокр.: С. 3—5. — Библиогр. в конце разд.
(Шифр 681.51 : 519.7/.8/Б 40-946328)
Экземпляры: всего:3 — (1), НА(1), ЧЗТ(1)
15. **Бельфер, Р. А.** Информационная безопасность сети связи для соединений абонентов ТфОП/ISDN через SIP-T / Р. А. Бельфер, А. М. Морозов // Электросвязь : науч.-техн. журн. по провод. радиосвязи, телевидению и радиовещанию. — 2012. — **N 3**. — С. 22—25 : схема, а-рис. — Библиогр. в конце ст.
16. **Белявин, В. Ф.** Разработка методов повышения помехоустойчивости охранных систем / В. Ф. Белявин // Управляющие системы и машины: информационные технологии : междунар. науч. журн. — 2013. — **N 1**. — С. 85—92 : схема, а-граф. — Библиогр. в конце ст.
17. **Бирюков, Д. Н.** Построение систем информационной безопасности: от живых организмов к киберсистемам / Д. Н. Бирюков, А. Г. Ломако // Защита информации. Инсайд : информ. — метод. журн. — 2013. — **N 2**. — С. 61—65 : схема. — Библиогр. в конце ст.
18. **Боровский, А. С.** Приближенная оценка защищенности потенциально опасных объектов. структурные параметры защищенности объектов / А. С. Боровский, А. Д. Тарасов // Программные продукты и системы. — 2013. — **N 3**. — С. 235—243. — Библиогр. в конце ст.

Рассматривается задача принятия решения о составе системы физической защиты потенциально опасных объектов. Определяется этап задачи, использующий знания экспертов – концептуальное проектирование, включающий анализ защищенности объекта, разработку

практических рекомендаций по созданию системы физической защиты, выбор варианта и состава инженерно-технических средств охраны. Целью статьи является разработка моделей для методик оценки защищенности объектов. Основа разрабатываемого метода – представление объекта защиты в виде графа. Рассмотрены общие свойства графа объекта. Введено определение меры структурной защищенности. Оценивается возможность нарушителя добраться до одного из критических элементов объекта без обнаружения техническими средствами защиты и без задержки физическими барьерами. Оценивается возможность применения алгоритма Дейкстры для поиска наименее защищенного пути и разрабатывается модифицированный алгоритм для поиска меры структурной защищенности. Описываются способы обработки экспертной информации в виде нечетких чисел. Показан пример поиска меры структурной защищенности с помощью программы.

19. **Бочков, М. В.** Имитационное моделирование процессов управления защищенностью ресурсов компьютерной сети на основе иерархических раскрашенных временных сетей Петри / М. В. Бочков, Ю. П. Лалушкин, А. А. Шкадов // Информационные технологии : Научно-технический и научно-производственный журнал. — 2012. — **N 6**. — С. 29—33 : схема, а-табл. — Библиогр. в конце ст.

    Предложена модель управления защищенностью компьютерной сети на основе иерархических раскрашенных временных сетей Петри. Проведен анализ существующих подходов к управлению защищенностью компьютерной сети. Рассмотрены особенности применения модели на примере реализации угроз, направленных на web-приложения.

20. **Брауде-Золотарев, Ю. М.** Криптостойкая защита информации в радиосвязи / Ю. М. Брауде-Золотарев // Защита информации. Инсайд : информ. — метод. журн. — 2013. — **N 3**. — С. 74—80 : табл. — Библиогр. в конце ст.

21. **Брюховецкий, А. А.** Адаптивная модель обнаружения уязвимостей в критических приложениях на основе решающих деревьев и байесовского классификатора [Текст] / А. А. Брюховецкий, А. В. Скатков, П. О. Березенко // Современные проблемы прикладной математики, информатики, автоматизации и управления" : материалы 3-го междунар. науч.-техн. семинара, 9—13 сент. 2013 г., Севастополь / М-во образования и науки, молодежи и спорта Украины, Севастоп. нац. техн. ун-т, Рос. акад. наук, Ин-т проблем информатики. — М., 2013. — С. 54—62 : рис., табл. — Библиогр. в конце ст. (4). (Шифр в БД 519.1(063)/С 568-133767)

22. **Брюховецкий, А. А.** Модель обнаружения нарушений прав доступа с использованием методов ИИС [Текст] / А. А. Брюховецкий, А. В. Скатков // Автоматизація: проблеми, ідеї, рішення : матеріали міжнар. наук.-техн. конф. (Севастополь, 5—9 верес. 2011 р.) / М-во освіти і науки, молоді та спорту

України, Севастоп. нац. техн. ун-т. — Севастополь, 2011. — С. 213.
(Шифр в БД 658.52.011.56(06)/А 224-083070)
В докладе представлен метод негативной селекции, который моделирует процесс генерации детекторов для обнаружения аномального поведения системы.

23. **Букин, М.** Безопасность при платежах в Сети / М. Букин // Банковские технологии. — 2011. — **N 1**. — С. 35—37. — Библиогр. в конце ст.
24. **Булдыжов, В. И.** Электротехнические аналоги в оценке рисков информационной безопасности / В. И. Булдыжов // Электронное моделирование : междунар. науч.-теорет. журн. — 2012. — **Том 34**, **N 6**. — С. 63—72 : рис. — Библиогр. в конце ст.
25. **Бычков, С. С.** Аудит информационной безопасности систем электронной подписи / С. С. Бычков // Защита информации. Инсайд : информ.- метод. журн. — 2012. — **N 4**. — С. 45—49 : схема, а-табл. — Библиогр. в конце ст.
26. **Васенин, В. А.** К созданию международной системы мониторинга и анализа информационного пространства для предотвращения и прекращения военно-политических киберконфликтов / В. А. Васенин // Информационные технологии : Научно-технический и научно-производственный журнал. — 2012. — **N 9**. — С. 2—10. — Библиогр. в конце ст.
Рассматриваются вопросы, связанные с появлением новой, очень востребованной и многоаспектной задачи создания международной системы мониторинга и анализа информационного пространства для предотвращения и прекращения военно-политических киберконфликтов. Анализируются модели и методы, нормативно-правовые и программные механизмы, которые могут быть положены в основу ее решения. Предлагаются общие подходы, учитывающие уже годами сложившиеся на этом направлении реалии.
27. **Васильков, А. В.** Информационные системы и их безопасность : учеб. пособие / А. В. Васильков, А. А. Васильков, И. А. Васильков. — М. : Форум, 2014. — 528 с. : ил. — (Профессиональное образование). — Библиогр.: с. 513—514. — Предм. указ.: с. 515—518.
(Шифр 004.7.056.5(075.8/В 19-195861)
Экземпляры: всего:1 — УА(1)
28. **Васильков, А. В.** Безопасность и управление доступом в информационных системах [Электронный ресур] : Учебное пособие / А.В. Васильков, И.А. Васильков. — М.: Форум: ИНФРА-М, 2013. — (Профессиональное образование) —

Электрон. данные. — Режим доступа : http://znanium.com/bookread2.php?book=405313; по паролю.

В пособии предложены для изучения подходы, базовая концепция, принципы построения систем безопасности и оценки уровня безопасности информации в информационных системах, сетях и автоматизированных системах управления. С этих позиций рассматриваются информация и условия ее обработки в информационных системах: потенциальные угрозы, возможные каналы несанкционированного доступа, методы, средства и системы управления в условиях обеспечения безопасности. Цель учебного пособия — показать будущему специалисту возможность создания системы безопасности информации с гарантированными характеристиками, качеством и оптимальными затратами. Для студентов среднего профессионального образования и бакалавров, специалистов в области защиты и безопасности информации в информационных и автоматизированных системах ее обработки и управления. Может быть рекомендована разработчикам, пользователям и владельцам информационных систем, государственным и военным организациям, различным финансовым и корпоративным структурам.

29. **Воеводин, Д. П.** Структура понятия надежности вычислительной системы / Д. П. Воеводин // Информационные технологии : науч.-техн. и науч.-произв. журн. — 2013. — **N 9.** — С. 52—55 : рис. — Библиогр. в конце ст.

Надежность является обобщающим понятием, вокруг которого развивается множество связанных с ней теорий и исследований. С позиции программных систем определяется структура понятия надежности вычислительной системы и круг относящихся к надежности вопросов, которые могут потребовать рассмотрения и решения при проектировании больших информационно-вычислительных и управляющих программно-аппаратных комплексов. Указываются некоторые имеющие отношение к надежности вычислительных систем методики и технологии. Отмечаются связи основных структурных элементов надежности вычислительной системы с другими предметными областями.

30. **Галатенко, А. В.** К постановке задачи разграничения доступа в распределенной объектной среде / А. В. Галатенко, В. А. Галатенко // Программная инженерия : теорет. и приклад. науч.-техн. журн. — 2013. — **N 5.** — С. 27—30. — Библиогр. в конце ст.

Рассматривается задача разграничения доступа применительно к объектным системам. По мнению авторов, с позиций объектного подхода и с опорой на логический аппарат удается добиться естественной и технологичной постановки этой задачи. Подобный подход целесообразно реализовать и применить в рамках концепции контролируемого выполнения.

31. **Галатенко, В. А.** Категорирование и разделение программ и данных как принцип архитектурной безопасности / В. А. Галатенко // Программная инженерия : теорет. и приклад. науч.-техн. журн. — 2012. — **N 7.** — С. 2—6 : рис. — Библиогр. в конце ст.

Рассматриваются архитектурные аспекты обеспечения информационной безопасности. В качестве одного из принципов архитектурной безопасности предлагается категорирование и разделение программ и данных. Это особенно важно при разработке и реализации программных средств обеспечения информационной безопасности, способных противостоять деструктивным воздействиям.

32. **Гвоздева, В. А.** Базовые и прикладные информационные

технологии : учеб. для студ. вузов, обуч. по техн. спец. / В. А. Гвоздева. — М. : Форум : Инфра — М, 2014. — 384 с. : ил. — (Высшее образование). — Библиогр.: с. 376—378.
(Шифр 004(075.8)/Г 256-274365)
Экземпляры: всего:1 — ЧЗТ(1)

33. **Геоинформационные системы и** основы дешифрования : учебное пособие для студентов вузов специальностей 230100.62 "Информатика и вычислительная техника (для бакалавров) в области АСОИУ и САПР" и для магистерской программы 230100.68-27 "Компьютерная графика и Web-дизайн" направления 230100.68 "Информатика и вычислительная техника" / сост. М. В. Телегина. — Ижевск : Издательство Ижевского государственного технического университета им. М. Т. Калашникова, 2012. — 157, [1] с. : ил. ; 20 см. — Библиография: с. 156-158.
(Шифр 528 : 004.9(075.8/Г 357-676473)
Экземпляры: всего:1 - ЧЗТ(1)

34. **Гизатуллин, З. М.** Моделирование электромагнитной обстановки на основе теории масштабного эксперимента для задач электромагнитной совместимости и защиты информации / З. М. Гизатуллин, Р. М. Гизатуллин // Информационные технологии : науч.-техн. и науч.-произв. журн. — 2013. — **N 4.** — С. 19—22 : табл., а-фото, а-граф. — Библиогр. в конце ст.
Предложена методика и приведены результаты моделирования магнитных полей внутри здания при воздействии источника тока на элементы металлоконструкции здания на основе теории масштабного эксперимента.

35. **Гильберт, К.** Применение средств криптографической защиты мобильной информации в локальных приложениях / К. Гильберт // Защита информации. Инсайд : информ. — метод. журн. — 2013. — **N 3.** — С. 35—37 : рис. — Библиогр. в конце ст.
Кратко проанализированы способы сетевого взаимодействия между виртуальной машиной и хостом, которые реализуются большинством современных систем виртуализации. К ним относятся NAT, сетевой мост, подключение только к хосту и внутренняя виртуальная сеть, не имеющая выход за пределы хоста. Также отмечены основные проблемные вопросы реализации этих режимов.

