**Зохре Карім Заде. Програмно-апаратні засоби генерації псевдовипадкових (послідовностей для підвищення ефективності захисту інформації в ЕОМ та мережах : Дис... канд. наук: 05.13.13 - 2007.**

|  |  |
| --- | --- |
| |  | | --- | | **Зохре Карім Заде**. Програмно-апаратні засоби генерації псевдо випадкових послідовностей для підвищення ефективності захисту інформації в ЕОМ та мережах. – Рукопис.  Дисертація на здобуття наукового ступеня кандидата технічних наук за спеціальністю 05.13.13 – Обчислювальні машини, системи та мережі. – Національний технічний університет України ”Київський політехнічний інститут”, Київ, 2007.  Дисертаційна робота присвячена проблемі створення засобів генерації псевдовипадкових двійкових послідовностей, що забезпечують поліпшення їх характеристик, які впливають на ефективність захисту інформації.  Основна увага приділена розробці методів проектування зсувних регістрів з нелінійною функцією зворотного зв’язку, яка забезпечує період повторення 2*n* для *n*–розрядного регістру. Проведено теоретичне дослідження властивостей таких функцій. Базовою концепцією методу побудови нелінійних функцій зворотного зв’язку, що забезпечують період повторення 2*n* для *n*–розрядного зсувного регістру є направлене об’єднання кодових кілець – множин *n*–розрядних кодів, які утворюються при циклічному зсуві.  Виконано аналіз числа функцій вказаного класу, що можуть бути синтезовані з застосуванням запропоновано методу. Доведено, що метод дозволяє одержувати на порядок більше вказаних функцій в порівнянні з відомими методами.  Виконана розробка модифікації запропонованого методу, яка використовує алгебраїчну форму для представлення булевої функції зворотного зв’язку. На відміну від відомих методів, обчислювальна складність яких *O*(2*n*), розроблена модифікація вимагає суттєво менших обчислювальних ресурсів - *O*(*n*2) і дозволяє одержувати функції зворотного зв’язку для зсувних регістрів значної розрядності.  Крім методів побудови зсувних регістрів з нелінійною функцією зворотного зв’язку, в дисертації виконано вдосконалення схеми двокаскадного генератора. Запропоновано метод проектування генератора балансних нелінійних булевих функцій, що задовольняють критерію лавинного ефекту і управляється кодом. Показано, що використання таких генераторів покращує характеристики псевдовипадкових послідовностей і тим самим підвищує ефективність захисту інформації. | |
| |  | | --- | | В дисертаційній роботі, відповідно до поставленої мети, виконано теоретичне обґрунтування і одержано нове вирішення наукової задачі: підвищення ефективності захисту інформації в комп’ютерних системах та мережах з використанням псевдовипадкових двійкових послідовностей за рахунок поліпшення їх характеристик шляхом вдосконалення програмно-апаратних засобів їх генерації.  *Основні наукові і практичні результати полягають у наступному:*  1. Одержала подальший розвиток теорія послідовних машин, а саме: виявлені нові властивості нелінійних булевих функцій зворотного зв’язку, що забезпечують максимальний період повторення коду на зсувному регістрі, одержані аналітичні оцінки кількості кодових кілець. Отримані теоретичні результати, які покладені в основу побудови програмно-апаратних засобів псевдовипадкових двійкових послідовностей, використання яких дозволяє підвищити ефективність функцій захисту інформації.  2. Модифіковано метод проектування *n*-розрядних зсувних регістрів з нелінійною функцією зворотного зв’язку для формування псевдовипадкових двійкових послідовностей з періодом повторення 2*n*. Відмінністю методу є застосування для одержання функції направленого об’єднання кодових кілець виходячи з заданих характеристик її складності і нелінійності, що забезпечує високу ефективність використання двійкових послідовностей, які сформовані такими схемами, для захисту інформації.  3. Удосконалено метод синтезу нелінійних булевих функцій зворотного зв’язку *n*-розрядного зсувного регістру з періодом повторення 2*n* коду на ньому, за рахунок оптимізації побудови диз’юнктивної нормальної форми функції, що дозволило знизити обчислювальну складність процедури синтезу до рівня *O(n2)*, що є суттєво меншим в порівнянні з синтезом за відомими методами, які мають обчислювальну складність *O(2n).*Використання вдосконаленого методу дозволяє синтезувати нелінійні функції зворотного зв’язку для зсувних регістрів великої розрядності.  4. Запропоновано комбінаторний метод формування нелінійних булевих функцій зворотного зв’язку *n*-розрядного зсувного регістру, які забезпечують формування псевдовипадкових двійкових послідовностей з періодом 2*n*. Відмінністю методу є те, що він дозволяє одержувати всі нелінійні булеві функцій зворотного зв’язку вказаного класу, що, з одного боку відкриває можливості оптимізації засобів генерації послідовностей, а з другого – утруднює підбір функцій зворотного зв’язку при спробах порушення захисту інформації.  5. Розроблено метод синтезу генератора нелінійних булевих функцій, що відповідають критерію лавинного ефекту, використання якого в двокаскадній схемі формування псевдовипадкових послідовностей забезпечує можливість зміни функцій нелінійного перетворення зі збереженням важливих для захисту інформації характеристик. Можливість переналагодження за ключем нелінійного перетворювача в схемі генерації двійкових послідовностей дозволяє значно підвищити ефективність їх застосування в системах захисту інформації. | |