

4. Bardis N.G., Markovskiy A. P., Doukas N., Karadimas N. V. True Random Number Generation Based on Environmental Noise Measurements for Military Applications. *Proceedings of the 8th WSEAS International Conference on Signal Processing, Robotics, and Automation*. 2009. P. 68–73.

5. Гріненко Т.О., Нарезній О. П. Квантові генератори випадкових чисел в криптографії. *Системи обробки інформації*. 2015. Вип. 10(135). С. 86–89.

Ключові слова: послідовності псевдовипадкових чисел, генератор псевдовипадкових чисел.

Ключевые слова: последовательности псевдослучайных чисел, генератор псевдослучайных чисел.

Keywords: sequences of pseudorandom numbers, pseudorandom number generator

Науковий керівник: к.т.н., доц. Трофименко О. Г.

Дроздов Богдан Михайлович

Національний університет «Одеська юридична академія»,
студент 4-го курсу факультету кібербезпеки
та інформаційних технологій

СИСТЕМА ІДЕНТИФІКАЦІЇ З ЕЛЕМЕНТАМИ КОНТРОЛЮ ДОСТУПУ ДО ПРИМІЩЕННЯ

Охорона всякого об'єкта включає кілька рубежів, число яких залежить від рівня режимності об'єкта. При цьому у всіх випадках значущим кордоном буде система управління контролю доступом (СУКД) на об'єкт.

Якісно організована із застосуванням новітніх технічних засобів СУКД дозволить вирішувати цілий ряд завдань. До числа особливо головним можна віднести наступні:

- протидія індустріального шпигунства;
- протидія розкраданню;
- протидія саботажу;

- протидія умисного пошкодження матеріальних цінностей;

- контроль робочого часу;
- контроль своєчасності приїзду і звільнення працівників;
- охорона конфіденційності інформації;
- регулювання потоку відвідувачів;
- контроль в'їзду та виїзду транспорту.

Крім цього, СУКД є бар'єром для «цікавих». При реалізації певних СУКД застосовують різні методи і реалізують їх пристрої для ідентифікації і аутентифікації особи. Слід зазначити, що СУКД є одним з особливо розвинених секцій ринку безпеки як в Україні, так і за кордоном.

За даними ряду експертів річний прихід ринку СУКД становить більше двадцять п'ять відсотків. Число фахівців, що працюють в галузі технічних систем безпеки, перевищило п'ятсот тис. чоловік.

Як особливо часто використовуваних СУКД можна назвати наступні:

- турнікети звичайні настінні;
- турнікети для проходу в коридорах;
- шлюзові кабінки;
- механічні хвіртки;
- роторні турнікети;
- обертові двері;
- дорожні блокіратори;
- шлагбауми;
- паркувальні системи;
- круглі розсувні двері;
- трештангові турнікети;
- повнозростові турнікети;
- розсувні турнікети.

Головним є питання про засоби інтеграції СУКД з всякий системою безпеки із застосуванням відкритого протоколу. Значущою специфікою ринку СУКД є те, що покупці стали купувати більше дорогі виконавчі пристрої, причому іноземного виробництва.

Іншою специфікою новітніх СУКД є впровадження спец-спецтехнології смарт-карти, натомість класичних проксіміті-карт, технології далекої ідентифікації (частоти 800–900 МГц і 2.45 ГГц).

Як вже говорилося вище, будь-яка СУКД призначена для того, щоб автоматично пропускати тих, кому цей вхід дозволений, і не пропускати тих, кому вхід заборонений. Всі її інші функції (збереження матеріальних цінностей, контроль і облік робочого часу і ін.) що є результатом основного призначення.

У загальному випадку під СУКД зазвичай розуміють сукупність програмнотехнічних і організаційно-методичних засобів, за допомогою яких вирішується завдання контролю і управління приміщенням підприємства і окремими приміщеннями, а також оперативний контроль за пересуванням персоналу і часу його перебування на території підприємства.

Для багатьох організацій завдання контролю праці, а також підвищення продуктивності і трудової дисципліни є дуже актуальними.

Більшість підприємств бажають платити своїм співробітникам тільки за відпрацьований ними час, виключивши запізнення, передчасні відходи і самовільні відлучки з роботи. Дуже важливо стежити за роботою співробітника протягом робочого часу, адже своєчасне поява не можна назвати гарантією сумлінного виконання всіх обов'язків. Тому варто використовувати вже готові рішення [1].

Багато компаній знають, що таке СУКД і як її використовувати. Вона вже довго допомагає керівникам, співробітникам бухгалтерії і відділу кадрів вирішувати завдання, пов'язані з управлінням доступу і контролем відповідно до Трудового законодавства. Саме системи контролю створюють доказову базу під час трудових спорів, за допомогою якої запобігають зловживанням і помилки.

Можна зробити висновок що системи контролю та управління доступом в наш час дуже актуально як в сфері захисту, так і в повсякденному житті. Ми часто стикаємося з

прикладами їх застосування в банках, пропуск в приміщення тощо.

Список використаних джерел:

1. Сабынин В. Н. Организация пропускного режима первый шаг к обеспечению безопасности и конфиденциальности информации // *Информост – радиоэлектроники и телекоммуникации*, 2001. № 3 (16).

Ключові слова: Система управління контролю доступом, контроль, система безпеки, технічні засоби.

Ключевые слова: Сисетема контролю доступа, контроль, система безопасности, технические средства.

Key words: Access control system, control, safety system, technical means.

Науковий керівник: к.т.н., доцент Бойко В. Д.

Золотверх Денис Олегович

Національний університет «Одеська юридична академія»,
студент 4-го курсу факультету кібербезпеки
та інформаційних технологій

ДОСЛІДЖЕННЯ КРИПТОГРАФІЧНИХ ОЗНАК КРИПТОСТІЙКИХ ХЕШ-ФУНКЦІЙ

Хеш-функції надзвичайно корисні і з'являються майже у всіх програмах захисту інформації.

Хеш-функція – це математична функція, яка перетворює числове вхідне значення в інше стиснене числове значення. Вхід у хеш-функцію є довільної довжини, але вихід завжди має фіксовану довжину.

Значення, що повертаються хеш-функцією, називаються дайджестом повідомлення або просто хеш-значеннями.

Хеш функціям притаманні наступні ознаки:

Дайджест фіксованої довжини. Кожна хеш функція може приймати на вході повідомлення довільної довжини, та на виході видавати дайджест однієї, чітко визначеної довжини.