36. **Гладыш, С. В.** Настройка параметров модели распределения ресурсов информационной безопасности с помощью нечетких нейронных сетей / С. В. Гладыш // Вестник СевГТУ : сб. науч. тр. / Севастоп. нац. техн. ун-т. — Севастополь : Изд-во

Севастоп. нац. техн. ун-та, 2007. — Вып. 82: Информатика, электроника, связь. — С. 33—39 : рис. — Библиогр. в конце ст.(4). (Шифр в БД 06/С 28-835043)
Проведен анализ возможностей использования нечетких нейронных сетей в задачах настройки параметров нечетких моделей. Показаны особенности настройки параметров модели распределения ресурсов информационной безопасности. В инструментальной среде моделирования ANFIS пакета Fuzzy Logic Toolbox MATLAB 6.5 построена Jang - адаптивная нечеткая нейронная сеть, с помощью которой выполняется настройка и исследование функций принадлежности разрабатываемой модели.
Экз-ры: всего: ОКХ(29), ЧЗ НП(1)

37. **Глазырин, И.** Как снизить банковские риски: IT и информационная безопасность / И. Глазырин // Банковские технологии. — 2012. — **N 5.** — С. 65—67. — Библиогр. в конце ст.
38. **Глинская, Е. В.** Информационная безопасность конструкций ЭВМ и систем [Электронный ресурс] : учебное пособие / Е.В. Глинская, Н.В. Чичварин. — М.: ИНФРА-М, 2016. — 118 с.: 60х90 1/16. - (Высшее образование). — Электрон. данные. — Режим доступа : http://znanium.com/bookread2.php?book=507334; по паролю.
39. **Глоба, Л. С.** Обнаружение сетевых аномалий на основе нейросетевых технологий [Текст] / Л. С. Глоба; Я. А. Демидова, М. Ю. Терновой // СВЧ-техника и телекоммуникационные технологии (КрыМико 2006): Материалы 16-й Междунар. Крымской конф. в 2-х т., 11—15 сентября 2006 г. — Севастополь : Вебер, 2006. — **Т.1.** — С. 412—413. — Библиогр. в конце ст.Обоснована целесообразность использования нейросетевых технологий для выявления аномалий в сетевом трафике. Предложен метод решения задачи выявления аномалий сетевого трафика на основе нейросетевого подхода. Для решения поставленной задачи произведен выбор модели нейросети с обратным распространением ошибки. Промоделированы некоторые типы DoS/DDos (Danial of Service) атак. Проанализирована эффективность данного подхода для выявления Dos/DDoS атак на практике.
40. **Голубев, Е. А.** Эволюция парадигмы защиты информации / Е. А. Голубев // Электросвязь : науч.-техн. журн. по провод. радиосвязи, телевидению и радиовещанию. — 2012. — **N 3.** — С. 36—38. — Библиогр. в конце ст.
41. **Горшков, Ю. Г.** Анализ риска информационной безопасности сетей GSM при выполнении функций защиты приватности / Ю. Г. Горшков, Р. А. Бельфер // Электросвязь : науч.-техн. журн. по провод. радиосвязи, телевидению и радиовещанию. — 2012.

— **N 3**. — С. 26—29. — Библиогр. в конце ст.

42. **Гришина, Н. В.** Информационная безопасность предприятия [Электронный ресурс] : Учебное пособие / Н.В. Гришина. — 2-е изд., доп. — М.: Форум: ИНФРА-М, 2015. — 240 с.: ил.; 60x90 1/16. — (Высшее образование: Бакалавриат). — Электрон. данные. — Режим доступа : http://znanium.com/bookread2.php?book=491597; по паролю.

В учебном пособии рассмотрены основные понятия, определения, положения и методологические подходы к организации комплексной системы защиты информации. Особое внимание уделено проблеме «человеческого фактора». Соответствует требованиям государственного стандарта образовательной программы полготовки бакалавров 090900.62 «Информационная безопасность». Пособие предназначено для студентов, аспирантов, преподавателей высших учебных заведений, занимающихся вопросами защиты информации.

43. **Груздева, Л. М.** Повышение производительности корпоративной сети АСУ в условиях воздействия угроз информационной безопасности / Л. М. Груздева, М. Ю. Монахов // Известия ВУЗов. Сер, Приборостроение. — 2012. — **Том 55**, **N 8**. — С. 53—56 : схема. — Библиогр. в конце ст.

Формализована задача повышения производительности в условиях воздействия угроз информационной безопасности корпоративной сети как задача построения системы защиты, обеспечивающей максимально возможный уровень производительности сети при достоверном обнаружении и эффективном противодействии угрозам информационной безопасности.

44. **Гуриков, С. Р.** Информатика : учеб. для студ. образоват. учреждений высш. образования / С. Р. Гуриков. — М. : Форум, 2014. — 462 с. : ил. — (Высшее образование. Бакалавриат). — Библиогр.: с. 462 (19 назв.).
(Шифр 004(075.8)/Г 952-775242)
Экземпляры: всего:1 — ЧЗТ(1)

45. **Гусева, А. И.** Вычислительные системы, сети и телекоммуникации : учебник для студентов высших учебных заведений, обучающихся по направлению "Прикладная информатика" / А. И. Гусева, В. С. Киреев. — Москва : Академия, 2014. — 287, [1] с. : ил. ; 22 см. — (Учебник). — (Высшее профессиональное образование. Бакалавриат. Информатика и вычислительная техника). — Библиография: с. 284.
(Шифр 004.7(075.8)/Г 962-633802)
Экземпляры: всего:1 — ЧЗТ(1)

46. **Дзялошинский, И.** Ресурсы взаимодействия: информационная агрессия в бизнес-коммуникациях / И. Дзялошинский // Проблемы теории и практики управления : междунар. журн. —

2012. — **N 11/12.** — С. 113—117. — Библиогр. в конце ст. (15).

Рассматриваются методы и приемы так называемой информационной войны. Разбираются примеры из практики рекламных кампаний известных фирм.

47. **Докучаев, В. А.** Защита информации на корпоративных сетях VoIP / В. А. Докучаев, А. В. Шведов // Электросвязь : науч.-техн. журн. по провод. радиосвязи, телевидению и радиовещанию. — 2012. — **N 4.** — С. 5—8 : рис. — Библиогр. в конце ст.

48. **Дрозд, А.** Киберугрозы при использовании мобильного Интернета / А. Дрозд // Защита информации. Инсайд : информ. — метод. журн. — 2013. — **N 1.** — С. 42—47 : ил. — Библиогр. в конце ст.

Большинство людей лет 10–15 назад вряд ли смогли даже представить функциональные возможности современных смартфонов. Электронная почта, музыка, видео, книги, мессенджеры, интернет-серфинг, NFC-чипы, и все это собрано воедино в пластиковом корпусе, умещающемся в кармане джинсов. Но, как известно, спрос рождает предложение. И чем более популярным становится то или иное решение, тем большее внимание ему уделяют киберпреступники. Мобильные гаджеты — яркое тому подтверждение.

49. **Дубинин, Е. А.** Оценка относительного ущерба безопасности информационной системы [Электронный ресурс] : Монография. / Е. А. Дубинин, Ф. Б. Тебуева, В. В. Копытов. — М.: РИОР: ИНФРА-М, 2014. — (Научная мысль) — Электрон. данные. — Режим доступа : http://znanium.com/bookread2.php?book=471787; по паролю.

В монографии исследуется адекватность существующих способов оценки ущерба безопасности информационной системы. Для повышения достоверности оценки относительного ущерба безопасности информационной системы предложено использовать мнения экспертов. Разработан модифицированный метод сложения функций принадлежности нечетких экспертных оценок, который учитывает важность мнений экспертов и пригоден для носителей в относительных величинах. Модифицированный метод сложения функций принадлежности нечетких экспертных оценок пригоден для реализации в системах менеджмента и аудита информационной безопасности. Для специалистов в области аудита безопасности объектов информатизации, а также для преподавателей, студентов и аспирантов технических специальностей.

50. **Елович, И. В.** Информатика : учебник для студентов вузов, обучающихся по техническим и естественно-научным направлениям / И. В. Елович, И. В. Кулибаба ; под редакцией профессора Г. Г. Раннева. — Москва : Академия, 2011. — 393, [1] с. : ил. ; 22 см. — (Учебник). — (Высшее профессиональное образование. Бакалавриат. Информатика). — Библиография: с. 388-390 (57 назв.)
(Шифр 004(075.8)/Е 53-913818)
Экземпляры: всего:1 — ЧЗТ(1)

51. **Жданов, О. Н.** Методика выбора ключевой информации для алгоритма блочного шифрования [Электронный ресурс] : Монография / О.Н. Жданов. — М.: ИНФРА-М, 2013. — (Научная мысль; Информатика). — Электрон. данные. — Режим доступа : http://znanium.com/bookread2.php?book=412754; по паролю.

    Как известно, при использовании незащищенного канала актуальными являются задачи обеспечения конфиденциальности передаваемых данных и аутентификации источника сообщений. В настоящее время для решения этих задач используются итерированные симметричные алгоритмы блочного шифрования, такие как ГОСТ 28147-89, DES, IDEA, AES и т.п. Безопасность зашифрованных сведений обеспечивается не только алгебраической структурой алгоритма, но также и корректным выбором элементов ключевой информации (ключа и таблиц замен). Автором на основе проведенного анализа существующих подходов к построению ключей и таблиц замен разработана методика генерации и тестирования ключевой информации для алгоритмов блочного шифрования. Автором совместно с Чалкиным В. А. эта методика программно реализована. Представлены алгоритм и исходные тексты программ, приведены результаты экспериментов.

52. **Жидко, Е. А.** Принципы системного математического моделирования информационной безопасности / Е. А.Жидко, Л. Г Попова // Науковедение : Интернет-журнал — [Электронный ресурс]. — 2014. — Вып. 2 (21). — (Электронно-библиотечная система «Znanium»). — Электрон. данные. — Режим доступа : http://znanium.com/bookread2.php?book=487844; по паролю.

53. **Жуков, В. Г.** Модель нарушителя прав доступа в автоматизированной системе / В. Г. Жуков, М. Н. Жукова, А. П. Стефаров // Программные продукты и системы. — 2012. — **N 2.** — С. 75—78 : схема, а-табл. — Библиогр. в конце ст.

54. **Жукова, М. Н.** Управление информационной безопасностью. Ч. 2. Управление инцидентами информационной безопасности [Электронный ресурс] : учеб. пособие / М. Н. Жукова, В. Г. Жуков, В. В. Золотарев. — Красноярск : Сиб. гос. аэрокосмич. ун-т, 2012. — Электрон. данные. — Режим доступа : http://znanium.com/bookread2.php?book=463061; по паролю.

    Во второй части учебного пособия рассматриваются методы и средства управления инцидентами информационной безопасности, начиная от организационных моментов и заканчивая применением интеллектуальных технологий в области анализа аномалий и обнаружения атак. Особое внимание уделено практическим примерам применения интеллектуальных технологий обнаружения и анализа инцидентов.

55. **Задирака, В. К.** Облачные вычисления в криптографии и стеганографии / В. К. Задирака, А. М. Кудин // Кибернетика и системный анализ : междунар. науч.-теорет. журн. — 2013. - **N 4.** — С. 113—119. — Библиогр. в конце ст.

56. **Задирака, В. К.** О технологии картографической защиты информации на специальных цифровых носителях / В. К. Задирака, А. М. Кудин, В. А. Людвиченко, А. С. Олексюк // УСиМ. — 2010. — **№4**. — с. 77—83. — Библиогр. в конце ст.Исследованы вопросы разработки новой технологии реализации средств криптографической защиты информации, адекватных современным технологиям распределенной обработки данных.
57. **Защита информации** [Электронный ресурс] : Учебное пособие / А. П. Жук, Е. П. Жук, О. М. Лепешкин, А. И. Тимошкин. — 2-е изд. — М.: РИОР: ИНФРА-М, 2015. — (Высшее образование: Бакалавриат; Магистратура). — Электрон. данные. — Режим доступа : http://znanium.com/bookread2.php?book=474838; по паролю. Рассматриваются основы защиты информации, анализируются угрозы информационной безопасности, стратегии и модели защиты информации, основы государственной политики РФ в области защиты информации, а также раскрыты основные виды обеспечения системы защиты информации в них. Основное внимание уделяется четырем основным видам обеспечения защиты информации в инфокоммуникационных системах: правовому, организационному, инженерно-техническому и программно-аппаратному. Материал учебного пособия опирается на современные подходы в области защиты информации. Предназначено для студентов, обучающихся по направлению подготовки 210700 «Инфокоммуникационные технологии и системы связи».
58. **Золотарев, В. В.** Управление информационной безопасностью. Ч. 1. Анализ информационных рисков [Электронный ресурс] : учеб. пособие/ В. В. Золотарев, Е. А. Данилова. — Красноярск :Сиб. гос. аэрокосмич. ун-т, 2010. — Электрон. данные. — Режим доступа : http://znanium.com/bookread2.php?book=463037; по паролю.
Пособие знакомит студентов с основными особенностями анализа и управления информационными рисками как базового уровня моделей и методов управления информационной безопасностью. Рассматриваются методы количественного и качественного измерения показателей, характеризующих информационный риск, приводятся базовые и новые модели риска, дается обзор основных методик и инструментальных средств управления риском. Приведены необходимые справочные данные.
59. **Иванов, В.** Trusteer Rapport: на страже безопасности систем ДБО / В. Иванов // Банковские технологии. — 2012. — **N 4**. — С. 74—75. — Библиогр. в конце ст.
60. **Иванов, В.** Контроль браузера клиента: важный шаг в безопасности ДБО / В. Иванов // Банковские технологии. — 2012. — **N 3**. — С. 72—73. — Библиогр. в конце ст.
61. **Имамвердиев, Я. Н.** Метод обнаружения переделанных отпечатков пальцев на основе фрактальных характеристик / Я. Н. Имамвердиев // Информационные технологии : Научно-

технический и научно-производственный журнал. — 2012. — **N 9**. — С. 1—16 : рис., а-табл. — Библиогр. в конце ст.

