

Авторам и издателям

Рецензируемый журнал «Защита информации. Инсайд» рассматривает и публикует научные статьи, касающиеся проблематики информационной безопасности. Правила публикации научных статей ориентированы на свод правил COPE (Комитет по этике публикаций, Committee on Publication Ethics, www.publicationethics.org).

Все опубликованные в журнале статьи в полнотекстовом виде направляются в НЭБ (Научная электронная библиотека, http://elibrary.ru/title_about.asp?id=25917).

Авторские гонорары не выплачиваются, рукописи не возвращаются. Решение о публикации статьи принимается членами редакционной коллегии журнала.

Одобренные редакционной коллегией журнала материалы публикуются в течение полугода с момента принятия решения о публикации.

Заявка на публикацию отправляется на электронную почту журнала: editor@inside-zi.ru.

Условия публикации

К рассмотрению принимаются ранее нигде не опубликованные материалы, соответствующие проблематике информационной безопасности по следующим группам специальностей научных работников:

05.13.06 – Автоматизация и управление технологическими процессами и производствами (по отраслям) (технические науки)

Принимаются к публикации статьи по тематике **п. 12**. Методы контроля, обеспечения достоверности, защиты и резервирования информационного и программного обеспечения АСУТП, АСУП, АСТПП и др.

05.13.11 – Математическое и программное обеспечение вычислительных машин, комплексов и компьютерных сетей (технические науки)

Принимаются к публикации статьи по тематике **п. 10**. *Оценка качества, стандартизация и сопровождение программных систем.*

05.13.15 – Вычислительные машины, комплексы и компьютерные сети (технические науки)

Принимаются к публикации статьи по тематике **п. 5**. *Разработка научных методов и алгоритмов создания структур и топологий компьютерных сетей, сетевых протоколов и служб передачи данных в компьютерных сетях, взаимодействия компьютерных сетей, построенных с использованием различных телекоммуникационных технологий, мобильных и специальных компьютерных сетей, защиты компьютерных сетей и приложений.*

05.13.17 – Теоретические основы информатики (технические науки)

Принимаются к публикации статьи по тематике **п. 3**. *Исследование методов и разработка средств кодирования информации в виде данных. Принципы создания языков описания данных, языков манипулирования данными, языков запросов. Разработка и исследование моделей данных и новых принципов их проектирования и п. 11*. *Разработка методов обеспечения высоконадежной обработки информации и обеспечения помехоустойчивости информационных коммуникаций для целей передачи, хранения и защиты информации; разработка основ теории надежности и безопасности использования информационных технологий.*

05.13.19 – Методы и системы защиты информации, информационная безопасность (технические науки)

Принимаются к публикации статьи по тематике всех пунктов:

1. *Теория и методология обеспечения информационной безопасности и защиты информации.*
2. *Методы, аппаратно-программные и организационные средства защиты систем (объектов) формирования и предоставления пользователям информационных ресурсов различного*

вида.

3. Методы, модели и средства выявления, идентификации и классификации угроз нарушения информационной безопасности объектов различного вида и класса.
4. Системы документооборота (вне зависимости от степени их компьютеризации) и средства защиты циркулирующей в них информации.
5. Методы и средства (комплексы средств) информационного противодействия угрозам нарушения информационной безопасности в открытых компьютерных сетях, включая Интернет.
6. Модели и методы формирования комплексов средств противодействия угрозам хищения (разрушения, модификации) информации и нарушения информационной безопасности для различного вида объектов защиты вне зависимости от области их функционирования.
7. Анализ рисков нарушения информационной безопасности и уязвимости процессов переработки информации в информационных системах любого вида и области применения.
8. Модели противодействия угрозам нарушения информационной безопасности для любого вида информационных систем.
9. Модели и методы оценки защищенности информации и информационной безопасности объекта.
10. Модели и методы оценки эффективности систем (комплексов) обеспечения информационной безопасности объектов защиты.
11. Технологии идентификации и аутентификации пользователей и субъектов информационных процессов. Системы разграничения доступа.
12. Мероприятия и механизмы формирования политики обеспечения информационной безопасности для объектов всех уровней иерархии системы управления.
13. Принципы и решения (технические, математические, организационные и др.) по созданию новых и совершенствованию существующих средств защиты информации и обеспечения информационной безопасности.
14. Модели, методы и средства обеспечения внутреннего аудита и мониторинга состояния объекта, находящегося под воздействием угроз нарушения его информационной безопасности.
15. Модели и методы управления информационной безопасностью.

Материалы для публикации передаются в редакцию в электронном виде по электронной почте editor@inside-zi.ru.

Все присылаемые работы должны быть оформлены в соответствии с формальными редакционными требованиями (http://inside-zi.ru/pages/editors/rus/design_require.pdf).

Редакция оставляет за собой право при необходимости запросить у авторов заключение о возможности публикации статьи в открытых источниках. Переписка с авторами осуществляется по электронной почте.

Порядок рецензирования

Все статьи, поступающие в редакцию (соответствующие тематике и оформленные согласно требованиям к публикации), подлежат обязательному рецензированию в течение месяца с момента поступления. Одобренные статьи публикуются в течение полугода с момента одобрения, а отправленные на доработку – с момента устранения замечаний.

В качестве рецензентов привлекаются члены редсовета, которые являются признанными специалистами по тематике рецензируемых материалов и имеют в течение последних 3 лет публикации по тематике рецензируемой статьи.