Рассмотрена возможность использования концепций теории фракталов для описания свойств отпечатков пальцев. Разработан метод определения фрактальной размерности отпечатков пальцев и на его основе предложен эффективный подход для обнаружения переделанных отпечатков пальцев. Результаты экспериментов показывают, что метод хорошо отличает изображения реальных отпечатков пальцев от переделанных. Предложенный метод не требует дополнительного оборудования и легко встраивается в существующие системы распознавания отпечатков пальцев.

62. **Информационные процессы** и технологии "Информатика-2014", Международная научно-практическая конференция (7 ; 2014 ; Севастополь).

    7-я Международная научно-практическая конференция "Информационные процессы и технологии "Информатика-2014", 22-26 апреля 2014 г. = Information Processes and Technologies "Computer Sciences-2014" = Інформаційні процеси і технології "Інформатика-2014" : материалы конференции / науч. ред. С. В. Доценко ; ред.: А. П. Фалалеев, И. В. Кудрявченко, В. Ю. Карлусов. — Севастополь : Вебер, 2014. — 188 с. : ил. ; 29 см. — Библиография в конце статей. (Шифр 004(063)/И 74-397825)

    Экземпляры: всего:1 — ОКХ(1)

63. **Информационные системы и** технологии в экономике и управлении [Текст] : учеб. для бакалавров : учеб. по спец. "Менеджмент организации" / С.-Петерб. гос. ун-т экономики и финансов ; ред. В. В. Трофимов. — 3-е изд., перераб. и доп. — М. : Юрайт, 2012. — 526 с. : ил. — (Бакалавр). — Библиогр. в конце разд.

64. **Информационные технологии для** критических инфраструктур = Information Technologies for Critical Infrastructures : монография / А. В. Скатков, В. С. Харченко, Д. Ю. Воронин ; ред. А. В. Скатков ; М-во образования и науки, молодежи и спорта Украины, Севастоп. нац. техн. ун-т. — Севастополь : Изд-во Севастоп. нац. техн. ун-та, 2012. — 306 с. — Библиогр. в конце гл. (Шифр 004 : 62/И 741-279615)

    Экземпляры: всего:5 — ЧЗТ(1), НА(3), ОКХ(1)

65. **Исследование пассивных инфракрасных** извещателей охранной сигнализации [Текст] : метод. указания к выполнению лаборатор. работы по дисц. "Радиоэлектронные системы защиты объектов и информации" для студ. спец.

"Радиотехника" дневной и заоч. форм обучения / СевНТУ ; Сост. И. В. Лащенко, Г. А. Лукьянчук. — Севастополь : Изд-во СевНТУ, 2008. — 16 с. : ил.

66. **Исследование электронного** металлодетектора [Текст] : метод. указания к выполнению лаборатор. работы № 2 по дисц. "Радиоэлектронные системы защиты объектов и информации" студ. спец. "Радиотехника" дневной и заоч. форм обучения / СевНТУ ; Сост. И. В. Лащенко, В. И. Носкович. — Севастополь : Изд-во СевНТУ, 2008. — 16 с. : ил.
67. **Ищейнов, В. Я.** Основные положения информационной безопасности [Электронный ресурс] : Учебное пособие/В. Я. Ищейнов, М. В.Мецатунян — М.: Форум, ИНФРА-М, 2015. — Электрон. данные. — Режим доступа : http://znanium.com/bookread2.php?book=508381; по паролю.

В учебном пособии рассмотрены основные положения информационной безопасности; методы и средства обеспечения информационной безопасности; вопросы зашиты информации; способы и средства противодействия техническим разведкам. Изложены основы безопасности систем обработки данных. Пособие написано в соответствии с учебной программой «Основы информационной безопасности» и соответствует требованиям государственного стандарта образовательной программы среднего профессионального образования подготовки специалистов по специальности 10.02.01 «Организация и технология зашиты информации». Учебное пособие предназначено для студентов средних профессиональных учебных заведений, обучающихся в области информационной безопасности, а также организации и технологии зашиты конфиденциальной информации.

68. **Казарин, О. В.** Методология обеспечения проактивной безопасности компьютерных систем / О. В. Казарин, В. Ю. Скиба // Защита информации. Инсайд : информ. — метод. журн. — 2013. — **N 2.** — С. 52—60 : схема. — Библиогр. в конце ст.
69. **Калинкина, Т. И.** Телекоммуникационные и вычислительные сети. Архитектура, стандарты и технологии : учеб. пособие для студ. вузов, обуч. по напр. "Информатика и вычислительная техника" / Т. И. Калинкина, Б. В. Костров, В. Н. Ручкин. — СПб. : БХВ - Петербург, 2010. - 288 с. : ил. — (Учебные пособия). — Библиогр.: с. 281—283. (Шифр 004.7(075.8)/К 172-026893)

Экземпляры: всего:2 — УА(1), ЧЗТ(1)
70. **Каратунова, Н. Г.** Защита информации. Курс лекций [Электронный ресурс] : Учебное пособие / Н. Г. Каратунова. — Краснодар: КСЭИ, 2014. — Электрон. данные. — Режим

доступа: http://znanium.com/bookread2.php?book=503511; по паролю.

Учебное пособие по дисциплине «Защита информации» содержит курс лекций, предназначенных для бакалавров, направления подготовки: экономика, менеджмент, юриспруденция, сервис, туризм, а также для специальности пожарная безопасность.

71. **Карпов, В. В.** Разработка автоматизированных систем управления в защищенном исполнении / В. В. Карпов // Программные продукты и системы. — 2013. — **N 2.** — С. 3—5. — Библиогр. в конце ст.

Одним из основных научно-технических направлений деятельности научно-исследовательского института «Центрпрограммсистем» (г. Тверь) является разработка автоматизированных систем управления в защищенном исполнении. В данной статье подчеркивается актуальность этого направления работ, которая подтверждается, в частности, пристальным вниманием государства, выразившимся в разработке и принятии целого ряда документов, регламентирующих деятельность в области защиты информации, обосновывается выбор подхода к проектированию защищенных автоматизированных систем, заключающегося в создании многоуровневого комплекса средств защиты. Основой такой системы защиты должен быть аппаратно-программный комплекс уровня операционной системы, полностью базирующийся на отечественных проектных решениях. Разработанный в «Центрпрограммсистем» аппаратно-программный комплекс защиты информации от несанкционированного доступа «Ребус» позволил решить часть задачи – создать базис системы защиты, в планах на ближайшее будущее – создание технологии разработки защищенных автоматизированных систем.

72. **Кийко, М.** Угрозы национальной безопасности, их классификация и характеристики / М. Кийко // Проблемы теории и практики управления : междунар. журн. — 2013. — **N 2.** — С. 31—39 : рис. — Библиогр. в конце ст. (3).

Дается понятие национальной безопасности в современных условиях. Приводится классификация угроз, представляющих опасность для национальной безопасности России.

73. **Кнауб, Л. В.** Теоретико-численные методы в криптографии [Электронный ресурс] : Учеб. пособие / Л. В. Кнауб, Е. А. Новиков, Ю. А. Шитов.

— Красноярск : Сибирский федеральный университет, 2011. — Электрон. данные. — Режим доступа : http://znanium.com/bookread2.php?book=441493; по паролю.

Излагаются некоторые элементы теории чисел, отношения сравнимости, модулярная арифметика, степенные вычеты, первообразные корни, индексы, алгоритмы дискретного логарифмирования, китайская теорема об остатках, простые числа и проверка на простоту, разложение чисел на множители и арифметические операции над большими числами. В прил. 1 описаны основы теории групп, колец и полей, а в прил. 2 приведены реализации некоторых алгоритмов, даны тексты программ на языке Borland C++, снабженные подробными комментариями. Для студентов, обучающихся по специальности 090102 «Компьютерная безопасность» и направлениям подготовки 090900 «Информационная безопасность» и 010200 «Математика и компьютерные науки».

74. **Комаров, А. А.** Система управления инцидентами информационной безопасности / А. А. Комаров // Защита информации. Инсайд : информ. — метод. журн. — 2012. — **N 2.** — С. 64—67 : схема. — Библиогр. в конце ст.

Среди задач, стоящих перед любой системой управления информационной безопасностью (ИБ), можно выделить две наиболее значимые: предотвращение инцидентов и, в случае их наступления, своевременная и корректная ответная реакция. Несмотря на то что цель у обеих задач одна — минимизировать риски, связанные с инцидентами ИБ, — подходы к их реализации совершенно разные.

75. **Комашинский, Д. В.** Метод извлечения структурных признаков вредоносного программного обеспечения в задаче его обнаружения / Д. В. Комашинский, И. В. Котенко // Известия ВУЗов. Сер, Приборостроение. — 2012. — **Том 55, N 11.** — С. 58—63 : схема. — Библиогр. в конце ст.

Представлен метод извлечения из набора данных статических структурных признаков, развивающий ранее предложенный авторами подход к обнаружению вредоносных документов на основе применения методов машинного обучения. Метод базируется на использовании структурных особенностей элементов вредоносных документов и связей между ними.

76. **Коноплева, И. А.** Управление безопасностью и безопасность бизнеса : учеб. пособие для студ. вузов, обуч. по спец. "Приклад. информатика (по областям)" / И. А. Коноплева, И. А. Богданов. — М. : ИНФРА — М, 2014. — 447 с. : ил. — (Высшее образование). — Список сокр.: с. 431-432. — Глоссарий: с. 433—440. — Библиогр.: с. 441—443. (Шифр 65.290.4 я73/К 648-401521)

Экземпляры: всего:1 — ЧЗОН(1)

77. **Контроль утечек информации** в голосовом канале // Защита информации. Инсайд : информ.- метод. журн. — 2013. — **N 1.** — С. 40—41 : рис. — Библиогр. в конце ст.

Уникальные разработки, прототипы, «ноу-хау» — все это может стать мишенью конкурентной разведки, промышленного шпионажа и просто недобросовестной борьбы между участниками рынка, стремящимися любыми путями, порой неблаговидными, достичь своих целей. Нематериальные активы компаний приобретают все большую ценность для бизнеса, а их утечка за пределы организаций может привести к серьезным последствиям как репутационного, так и финансового характера.

78. **Копылов, А. И.** Программно-методический комплекс шифрования данных симметричным алгоритмом Rijndael в производственных системах [Текст] / А. И. Копылов, С. Н. Фисун // Автоматизація: проблеми, ідеї, рішення : матеріали міжнар. наук.-техн. конф. (Севастополь, 5-9 верес. 2011 р.) / М-во освіти і науки, молоді та спорту України, Севастоп. нац. техн. ун-т. — Севастополь, 2011. — С. 224—225. — Библиогр. в конце ст. (2). (Шифр в БД 658.52.011.56(06)/А 224-083070)

Было разработана программно-обучающая система, позволяющая шифровать данные алгоритмом Rijndael в пошаговом и автоматическом режимах. Данная программа может применяться как в задачах защиты информации в производственных системах, так и в образовательных целях.

79. **Королев, В. Ю.** Комбинаторная модель украинского ключа-аутентификатора и считывателя / В. Ю. Королев, В. В. Полиновский // Управляющие системы и машины: информационные технологии : междунар. науч. журн. — 2013. — **N 3.** — С. 61—67; 80 : рис., а-табл. — Библиогр. в конце ст.
80. **Котенко, И. В.** Интеллектуальные сервисы защиты информации в компьютерных системах и сетях / И. В. Котенко, И. Б. Саенко // Защита информации. Инсайд : информ. — метод. журн. — 2013. — **N 2.** — С. 32—41 : схема. — Библиогр. в конце ст.
81. **Котенко, И. В.** SIEM-системы для управления информацией и событиями безопасности / И. В. Котенко, И. Б. Саенко // Защита информации. Инсайд : информ.- метод. журн. — 2012. — **N 5.** — С. 54—65 : рис., s-схема. — Библиогр. в конце ст.

    Для успешной реализации мероприятий защиты информационных инфраструктур необходимо решение ряда задач, основная из которых связана с созданием системы мониторинга угроз безопасности. Системы мониторинга реализуют апостериорный подход к защите информации и основной целью своего создания имеют снижение воздействия на инфраструктурные объекты до минимального уровня риска и минимизацию возникающего ущерба. Одним из наиболее перспективных и эффективных направлений в создании систем мониторинга угроз безопасности в настоящее время считаются SIEM-системы, обеспечивающие управление информацией и событиями безопасности. Целью настоящей статьи является изложение основных взглядов на построение SIEM-систем и результатов, полученных авторами в рамках указанного проекта.
82. **Кошкина, Н. В.** Выявление в аудиосигналах скрытых сообщений, внедренных с помощью HIDE4PGP / Н. В. Кошкина // Проблемы управления и информатики : междунар. науч.-техн. журн. — 2013. — **N 3.** — С. 151—156 : граф., а-табл. — Библиогр. в конце ст.
83. **Кромин, Н.** Вопросы безопасности в управлении проектами внедрения АБС / Н. Кромин // Банковские технологии. — 2012. — **N 8.** — С. 69—75 : табл.
84. **Кромин, Н.** Вопросы безопасности в управлении проектами внедрения АБС / Н. Кромин // Банковские технологии. — 2012. — **N 8.** — С. 69—75 : табл.
85. **Крупнов, И. В.** Анализ проблем обеспечения информационной безопасности системы электронного голосования в условиях российского информационного пространства / И. В. Крупнов // Информационные технологии : Научно-технический и научно-производственный журнал. — 2012. — **N 4.** — С. 45—49 : рис. — Библиогр. в конце ст.

Представлен анализ проблем обеспечения информационной безопасности информационной системы Интернет-голосования (ОИСИГ), предназначенной для использования в реальных условиях Российской Федерации. Анализируются потенциально слабые звенья системы, предлагаются дополнительные механизмы повышения уровня надежности и защищенности ОИСИГ. Проводится анализ алгоритма контроля состояния голоса, поданного избирателем. По результатам анализа системы предлагаются пути ее модернизации, позволяющие существенно повысить защищенность системы без кардинального изменения используемой программно-аппаратной базы.

86. **Крупнов, И. В.** Анализ проблем обеспечения информационной безопасности системы электронного голосования в условиях российского информационного пространства / И. В. Крупнов // Информационные технологии : Научно-технический и научно-производственный журнал. — 2012. — **N 4.** — С. 45—49 : рис. — Библиогр. в конце ст.
87. **Кропачев, Л. А.** Основы теории информации : учебное пособие для студентов вузов специальностей "Комплексное обеспечение информационной безопасности автоматизированных систем", "Вычислительные машины, комплексы, системы и сети" и направления "Информатика и вычислительная техника" / Л. А. Кропачев. — Ижевск : Издательство Ижевского государственного технического университета, 2011. — 365, [1] с. : ил., табл. ; 21 см. — Библиография: с. 359—361. — Алфавитно-предметный указатель: с. 362—366.
(Шифр 621.391(075.8)/К 835-337054)
Экземпляры: всего:1 — ЧЗТ(1)
88. **Кудинов, Ю. И.** Практикум по основам современной информатики : учеб. пособие / Ю. И. Кудинов, Ф. Ф. Пащенко, А. Ю. Келина. — СПб. ; М. ; Краснодар : Лань, 2011. — 350 с. : ил., табл. — Библиогр.: с. 344.
(Шифр 004(075.8)/К 887-346705)
Экземпляры: всего:1 — ЧЗТ(1)
89. **Кузьминов, И.** Практическое использование DLP-системы DeviceLock в корпоративной среде банка. Взаимодействие и безопасность компонентов / И. Кузьминов // Банковские технологии. — 2012. — **N 3.** — С. 69—71.
Программный комплекс DeviceLock Endpoint DLP Suite разработки российской компании Смарт Лайн Инк предназначен для управления доступом пользователей ОС семейства Windows к периферийным устройствам хранения и обработки данных, каналам сетевых коммуникаций, а также для контроля действий пользователей с устройствами и сетевыми протоколами (чтение, запись файлов, форматирование) и контроля содержимого переданных файлов и данных. Возможности продукта и механизмы управления им описаны подробно на

сайте разработчика и в руководстве пользователя. Данный цикл статей посвящен описанию неочевидных нюансов, с которыми мы столкнулись в практике использования DeviceLock Endpoint DLP Suite в банковской корпоративной среде, и которые необходимо учитывать при развертывании и эксплуатации программы в достаточно большом домене. Вторая статья цикла описывает особенности сетевого взаимодействия компонентов и механизмы обеспечения собственной безопасности компонентов DeviceLock Endpoint DLP Suite.

90. **Ларин, Д. А.** Криптографическая деятельность в России от Полтавы до Бородина [Электронный ресурс] : Монография / Д. А. Ларин. — М.: РИОР: ИНФРА-М, 2015. — Электрон. данные. — Режим доступа : http://znanium.com/bookread2.php?book=479196; по паролю.

Монография посвящена истории российской криптографии в период от начала правления императора Петра I до окончании 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.

91. **Латчук, В.** Стратегия комплексного подхода к обеспечению информационной безопасности и защите информационных объектов образовательных учреждений / В. Латчук, С. // Основы безопасности жизнедеятельности : Информационно-методическое издание для преподавателей. - 2012. — **N 6**. — С. 14—17 : схема, а-фото. — Библиогр. в конце ст. (6).

Управление подсистемой информационной безопасности можно представить как совокупность совместной деятельности субъекта и объекта управления. направленной на защиту информационной собственности образовательного учреждения путем реализации управленческих функций, которые могут быть обеспечены только с учетом реализации основных методов предотвращения угроз информационной безопасности образовательного учреждения.

92. **Липаев, В. В.** Надежность и функциональная безопасность комплексов программ реального времени / В. В. Липаев // Программная инженерия : теорет. и приклад. науч.-техн. журн. — 2013. — **N 8**. — С. 10—18. — Библиогр. в конце ст.

Рассматриваются основные факторы, определяющие надежность и безопасное использование программных продуктов реального времени в составе автоматизированных систем. Анализируются характеристики таких систем и среды их функционирования, для которых должна обеспечиваться функциональная безопасность. Представлены требования к проектным решениям, обеспечивающим функциональную пригодность сложных программ. Обсуждаются вопросы организации и планирования жизненного цикла таких программ, в том числе процессы разработки требований к их безопасности. Выделены основные международные стандарты технологических процессов, которые поддерживают функциональную безопасность в жизненном цикле сложных комплексов программ. Значительное внимание уделено испытаниям систем на функциональную безопасность используемых в их составе программных продуктов.

93. **Лукьянчук, А. Г.** Обобщенная модель оценки защищенности цифровых систем передачи информации с отводными

каналами [Текст] / А. Г. Лукьянчук, А. И. Цопа, В. М. Шокало // Труды 12-й Международной научно-практической конференции "Современные информационные и электронные технологии", 23—27 мая, 2011 г., Украина, г. Одесса / М-во образования и науки Украины, Одес. нац. политехн. ун-т [и др.]. — Одесса, 2011. — С. 166. — Библиогр. в конце ст. (Шифр в БД 004(063)/С 568-814278)

94. **Маклаков, Г. Ю.** Коммуникационные технологии информационной безопасности человека [Текст] / Г.Ю. Маклаков // "Высшее образование в XXI веке: Информация- Коммуникация- Мультимедиа": Материалы 10-й юбилей. Междунар. науч.-метод. конф., Севастополь, 17—19 сент., 2003г. — Севастополь, 2003. —С. 219—222. — Библиогр. в конце ст.
95. **Маклаков, Г. Ю.** О некоторых принципах преподавания цикла компьютерных дисциплин на основе концепции информационной безопасности [Текст] / Г.Ю. Маклаков // Актуальные вопросы совершенствования подготовки конкурентоспособных специалистов в новых социально-экономических условиях: Материалы IX межд. науч.-метод. конф., 18—20 сент. 2002 г. — Севастополь : Изд-во СевГТУ, 2002. — С. 82—83. Библиогр. в конце ст.
Базовым элементом в решении различных задач является формирование новой информационной культуры у студентов и школьников. Понятие информационной культуры гораздо шире, чем только знание компьютерных технологий, она включает в себя умение адекватно оценивать новую информацию, разбираться в мирровоззренческих вопросах религии, философских течениях, грамотно организовывать информационное общение с др. людьми. Важно научить молодежь противостоять деструктивным внешним информационным воздействиям, умению сохранять общие культурно-этические ценности и совершенствовать свой духовно-моральный статус.
96. **Маклаков, Г. Ю.** Коммуникационные технологии и информационная безопасность человека [Текст] / Г. Ю. Маклаков // Высшее образование в XXI веке: Информация. Коммуникация. Мультимедиа, Материалы 10-й юбилей. междунар. науч.-метод. конф., 17—19 сент., 2003 г. — Севастополь : Изд-во СевНТУ, 2003. — С. 219—222. — Библиогр. в конце ст.
97. **Маригодов, В. К.** Защита учебной информации в системах дистанционного обучения / В. К. Маригодов // Вісник СевНТУ : зб. наук. пр. / Севастоп. нац. техн. ун-т. — Севастополь : Вид-

во Севастоп. нац. техн. ун-ту, 2012. — Вип. 127: Педагогіка. — С. 68—71 : рис. — Библиогр. в конце ст.(9); То же [Электронный ресурс]. — Электрон. данные. — Режим доступа : http://sevntu.com.ua/jspui/handle/123456789/5355 (Шифр в БД 06/С 28-171737)
Рассматриваются методы защиты учебной информации в системах дистанционного обучения. Проведен сравнительный анализ эффективности методов и рассмотрена целесообразность их практического использования.

98. **Марков, А. С.** Систематика уязвимостей и дефектов безопасности программных ресурсов / А. С. Марков, А. А. Фадин // Защита информации. Инсайд : информ.- метод. журн. — 2013. — **N 3.** — С. 56—61 : табл., s-схема. — Библиогр. в конце ст.
99. **Маслов, О. Н.** Защита акустической информации: резервы системного подхода / О. Н. Маслов, В. Ф. Шашенков // Защита информации. Инсайд : информ. — метод. журн. — 2013. — **N 1.** — С. 30—35 : схема, а-фото, а-граф. — Библиогр. в конце ст.
Системный подход к разработке комплексов оборудования для активной защиты (далее — систем активной защиты, САЗ) конфиденциальной информации (КИ) имеет в виду ряд особенностей.
100. **Маслов, О. Н.** О моделировании риска принятия решений в области обеспечения информационной безопасности / О. Н. Маслов // Защита информации. Инсайд : информ. - метод. журн. — 2011. — **N 4.** — С. 16—20 : табл., схема, граф. ; **N 5.** — С. 12—15 : табл. — Библиогр. в конце ст. (14). В статье рассматриваются пути моделирования и прогнозирования количественных характеристик риска, связанного с защитой конфиденциальной информации на объектах различного назначения.
101. **Матвеев, В. А.** Сравнение различных технологий сетей передачи данных ограниченных пользователей в аспекте обеспечения ИБ от угроз несанкционированного доступа / В. А. Матвеев, Р. А. Бельфер // Электросвязь : науч.-техн. журн. по проводной радиосвязи, телевидению и радиовещанию. — 2013. — **N 7.** — С. 6—9 : рис. — Библиогр. в конце ст. (14). Предложен математический аппарат для сравнительного анализа защищенности от рассматриваемых угроз несанкционированного доступа в технологических и других сетях передачи данных с высокими требованиями информационной безопасности. Приведен пример сравнения семи технологий при использовании этого метода.
102. **Мельников, В. П.** Информационное обеспечение систем управления : учебник для студентов высших учебных заведений, обучающихся по направлению подготовки

"Автоматизированные технологии и производства" / В. П. Мельников. — Москва : Академия, 2010. — 335, [1] с. : ил ; 22 см. — (Высшее профессиональное образование. Автоматизация и управление). — (Учебник). — Библиография: с. 331—333.
(Шифр 004.65(075.8)/М 482-795203)
Экземпляры: всего:3 — ЧЗТ(1), УА(2)

103. **Менгазетдинов, Н. Э.** Новые кибернетические угрозы и методы обеспечения кибербезопасности в цифровых системах управления / Н. Э. Менгазетдинов, А. Г. Полетыкин, В. Г. Промыслов // Энергетик : произв.-массов. журн. — 2012. — **N 7.** — С. 18—23 : схема. — Библиогр. в конце ст. (4).
Рассмотрена задача обеспечения кибербезопасности цифровых систем управлении (ЦСУ), выделены её основные аспекты, указаны отличительные особенности по сравнению с обычными информационными системами. Выполнен анализ применения экспертной системы для оценки кибербезопасности ЦСУ на этапе эксплуатации.

104. **Методика построения модели** безопасности автоматизированных систем / В. Г. Жуков [и др.] // Программные продукты и системы. — 2012. — **N 2.** — С. 70—74 : схема. — Библиогр. в конце ст.

105. **Методика построения модели** безопасности автоматизированных систем / В. Г. Жуков [и др.] // Программные продукты и системы. — 2012. — **N 2.** — С. 70—74 : схема. — Библиогр. в конце ст.

106. **Методические указания к** выполнению контрольной работы по дисциплине "Криптография и **защит**а данных" для магистров заочной формы обучения направления 09.04.01 "Информатика и вычислительная техника" [Текст] / составитель М. А. Лебедева. — Севастополь : Издательство Севастопольского государственного университета, 2015. — 23 с. : ил., табл. — Библиография: с. 20.

107. **Методические указания** к выполнению контрольной работы по дисциплине "Радиоэлектронные системы защиты объектов и информации" для студентов заочной формы обучения специальности 7.090701 — "Радиотехника" [Текст] / СевНТУ ; Сост. И. В. Лащенко. — Севастополь : Изд-во СевНТУ, 2007. — 20 с.

108. **Методические указания к** выполнению лабораторных работ по дисциплине "**Защит**а **информац**ии в компьютерных

системах" для студентов специальности 7.05010201 "Компьютерные системы и сети" всех форм обучения [Текст] / составители: Л. И. Новикова, М. А. Лебедева, А. О. Смагина. — Севастополь : Издательство Севастопольского национального технического университета, 2013. — 30 с. : ил., табл. — Библиография: с. 30.

109. **Моисеев, В. С.** Вероятностная динамическая модель функционирования программных средств активной защиты мобильных распределенных АСУ / В. С. Моисеев, П. И. Тутубалин // Информационные технологии : науч.-техн. и науч.-произв. журн. — 2013. — **N 6.** — С. 37—42 : граф., а-табл. — Библиогр. в конце ст. Предлагается состав функций (задач) средств активной защиты информационных систем. Для описания процесса реализации этих функций во времени разработана марковская модель работы программного обеспечения таких средств применительно к мобильным распределенным АСУ, имеющим ограниченное время функционирования на каждом месте их дислокации. Предложены методы расчета вероятностно-временных характеристик функционирования каждого комплекса программ, решающих задачи активной защиты системы. Приводится пример моделирования и расчета характеристик предложенных программных средств.

110. **Монахов, М. Ю.** Инвентаризация информационных ресурсов как основа безопасного функционирования АСУ / М. Ю. Монахов, О. И. Файман // Известия ВУЗов. Сер, Приборостроение. — 2012. — **Том 55, N 8.** — С. 35—39 : табл. — Библиогр. в конце ст.

Приведен перечень информационных ресурсов автоматизированных систем управления (АСУ) на основе степени их вовлеченности в протекающие на предприятии бизнес-процессы. Определены критичные для безопасного функционирования АСУ характеристики информационных ресурсов. Предложена методика инвентаризации информационных ресурсов, проанализированы особенности ее применения.

111. **Морозов, А. М.** Анализ уязвимостей сети SIP к угрозам фрода / А. М. Морозов // Электросвязь : науч.-техн. журн. по проводной радиосвязи, телевидению и радиовещанию. — 2013. — **N 7.** — С. 10—13 : рис. — Библиогр. в конце ст. (4).

В работе приводится анализ риска информационной безопасности (ИБ) при реализации некоторых из угроз фрода. Разработаны соответствующие алгоритмы атак злоумышленника и предложены способы защиты от них. Результаты получены с помощью тестирования, проведенного на стенде оборудования одного из российских операторов связи.

112. **Морозов, А. М.** Анализ уязвимостей сети voip на базе ngn к угрозам нелегитимных сигнальных и медиасообщений / А. М. Морозов // Электросвязь : науч.-техн. журн. по проводной радиосвязи, телевидению и радиовещанию. — 2013. — **N 4.** — С. 33—35 : обр. — Библиогр. в конце ст.

113. **Мукминов, В. А.** Методика оценки реального уровня

защищенности автоматизированных систем / В. А. Мукминов, В. М. Хуцишвили, А. В. Лобузько // Программные продукты и системы. — 2012. — **N 1.** — С. 39—42 : табл. — Библиогр. в конце ст.

Рассмотрена методика оценки уровня защищенности АСУ в условиях моделирования компьютерных атак. Приведен перечень инструментальных средств, используемых для проведения оценки, включая средства моделирования компьютерных атак. Предложено комплексное использование новых форм испытаний и тестирования программных средств АСУ на основе натурного и имитационного моделирования. Применение новой методики оценки реального уровня защищенности позволит повысить эффективность работы служб информационной безопасности при эксплуатации АСУ.

114. **Наукоемкие** технологии в инфокоммуникациях: обработка и защита информации : коллективная монография / ред.: В. М. Безрук, В. В. Баранник. — Харьков : СМИТ, 2013.— 396, [1] с. ; 21 см. — Библиография в конце разделов.

(Шифр 621.39/Н 34-420642)

Экземпляры: всего:1 — ОКХ(1)

Коллективная монография содержит материалы по актуальным направлениям инфокоммуникационных технологий. Излагаются направления развития таких важных областей как планирование инфокоммуникационных сетей, повышение качества предоставляемых услуг, обработка и защита информации, в том числе, вопросы обеспечения эффективного хранения, обработки, сжатия и безопасности информации, управления инфокоммуникационными сетями с использованием методов прогнозирования временных рядов, принятия оптимальных решений, распознавания образов, распределенной обработки информации и облачных вычислений.

115. **Новикова, Л. И.** Односторонние функции в криптографии с открытыми ключами [Текст] / Л. И. Новикова // Информационные технологии и информационная безопасность в науке, технике и образовании "ИНФОТЕХ-2009" : материалы конф. / Севастоп. нац. техн. ун-т, С.-Петерб. гос. ун-т аэрокосм. приборостроения, Ин-т проблем информатики, Люблин. техн. ун-т. — Севастополь : Изд-во Севастоп. нац. техн. ун-та, 2009. — С. 256—258. — Библиогр. в конце ст.(2).

(Шифр в БД 004(06)/И 741-994438)

116. **Новикова, Е. С.** Проектирование компонента визуализации для автоматизированной системы управления информационной безопасностью / Е. С. Новикова, И. В. Котенко // Информационные технологии : науч.-техн. и науч.-произв. журн. — 2013. — **N 9.** — С. 32—36 : схемы. — Библиогр. в конце ст.

Представлены результаты проектирования подсистемы визуализации автоматизированной системы управления информационной безопасностью. Исследованы механизмы визуализации

в современных системах управления информационной безопасностью. Описана архитектура подсистемы визуализации, позволяющая расширять графический функционал системы и использовать различные технологии для реализации графических элементов. Приведено описание реализации системы, иллюстрирующее предложенный подход.

117. **Новожилов О. П.** Информатика : учебник для прикладного бакалавриата : учебное пособие для студентов высших учебных заведений, обучающихся по специальностям групп "Экономика и управление" и направлению "Информатика и вычислительная техника" / О. П. Новожилов. — 3-е издание, переработанное и дополненное. — Москва : Юрайт, 2014. — 619 с. : ил., табл. ; 21 см. — (Бакалавр. Прикладной курс). — Список сокращений: с. 9. — Предметный указатель: с. 606—617. — Библиография: с. 618—619 (32 назв.).
(Шифр 004(075)/Н 741-495828)
Экземпляры: всего:1 — ЧЗТ(1)

118. **Операционные системы** : Учебно-метод. пособие для студентов очной и заочной формы обучения / Р. В. Лазуренко [и др.]. — Севастополь : СНУЯЭиП, 2014. — 176 с. : ил. — Библиогр.: с. 173.
Экземпляры: всего:40 — ЧЗ(2), ХР(4), УФ(34) библ-ки ИЯЭиП
В пособии рассматриваются архитектура и ресурсы операционной системы, основные концепции эволюции разновидности операционных и систем.

119. **Оптимизация процессов защиты** информации с позиций виртуализации относительно условий теоретической недешифруемости / В. В. Котенко [и др.] // Прикладная радиоэлектроника. — 2013. — **N 2.** — С. 265—271 : рис. — Библиогр. в конце ст.
Приводится фундаментальное решение задачи оптимизации процессов защиты информации с позиций виртуализации относительно условий теоретической недешифруемости. Применение предложенного подхода открывает принципиально новую область возможностей для комплексного решения проблем повышения стойкости защиты информации.

120. **Партыка Т. Л.** Информационная безопасность : учеб. пособие для студ. учреждений сред. проф. образования, обуч. по спец. информатики и вычисл. техники / Т. Л. Партыка, И. И. Попов. — 5-е изд., перераб. и доп. — М. : Форум, 2014. — 431 с. : ил. — (Профессиональное образование). — Библиогр.: с. 406—407 (32 назв.). — Глоссарий: с. 408—429.
(Шифр 004.7.056.5(075.8/П 187-179659)
Экземпляры: всего:1 — ЧЗТ(1)

121. **Партыка, Т. Л.** Информационная безопасность [Электронный ресурс] : Учебное пособие / Т. Л. Партыка, И. И. Попов. — 5-е изд., перераб. и доп. — М.: Форум; ИНФРА-М, 2014. — Электрон. данные. — Режим доступа : http://znanium.com/bookread2.php?book=516806; по паролю.
Рассмотрены вопросы информационной безопасности и защиты данных, в том числе в информационно-вычислительных системах и сетях. Дано введение в общие проблемы безопасности, определены роль и место информационной безопасности в системе обеспечения национальной безопасности государства. Рассмотрены проблемы защиты информации в автоматизированных системах обработки данных, криптографические методы защиты информации, вопросы защиты информации в персональных компьютерах, компьютерные вирусы и антивирусные программы, а также проблемы защиты информации в сетях ЭВМ и организации комплексных систем технического обеспечения безопасности. Для учащихся техникумов, колледжей, а также студентов вузов.

122. **Перегуда, А. И.** Математическая модель надежности информационных систем с эшелонированной защитой от несанкционированного доступа / А. И. Перегуда, Д. А. Тимашов // Информационные технологии : науч.-техн. и науч.-произв. журн. — 2012. — N 12. — С. 61—66. — Библиогр. в конце ст.
Рассмотрена математическая модель надежности информационной системы систем защиты информации, состоящей из объекта защиты информации и двух систем безопасности. Процесс функционирования изучаемой системы защиты информации описывается как наложение альтернирующих процессов восстановления. Получены верхняя и нижняя оценки для математического ожидания времени до осуществления несанкционированного доступа к информации.

123. **Пескова, С. А.** Сети и телекоммуникации : Учебник для студентов высших учебных заведений, обучающихся по направлению подготовки 230100 "Информатика и вычислительная техника" (квалификации "бакалавр") / С. А. Пескова, А. В. Кузин. — 5-е издание, переработанное. — Москва : Академия, 2014. — 313, [1] с. : рис., табл. ; 21 см. — (Высшее образование. Бакалавриат. Информатика и вычислительная техника). — Список сокращений: с.302—303. — Библиография: с. 304—306. — Предметный указатель: с. 307—310.
(Шифр 004.7(075.8)/П 281-375812)
Экземпляры: всего:1 — ЧЗТ(1)

124. **Полянская, О. Ю.** Инфраструктуры открытых ключей [Текст] : учеб. пособие / О. Ю. Полянская, В. С. Горбатов. — М. : ИНТУИТ : БИНОМ. ЛЗ, 2007. — 368 с. : ил., табл. —

(Основы информационных технологий). — Библиогр.: с. 358—367 (220 назв.).

125. **Пономарева, О. А.** Применение стоимостной оценки рисков для определения требуемой степени обеспечения **безопасности информационных** технологий [Текст] / О. А. Пономарева, Н. А. Каин // 25-я Международная Крымская конференция "СВЧ-техника и телекоммуникационные технологии", 6—12 сентября 2015 г., Севастополь, Крым, Россия : КрыМиКо 2015 : материалы конф. : в 2 т. — Севастополь, 2015. — **Т. 1**, **секц. 3а/5** : Обработка и защита информации. — С. 365—366. — Библиогр. в конце ст. (3). (Шифр в БД 621.396.6.029.64/С 255-583772222)

126. **Права Интернет-пользователей: Россия** и мир, теория и практика : аналитический доклад / подгот.: И. Левов, Г. Шуклин, Д. Винник // Інтелектуальна власність. — 2013. — **№ 7**. — С. 15—23 ; **№ 8**. — С. 8—16 ; **№ 9**. — С. 10—16.

127. **Правовое регулирование деятельности** в информационной безопасности : Учебно-метод. пособие. Ч. 2 / Е. В. Куликова [и др.]. — Севастополь : СНУЯЭиП, 2011. — 128 с : рис. — Библиогр.: с. 126—128.

Экземпляры: всего:74 — ЧЗ(3), ХР(3), УФ(68) библ-ки ИЯЭиП

В пособии представлен теоретический материал для подготовки к лекционным и практическим занятиям по дисциплине.

128. **Программные комплексы серии** „Аура“ для защиты информационных систем персональных данных / А. А. Костин [и др.] // Известия ВУЗов. Сер, Приборостроение. — 2012. — **Том 55**, **N 11**. — С. 67—72. — Библиогр. в конце ст.

Рассматриваются возможности программных комплексов серии „Аура“ для защиты информационных систем персональных данных в соответствии с требованиями Федерального закона № 152-ФЗ „О персональных данных“.

129. **Радиотехника** : всеукр. межведомств. науч-техн. сб. / М-во образования и науки Украины, Харьк. нац. ун-т радиоэлектроники; ред. В. М. Шокало. — Харків : Вид-во Харк. нац. ун-ту радіоелектрон. — 1965.

**Вып. 165** : К 65-летию кафедры радиотехники : темат. вып. — 2011. — 290 с. : ил. — Библиогр. в конце ст.

(Шифр 621.37/Р 154-106304)

130. **Вып. 166** : Информационная безопасность : темат. вып. — 2011. — 292 с. : ил.

(Шифр 621.37/Р 154-381916)

131. **Вып. 169**. — 2012. — 388 с. : ил. — Библиогр. в конце ст.
(Шифр 621.37/Р 154-210941)

132. **Вып. 171** : Информационная безопасность : темат. вып. — 2012. — 400 с. : ил. — Библиогр. в конце ст.
(Шифр 621.37/Р 154-964474)

133. **Вып. 173**. — 2013. — 248 с. : ил. — Библиогр. в конце ст.
(Шифр 621.37/Р 154-018880)
Экземпляры: всего:1 — ОКХ(1)
Представлены работы ученых университета по проблемам радиотехники.

134. "**Радиоэлектроника и молодежь в XXI веке", Международный молодежный форум (16 ; 2012 ; Харьков).** Материалы 16-го Международного молодежного форума "Радиоэлектроника и молодежь в XXI веке", 17—19 апреля 2012 года. — Харьков : Издательство Харьковского национального университета радиоэлектроники. — 2012
**Т. 3** : Международная конференция "Современные проблемы радиотехники". — 2012. — 218 с. : ил. ; 20 см). — Алфавитный список: с. 216—217.
(Шифр 621.37/.39/Р 154-131206)
Экземпляры: всего:1 — ОКХ(1)

135. **Рембовский, А. М.** Радиомониторинг: задачи, методы, средства / А. М. Рембовский, А. В. Ашихмин, В. А. Козьмин ; ред. А. М. Рембовский. — 2-е изд., перераб. и доп. — М. : Горячая линия — Телеком, 2010. — 624 с. : ил. — Библиогр.: с. 606—619.
(Шифр 621.396.92/Р 371-150063)
Экземпляры: всего:1 — ОКХ(1)

136. **Рожнев, А.Ю.** Повышение надежности систем передачи информации на основе теории запретов булевых функций / А. Ю. Рожнев // Изв. ВУЗов. Сер. Приборостроение. — 2013. — Т. 56, № 1. — С. 13—18. — Библиогр. в конце ст.
Предложена схема повышения надежности систем передачи информации, построенная с использованием алгоритма шифрования повышенной стойкости.

137. **Сабанов, А. Г.** Аутентификация как составляющая

единого пространства доверия / А. Г. Сабанов // Электросвязь : науч.-техн. журн. по провод. радиосвязи, телевидению и радиовещанию. — 2012. — **N 8.** — С. 40—44. - Библиогр. в конце ст.

138. **Сабанов, А. Г.** Об оценке рисков удаленной аутентификации как процесса / А. Г. Сабанов // Электросвязь : науч.-техн. журн. по проводной радиосвязи, телевидению и радиовещанию. — 2013. — **N 4.** — С. 27—32 : рис., а-табл. — Библиогр. в конце ст.

139. **Сапожников, Н. Е.** Защита информации в компьютерных системах : Метод. указания к выполнению практических занятий для специальности СКС / Н. Е. Сапожников, Ю. Ю. Столярчук, А. В. Лавров. — Севастополь : СНУЯЭиП, 2012. — 140 с : рис. — Библиогр.: с. 137. Целью методических указаний является помощи студентам в подготовке к выполнению практических занятий по дисциплине "защита информации в информационных системах".

Экземпляры: всего:92 — ЧЗ(2), ХР(4), УФ(86) библ-ки ИЯЭиП

140. **Сапожников, Н. Е.** Информационные технологии и системы в экономике : Учеб. пособие / Н. Е. Сапожников. — Севастополь, 2011. — (Севастопольский филиал Саратовского госуд. социально-экономического ун-та). — Библиогр.: с. 278—281

Экземпляры: всего:1 — ЧЗ(1) библ-ки ИЯЭиП

Обработана и систематизирована информация, позволяющая изучать теоретические основы современных информационных технологий, математическое программное и аппаратное обеспечение современных информационных систем.

141. **Севастопольский национальный технический университет.** Адаптивная система **безопасност**и передачи данных в динамических беспроводных сетях [Текст] : отчет о НИР : "Барьер" : (заключ.) / М-во образования и науки Украины, Севастоп. нац. техн. ун-т ; начальник нис В. П. Поливцев ; рук. нир А. В. Скатков. — 2010. — 145 л. : ил. + 1 эл. опт. диск. — Библиогр.: с. 114—116. — Б. ц. — № ГР 0109U001705. — Инв.№ 0211Г0011603. Рукоп. закончена 01.12.2010 г.

142. **Сидоров, В. Д.** Аппаратное обеспечение ЭВМ : учеб. для нач. проф. образования / В. Д. Сидоров, Н. В. Струмпэ. — 2-е изд., стер. — М. : Академия, 2012. — 336 с. : ил. — (Начальное профессиональное образование. Информатика). —

Глоссарий: с. 320—332. — Библиогр.: с. 333.
(Шифр 004.3(075)/С 347-761921)
Экземпляры: всего:5 — УА(4), ЧЗТ(1)

143. **Семёнов, Д. В.** Метод оценки рисков нарушения информационной безопасности банковских учреждений / Д. В. Семёнов, Ф. Л. Демченко // Прикладная радиоэлектроника : Научно-техн. журнал. — 2012. — **Том 11, N 2.** — С. 304—308 : табл., а-рис. — Библиогр. в конце ст.

Предлагается метод оценки рисков нарушения информационной безопасности на основе опроса кадрового состава предприятия по трем направлениям: текущий уровень информационной безопасности организации; оценка системы управления информационной безопасностью организации; оценка уровня осознания руководством необходимости обеспечения информационной безопасности организации.

144. **Скатков, А. В.** Информационные технологии критериального обнаружения атак в телекоммуникационных сетях критического применения [Текст] / А. В. Скатков, В. С. Ловягин, С. А. Черномыз // Современные проблемы прикладной математики, информатики, автоматизации и управления : материалы 3-го междунар. науч.-техн. семинара, 9—13 сент. 2013 г., Севастополь / М-во образования и науки, молодежи и спорта Украины, Севастоп. нац. техн. ун-т, Рос. акад. наук, Ин-т пробл. информатики. — М., 2013. — С. 41—53 : рис. — Библиогр. в конце ст. (2).
(Шифр в БД 519.1(063)/С 568-133767)

145. **Слободенюк, Д.** Средства защиты информации в банковских системах / Д. Слободенюк // Банковские технологии : науч.-техн. журн. — 2013. — **N 2.** — С. 48—49.

146. **Снегуров, А. В.** Подход к выбору метрики маршрутизации в беспроводных телекоммуникационных сетях специального назначения в условиях действия средств радиоэлектронной разведки [Текст] / А. В. Снегуров, В. Х. Чакрян, А. А. Мамедов // 23-я Международная Крымская конференция "СВЧ-техника и телекоммуникационные технологии" (КрыМиКо 2013), 8—13 сентября, 2013 г. Севастополь, Крым, Украина : материалы конф. : в 2 т. — Севастополь, 2013. — **Т. 1, Секция 3а/5** : Управление и адаптация в беспроводных сетях. — С. 470—471 : рис. — Библиогр. в конце ст. (3).
(Шифр в БД 621.396.6.029.64/С 255-504319

147. **Сокращение риска несанкционированного** доступа к информационным ресурсам / подгот. специалистами компании "Индид" // Защита информации. Инсайд : информ.- метод. журн. — 2012. — **N 4**. — С. 67—71 : табл. — Библиогр. в конце ст.

Деятельность современного банка во многом сводится к управлению финансовой информацией: движение денег и обязательств на счетах, расчеты между кредитными организациями, торговля на валютном и других финансовых рынках. Эта финансовая информация создается, хранится, изменяется и контролируется со все более нарастающим участием информационных систем.

148. **Сорокин, К.** Биометрическая аутентификация пользователей — эффективный инструмент минимизации инсайдерских рисков / К. Сорокин // Банковские технологии. — 2012. — **N 4**. — С. 68—69. — Библиогр. в конце ст.

149. **Стельмах, А. П.** Кибернетическая безопасность: понятие и сущность феномена / А. П. Стельмах, А. В. Тонконогов // Социально-гуманитарные знания : науч.-образоват. изд. - 2013. — **N 2**. — С. 103—115. — Библиогр.: с. 103—115 (7).

В статье раскрыта сущность и предложена авторская научная дефиниция феномена «кибернетическая безопасность»; выявлены внутренние и внешние угрозы в данной сфере общественных отношений; определены основные направления государственной политики Российской Федерации по обеспечению кибернетической безопасности.

150. **Стратегия защиты непрерывной** информации с позиций виртуализации ансамбля ключей на формальные отношения ансамблей / В. В. Котенко [и др.] // Прикладная радиоэлектроника. — 2013. — **N 2**. — С. 308—312 : табл. — Библиогр. в конце ст.

Приводится фундаментальное обоснование стратегии защиты непрерывной информации с позиций виртуализации ансамбля ключей на формальные отношения ансамблей. Устанавливается, что применение стратегии впервые открывает возможность трехуровневой защиты непрерывной информации. Оценка эффективности защиты от криптоанализа на первом (начальном) уровне защиты показывает потенциальную возможность выполнения условий абсолютной недешифруемости путем соответствующего увеличения дисперсии ансамбля виртуальных ключей.

151. **Струков, А. В.** Разработка криптографического примитива с использованием теории хаоса / А. В. Струков // Радиотехника XXI век : науч.-техн. журн. — 2013. — **N 4**. — С. 58—64 : схема, а-табл. — Библиогр. в конце ст.

Представлены иерархия и наследственность методов в подсистеме защиты информации. Обоснован выбор функциональной схемы генератора хаоса, являющегося конструктивного элемента генератора случайных чисел с аппаратным формирование начальных условий. Разработана модель генератора случайных чисел с аппаратным формированием начальных условий.

152. **Стюгин, М. А.** Способ построения защищенных от исследования систем информационной безопасности / М. А. Стюгин // Программные продукты и системы. — 2013. — **N 3.** — С. 219—223. — Библиогр. в конце ст.

В статье обозначена проблема исследования в конфликтных системах. Рассмотрены методы противодействия процессу конфликте, включающая информационные ограничения при попытке исследовать объект конфликта. Представлены четыре класса, в которых может находиться исследователь с учетом его информационных ограничений. Приведен алгоритм проектирования защищенных от исследования информационных систем. Предполагается, что наиболее эффективно данный алгоритм можно применить на стадии разработки программных продуктов в области информационной безопасности. С использованием предложенных алгоритмов уже были разработаны системы анализа несанкционированных действий пользователей на интернет-ресурсах и в локальной сети предприятия (программы ReflexionWeb и ExLook).

153. **Стюгин, М. А.** Функциональное сопоставление сложных систем информационной безопасности / М. А. Стюгин // Программные продукты и системы : науч.- практ. изд. — 2013. — N 1. — С. 42—47 : рис., s-схема. — Библиогр. в конце ст.

154. **Тельный, А. В.** Об организации информационной распределенной среды интегрированных систем охраны и безопасности / А. В. Тельный, О. Р. Никитин, И. В. Храпов // Известия ВУЗов. Сер. Приборостроение. — 2012. — **Том 55, N 8.** — С. 28—32. — Библиогр. в конце ст.

Представлены критерии оценки и способы организации информационного обмена в распределенной информационной среде интегрированных систем охраны и безопасности различных производителей.

155. **Тепляков, И. М.** Телекоммуникационные системы : сб. задач : учеб. пособие для студ. вузов, обуч. по напр. подгот. дипломир. специалистов "Телекоммуникации" / И. М. Тепляков. — М. : РадиоСофт, 2011. — 240 с. : ил. (Шифр 621.39(075.8)/Т 345-147640)

Экземпляры: всего:2 — УА(1), ЧЗТ(1)

156. **Техническая защита информации** на объектах информационной деятельности : Учеб.-метод. пособие . В 2-х частях : Ч. 1 / А. А. Пименов [и др.]. — Севастополь : СНУЯЭиП, 2011. — 88 с. — Библиогр.: с. 88.

Экземпляры: всего:68 — ЧЗ(3), ХР(5), УФ(60) библ-ки ИЯЭиП

В пособии представлен теоретический материал для подготовки к лекционным и практическим занятиям по дисциплине.

157. **Техническая защита информации** на объектах информационной деятельности : Учебно-метод. пособие. В 2-х.

ч. : Ч. 2. — Севастополь : СНУЯЭиП, 2011. — 84 с. — Библиогр.: с. 83.

Экземпляры: всего:68 — ЧЗ(3), ХР(5), УФ(60) библ-ки ИЯЭиП

В пособии представлен теоретический материал для подготовки к лекционным и практическим занятиям по дисциплине.

158. **Тонконогов, А. В.** "Киберология" как научная дисциплина / А. В. Тонконогов // Социально-гуманитарные знания : науч.- образоват. изд. — 2013. — **N 1**. — С. 85—96. — Библиогр.: с. 87—96 (4). В статье обосновывается необходимость формирования новой научной дисциплины "Киберология", которая должна изучать проблемы эволюции "кибернетического пространства", обеспечения "кибернетической безопасности", формирования "кибернетического сознания".

159. **Трошина, С. М.** Особенности расследования инцидентов **информационн**ой **безопасност**и в телекоммуникационной сфере [Текст] / С. М. Трошина // 25-я Международная Крымская конференция "СВЧ-техника и телекоммуникационные технологии", 6—12 сентября 2015 г., Севастополь, Крым, Россия : Крымико 2015 : материалы конф. : в 2 т. - Севастополь, 2015. — **Т. 1**, **секц. Н/2** : История и методология науки и техники (VII Федотовские чтения). — С. 69—70. — Библиогр. в конце ст. (4). (Шифр в БД 621.396.6.029.64/С 255-583772222)

160. **Уязвимость спутниковых технологий** / А. В. Мишуров [и др.] // Прикладная радиоэлектроника. — 2013. — **Т. 12**, **N 3**. — С. 471—473 : портр. — Библиогр. в конце ст. в статье рассмотрены возможные варианты уязвимости спутниковых технологий на современном уровне развития техники в результате действий злоумышленников. Обращается внимание на возможный международный характер деструктивной деятельности, способной нарушить работу спутниковых систем, вплоть до потери космического аппарата. Проводится анализ технической деятельности злоумышленников и рассматриваются методы противодействия.

161. **Фаль, А. М.** Стандартизация в сфере менеджмента информационной безопасности / А. М. Фаль // Кибернетика и системный анализ. — 2010. — **№3**. — С. 181—184. — Библиогр. в конце ст. В работе описаны асимметричные криптографические алгоритмы, которые используются в современных системах электронного документооборота; отмечена также важность разработки и внедрения стандартов, относящихся к защите информации.

162. **Фисун, С. Н.** Аутентификация и авторизация в приложениях ASP.NET / С. Н. Фисун, А. И. Копылов // Вісник СевНТУ : зб. наук. пр. / Севастоп. нац. техн. ун-т; ред. Є. В. Пашков. — Севастополь : Вид-во Севастоп. нац. техн. ун-ту,

2012. — Вип. 131: Інформатика, електроніка, зв'язок. — С. 73—77 : рис. — Библиогр. в конце ст.(3); То же [Электронный ресурс]. — Электрон. текстовые документы. — Режим доступа : http://sevntu.com.ua/jspui/handle/123456789/5598 (Шифр в БД 06/С 28-192307)Рассматриваются способы обеспечения безопасности в Web-приложениях ASP.NET. Основное внимание уделено провайдерам аутентификации и авторизации платформы ASP.NET. С использованием этих провайдеров на языке программирования C# было разработано Web- приложение, которое реализует процесс регистрации и входа пользователей на Web-страницу**.**

163. **Фисун, С. Н.** Использование криптографических сервисов .NET и JAVA для защиты информации от несанкционированного доступа / С. Н. Фисун, А. И. Копылов // Вісник СевНТУ : зб. наук. пр. / Севастоп. нац. техн. ун-т; ред. Є. В. Пашков. — Севастополь : Вид-во Севастоп. нац. техн. ун-ту, 2011. — **Вип. 114**: Інформатика, електроніка, зв'язок. — С. 81—86 : рис. — Библиогр. в конце ст.(5); То же [Электронный ресурс]. — Электрон. текстовые данные. — Режим доступа : http://sevntu.com.ua/jspui/handle/123456789/3335 (Шифр в БД 06/С 28-865182) Рассматриваются возможности криптографических сервисов, предоставляемых платформами .NET и JAVA. Данные сервисы можно рассматривать, как альтернативу интерфейсу CryptoAPI Microsoft, который подробно рассматривается в статье [1]. Они позволяют использовать различные криптографические алгоритмы для шифрования данных. С использованием этих алгоритмов на языках программирования JAVA и C++ была разработана программа шифрования и скрытия зашифрованной информации в файле.

164. **Фисун, С. Н.** Сравнительный анализ методов шифрования информации в компьютерных системах / С. Н. Фисун, Т. А. Абрамов, А. И. Копылов // Інформаційні технології та інформаційна безпека в науці, техніці та навчанні "ІНФОТЕХ-2011" : матеріали міжнар. наук.-практ. конф., м. Севастополь, 5—10 верес. 2011 р. / М-во освіти і науки, молоді та спорту України, Севастоп. нац. техн. ун-т. — Севастополь, 2011. — С. 165—166 : табл. — Библиогр. в конце ст.(2). (Шифр в БД 004(06)/И 741-517245) Рассматривается сравнительный анализ симметричных длочных алгоритмов шифрования на примере алгоритмов DES, 3DES, AES. В качестве основных критериев оценки выступают два параметра: скорость шифрования информации и криптостойкость используемого шифра. Для оценки скорости шифрования авторами доклада было разработано необходимое программное обеспечение на языках программирования Java, C#. При оценке криптостойкости шифра в первую очередь учитывалась устойчивость рассматриваемых алгоритмов шифрования к различным криптографическим атакам.

165. **Фисун, С. Н.** Шифрование данных при помощи криптографических сервисов платформы Microsoft.net / С. Н.

Фисун, А. И. Копылов // Інформаційні технології та інформаційна безпека в науці, техніці та навчанні "ІНФОТЕХ-2011" : матеріали міжнар. наук.-практ. конф., м. Севастополь, 5—10 верес. 2011 р. / М-во освіти і науки, молоді та спорту України, Севастоп. нац. техн. ун-т. — Севастополь, 2011. — С. 167—168.
(Шифр в БД 004(06)/И 741-517245)
Рассматриваются возможности криптографических сервисов, предоставляемых платформой Microsoft.net. Данные сервисы можно рассматривать как альтернативу интерфейсу CryptoAPI, который был принят корпорацией Microsoft в 1996 году. Они позволяют использовать различные криптографические алгоритмы для шифрования данных. С использованием этих алгоритмов на языке программирования C# была разработана программа шифрования и скрытия зашифрованной информации в файле.

166. **Фисун, С. Н.** Безопасность приложений ASP.NET / С. Н. Фисун, А. И. Копылов // Інформаційні процеси і технології "Інформатика-2012" : матеріали міжнар. наук.-практ. конф. молодих учених і студ., Севастополь, 23—27 квіт. 2012 р. / М-во освіти і науки, молоді та спорту України, Севастоп. нац. техн. ун-т. — Севастополь, 2012. — С. 236—238. — Библиогр. в конце ст.(2).
(Шифр в БД 004(063)/І-74-259229)
Наряду с дорогими и высокотехнологичными системами безопасности существуют технологии более низкого ранга, но способные обеспечить безопасность на программном уровне. В работе рассматриваются средства, которые наиболее распространены в среде ASP.NET и платформе .NET Framework. Основное внимание будет уделено таким аспектам безопасности, как аутентификация и авторизация пользователей.

167. **Хорев, П. Б.** Программно-аппаратная защита информации)[Электронный ресурс] : Учебное пособие / П. Б. Хорев. — 2-е изд., испр. и доп. — М.: Форум: ИНФРА-М, 2015. — (Высшее образование. — Электрон. данные. — Режим доступа : http://znanium.com/bookread2.php?book=489084; по паролю. Учебное пособие посвящено методам и средствам программно-аппаратной защиты информации и особенностям их применения для обеспечения информационной безопасности компьютерных систем и сетей. Рассматриваются методы и средства идентификации и аутентификации субъектов компьютерных систем, разграничения их доступа к объектам КС, аудита их действий в компьютерной системе. Анализируются средства защиты информации, входящие в состав операционных систем Microsoft Windows, клона Unix и серверов IBM AS/400. Также рассматриваются программные средства криптографической защиты информации, входящие в состав операционных систем Microsoft Windows и клона Unix, и аппаратные шифраторы.

168. **Хорев, А. А.** Способы и средства подавления электронных устройств перехвата информации, подключаемых к двухпроводным телефонным линиям [Текст] / А. А. Хорев // Защита информации. Инсайд : информ. — метод. журн. —

2013. — **N 1.** — С. 12—19 : ил. — Библиогр. в конце ст.

169. **Шаньгин, В. Ф.** Защита компьютерной информации : эффективные методы и средства : учеб. пособие для студ. вузов, обуч. по напр. "Информатика и вычислительная техника" / В. Ф. Шаньгин. — М. : ДМК Пресс, 2010. — 544 с. : ил. — (Администрирование и защита). — Список сокр.: с. 19—22. — Библиогр.: с. 524—529. — Предм. указ.: с. 530—542.
(Шифр 004.7.056.5(075.8/Ш 228-309988)
Экземпляры: всего:2 — ЧЗТ(1), УА(1)

**Шаньгин, В. Ф.** Информационная безопасность компьютерных систем и сетей: Учебное пособие / В. Ф. Шаньгин. — М.: ФОРУМ: ИНФРА-М, 2014. — 416 с.: ил.; 60x90 1/16. — (Профессиональное образование) — Библиогр.: с. 401—408 (105 назв.).; То же [Электронный ресурс]. — Электрон. данные. — Режим доступа : http://znanium.com/bookread2.php?book=423927; по паролю.
(Шифр 004.7.056.5(075.8/Ш 228-024730)
Экземпляры: всего:1 — ЧЗТ(1)

В учебном пособии формулируются основные понятия и определения информационной безопасности и анализируются угрозы информационной безопасности в компьютерных системах и сетях. Определяются базовые понятия политики безопасности. Рассматриваются основные криптографические методы и алгоритмы защиты компьютерной информации. Обосновывается комплексный подход к обеспечению информационной безопасности корпоративных сетей. Описываются базовые технологии защиты межсетевого обмена данными. Рассматриваются методы и средства антивирусной защиты. Описывается организационно-правовое обеспечение информационной безопасности на основе стандартов и руководящих документов Государственной технической комиссии России. Предназначено в качестве учебного пособия для студентов, обучающихся по соответствующим специальностям.

170. **Шаньгин, В. Ф**. Комплексная защита информации в корпоративных системах [Электронный ресурс]: Учебное пособие / В.Ф. Шаньгин. — М.: ФОРУМ: ИНФРА-М, 2013. — (Высшее образование). — Электрон. данные. — Режим доступа : http://znanium.com/bookread2.php?book=402686; по паролю.

Книга посвящена методам и средствам комплексной защиты информации в корпоративных системах. Формулируются основные понятия защиты информации, анализируются угрозы информационной безопасности в корпоративных системах. Обсуждаются базовые понятия и принципы политики безопасности. Описываются криптографические методы и алгоритмы защиты корпоративной информации. Обсуждаются методы и средства идентификации, аутентификации и управления доступом в корпоративных системах. Анализируются методы защиты электронного документооборота. Обосновывается комплексный подход к обеспечению информационной безопасности корпоративных систем. Рассматриваются средства обеспечения безопасности операционных систем UNIX и Windows Vista..

171. **Шахайда, В. М.** Основы информационной безопасности : Метод. рекомендации по выполнению курсового проекта / В.

М. Шахайда, А. В. Лебеденко, В. В. Шилин. — Севастополь : СНУЯЭиП, 2011. — 32 с : рис. — Библиогр.: с. 31

Экземпляры: всего:95 — ЧЗ(4), ХР(6), УФ(85) библ-ки ИЯЭиП

Изложены общие требования к разработке, построению изложению и оформлению курсового проекта по изучению технических каналов утечки информации, которые могут быть реализованы на объектах информационной деятельности.

172. **Щербаков, В. Б.** Безопасность беспроводных сетей: стандарт IEEE 802.11 / В. Б. Щербаков, С. А. Ермаков ; ред. С. А. Борисов. — М. : РадиоСофт, 2010. — 256 с. : ил. — Библиогр.: с. 248-255.

(Шифр 004.7.056.5/Щ 612-766078)

Экземпляры: всего:1 — ОКХ(1)

173. **Аулов, І. Ф.** Хмарні обчислення та аналіз питань інформаційної безпеки в хмарі / І. Ф. Аулов, І. Д. Горбенко // Прикладная радиоэлектроника. — 2013. — **N 2.** — С. 194—201. — Бібліогр. наприкінці статті. Рассматривается современное состояние применения и развития облачных вычислений, основные преимущества и недостатки их использования, в государствах, на предприятиях и в научной деятельности. Определяются и анализируются стандарты, нормативные и руководящие документы в отрасли информационной безопасности облачных вычислений, которые разработаны Cloud Security Alliance (CSA), Европейским агентством сетевой и информационной безопасности (ENISA) и Национальным институтом стандартов и технологий (NIST), а также приводятся результаты детального анализа вопросов информационной безопасности в облаке.

174. **Бевз, О. М.** Шифрування даних на основі високонелінійних булевих функцій та кодів з максимальною відстанню : монографія / О. М. Бевз ; Вінниц. нац. техн. ун-т. — Вінниця : Вид-во Вінниц. нац. техн. ун-ту, 2010. — 96 с. : ил. — Бібліогр.: с. 91—95 (65 назв.).

(Шифр 004.056.55/Б 36-008453)

Экземпляры: всего:1 — ОКХ(1)

175. **Гордієнко, С. Б.** Управління безпекою в корпоративних розподілених обчислювальних системах на підприємствах зв'язку / С. Б. Гордієнко, Р. О. Рубан // Зв'язок : наук.-вироб. журн. — 2013. — **N 1.** — С. 62—64. — Бібліогр. наприкінці статті. Проанализированы угрозы, которым подвергается конфиденциальность деятельности структур, функционирующих на базе распределенных вычислительных систем. Даны рекомендации по обеспечению их информационной безопасности и перечень средств защиты, каждое из которых направлено на преодоление определенного набора угроз, обусловленных человеческим фактором.

176. **Демчишин, М. В.** Вплив вразливості об'єктів розв'язок прямої та зворотної задач менеджменту інформаційної безпеки / М. В. Демчищин, Є. Г. Левченко // Системні дослідження та

інформаційні технології : міжнар. наук.-техн. журн. — 2012. — **N 3**. — С. 43—57 : граф. — Бібліогр. наприкінці ст.

177. **Демчишин, М. В.** Співставлення чіткого та нечіткого підходів до розв'язку задач інформаційної безпеки / М. В. Демчишин, Є. Г. Левченко // Системні дослідження та інформаційні технології : міжнар. наук.-техн. журн. — 2013. — **N 2**. — С. 101—113 : граф. — Библиогр. в конце ст.

178. **Еннан, Р.** Особливості правового режиму ноу-хау / Р. Еннан // Інтелектуальна власність : наук.-практ. журн. — 2012. — **N 9**. — С. 27—33. — Бібліогр. наприкінці статті (10).

179. **Жураковський, Б. Ю.** Підвищення ефективності захисту повідомлень від помилок в інформаційних мережах / Б. Ю. Жураковський // Зв'язок : наук.-вироб. журн. — 2013. — **N 1**. — С. 19—22 : табл. — Библиогр. в конце ст.

Рассмотрены вопросы повышения эффективности защиты информации от ошибок. Выяснены причины и степень группирования ошибок в каналах разного типа. Приведены вероятности ошибки при передаче избыточными кодами по каналам с независимыми и пакетными ошибками. Даны рекомендации по выбору кодов для защиты информации от ошибок.

180. "**Інформаційні технології та інформаційна безпека в науці, техніці та навчанні "ІНФОТЕХ-2011", Міжнар. наук.-практ. конф. (2011 р. ; Севастополь).**

Міжнародна науково-практична конференція "Інформаційні технології та інформаційна безпека в науці, техніці та навчанні "ІНФОТЕХ-2011", 5—10 верес., 2011 р. = Информационные технологии и информационная безопасность в науке, технике и образовании "ИНФОТЕХ-2011" = Information technologies and information's safety in science, technigue and education "INFOTECH-2011" : матеріали конф. / М-во освіти і науки, молоді та спорту України, Севастоп. нац. техн. ун-т ; ред. О. В. Скатков. — Севастополь : Вид-во Севастоп. нац. техн. ун-ту, 2011. — 266 с. : іл. — Загл., сост. каталогизатором : Інформаційні технології та інформаційна безпека в науці, техниці та навчанні "ІНФОТЕХ-2011". — Загл. обл. : Информационные технологии и информационная безопасность в науке, технике и образовании "ИНФОТЕХ-2011". — Бібліогр. наприкінці ст. — Алф. покажч.: с. 262—264.

(Шифр 004(06)/И 741-517245)

Экземпляры: всего:1 — ОКХ(1)

181. **Кіслов, Д.** Проблемы безопасности информационного

развития человечества / Д. Кіслов // Політичний менеджмент : укр. наук. журн. — 2013. — **N 1/2.** — С. 145—152. — Бібліогр. наприкінці ст. (18).

Рассматриваются проблемы формирования безопасности информационного развития человечества в условиях глобальных экономических, социальных и политических трансформаций. Анализируются угрозы международным и национальным информационно-коммуникационным системам, а также показано влияние на них кризисных явлений современности. Предлагается формирование теоретических основ медиабезопасности на базе классических работ по философскому осмыслению феномена информации в XX веке.

182. **Климаш, М. М.** Аналіз та дослідження найпоширеніших загроз безпеки інформаційного корпоративного середовища / М. М. Климаш, І. С. Беляєв // Шоста міжнародна науково-технічна конференція та Четверта студентська науково-технічна конференція "Проблеми телекомунікацій", присвячені Дню науки і Всесвітньому дню телекомунікацій, 24—27 квітня 2012 року : матеріали конф. / НТУУ "Київ. політехн. ін-т", Ін-т телекомунікац. систем НДІ телекомунікацій. — К., 2012, **секц. 2** : Проводовий зв'язок, оптоволоконні системи та мережі. — С. 89—91 : ил. — Бібліогр. наприкінці ст. (3).

183. **Контроль** та візуалізація стану функціональної безпеки інформаційних систем із застосуванням бездротових сенсорних мереж / В. М. Чиж, М. П. Карпінськии, С. М. Балабан // Прикладная радиоэлектроника. — 2013. — **N 2.** — С. 356—362 : рис. — Бібліогр. наприкінці статті. Обоснована целесообразность использования кластерной модели с симплексным покрытием его поля. Рассмотрена важность и сложность организации эффективных методов контроля за состоянием надежности распространения информации в беспроводных сенсорных сетях. Предложены оригинальные методы контроля за параметрами сигналов отдельных или компактно расположенных сенсоров и визуализации атак на н поля для визуализации областей трансформации сенсоров, сигналов.

184. **Лахно, В.** Моделювання інформаційної безпеки корпоративних систем підприємств з використанням теорії ігор і марківських процесів / В. Лахно, А. Петров // Вісник Національного університету "Львівська політехніка" : зб. наук. праць / М-во освіти і науки України, Нац. ун-т "Львів. політехніка". — Львів : Вид-во Нац. ун-ту "Львів. політехніка", 2010. — **№ 663**: Комп'ютерні науки та інформаційні технології. — С. 122—127 : рис. — Бібліогр. наприкінці статті.

Рассмотрены вопросы моделирования системы защиты информации, построенной с использованием теории игр и теории случайных марковских процессов, с помощью которой рассматривается совокупность проектов систем защиты информации, рассчитываются вероятности осуществления угроз для ресурсов корпоративных информационных систем и риски по каждой угрозой, и на основе этих показателей выбирается оптимальный проект.

185. **Мельниченко, О.** Аудит електронних грошей у банках України / О. Мельниченко // Вісник Національного банку України. — 2013. — **№ 3**. — С. 41—45. — Бібліогр. в кінці ст.(16). Рассмотрены актуальные вопросы аудита электронных денег в банках Украины, их место и значение в активах банка и вопрос правильного отражения операций с ними в бухгалтерском учете банков, осуществляющих эмиссию электронных денег. Также описана процедура организации аудиторской проверки безопасности банка, в том числе информационной, при работе с электронными деньгами.

186. **Національний університет "Львівська політехніка".** Вісник Національного університету "Львівська політехніка" : зб. наук. пр. / М-во освіти і науки України, Нац. ун-т "Львів. політехніка". — Львів : Вид-во Львів. політехніки. — 1964.
№ 753 : Автоматика, вимірювання та керування / ред. В. Б. Дудикевич. — 2013. — 168 с. : ил. — Бібліогр. в кінці розд.
(Шифр 06/Н 35-263803)
Экземпляры: всего:1 — ОКХ(1)
В вестнике опубликованы статьи, которые отображают результаты работ в области измерений и способов управления с использованием современной аналоговой и цифровой техники, в том числе , микропроцессорных систем. Для научных работников, преподавателей, инженеров, аспирантов и студентов.

187. **Поля і хвили** в системах технічного захисту інформації : підручник для студентів вищих навчальних закладів, які навчаються за напрямом "Системи технічного захісту інформації" / В. М. Шокало [та ін.] ; за загальною редакціею . В. М. Шокало ; Міністерство освіти і науки, молоді та спорту України, Харківський національний університет радіоелектроніки. — Харків : Колегіум. — 2013
**Ч. 1**. — 2013. — 455, [1] с. : іл. ; 21 см. — Предметний покажчик: с. 6—10. — Бібліографія: с. 418—424. — Скорочений біографічний словник: с. 425—433. — Словник термінів: с. 443—449.
(Шифр 537.8/П 54-965104)
Экземпляры: всего:1 — ЧЗТ(1)

188. **Проскуровский, Р. В.** Аналіз стану підготовки фахівців у галузі «Інформаційна безпека» / Р. В. Проскуровский // Прикладная радиоэлектроника. — 2013. — **N 2**. — С. 303—307. — Бібліогр. наприкінці статті. Проведен обзор состояния подготовки специалистов по защите информации в Украине. Анализ отраслевых стандартов высшего образования Украины в отрасли "Информационная безопасность" показал, что есть потребность в их доработке и во второй редакции. Проведен короткий анализ состояния подготовки специалистов по защите информации в Казахстане и России.

189. **Філіпова, Л.** Морально-етичні заходи запобігання інформаційній небезпеці в Інтернеті / Л. Філіпова // Вісник Книжкової палати : наук.-практ. журн. — 2013. — **N 3.** — С. 42—44. — Библиогр. в конце ст. (14). Характеризуются современные проявления информационных угроз и компьютерных преступлений в сетевом пространстве Интернета. Рассматриваются морально-этические проблемы взаимоотношений в сети и обосновывается их важность для предупреждения и предотвращения информационной опасности в интернет-пространстве. Подчеркивается важность внедрения в украинскую образовательную систему учебного курса "Компьютерная этика".

190. **Чернега, В. С.** Безпровідні локальні комп'ютерні мережі : навч. посіб. для студ. вищ. навч. закл. / В. С. Чернега, Б. Платтнер ; наук. ред. О. В. Скатков. — К. : Кондор, 2013. — 238 с. : іл. — Бібліогр.: с. 232—233. — Предм. покажч.: с. 236—237.
(Шифр 004.732(075.8)/Ч-49-009350)
Экземпляры: всего:31 — УА(30), ЧЗТ(1)

**Просмотрено**: электронный каталог(http://lib.sevsu.ru/cgi-bin/irbis64r_72/cgiirbis_64.exe?C21COM=F&I21DBN=BOOK&P21DBN=BOOK&S21CNR=20&Z21ID=), из электронных ресурсов удаленного доступа Электронная Библиотечная Система «Znanium» (http://znanium.com/)

Составитель:библиограф Пряхина Л. В.