# Актуальні аспекти проектування системи комплексного захисту інформації підприємства

**Р.М. Загорський**, *студент,*
**О.П. До́ренський**, *викладач*
*Кіровоградський національний технічний університет*

Сьогодні, не зважаючи на стрімкий розвиток галузі захисту інформації та інформаційної безпеки в цілому, кількість інцидентів безпеки продовжує стрімко зростати. Однією з причин цього факту є криза загальносистемних розробок, направлених на розв'язок актуальних задач безпеки інформації та деякі суперечності спеціалістів щодо підходів організації безпеки інформації сучасних інформаційно-телекомунікаційних систем (ІТС) [1-3].

Інформаційна система (ІС) підприємства, як правило, складається з декількох рівнів управління, які в тій чи іншій мірі пов'язані між собою [2, 3]. Тому у зловмисників завжди знайдеться певний набір засобів і методів, які дозволяють обійти політику безпеки підприємства, організації, установи тощо, якщо він проник хоча б на один з них [4, 5]. Офіційна статистика представляє факти, які свідчать про те, що більшість несанкціонованих спроб доступу до інформаційний ресурсів залишаються невиявленими. Наприклад, за даними Національного відділу ФБР США, кількість невиявлених атак знаходиться в межах від 85% до 97% [5].

Звичайно, не всі недоліки, що призвели до результативних несанкціонованих доступів до інформаційних ресурсів, у тому числі і до найбільш захищених у світі, відомі [3]. Тому постійно актуальним є питання проектування і оцінювання ефективності комплексних систем захисту інформації (КСЗІ), які максимально ефективно реалізують відповідну політику безпеки підприємства, установи, організації тощо [4].

Стандарт ISO/IEC 15408 визначає профіль системи захисту інформації як сукупність функціональних та гарантійних вимог, що дозволяють реалізувати систему захисту з необхідним рівнем інформаційної безпеки.

Як показало дослідження [6], методологія оцінювання інформаційної безпеки профіля захисту інформації ґрунтується на використанні методів аналізу та ідентифікації множини факторів, серед яких, зокрема, активи підприємства, можливі недоліки системи комплексного захисту інформації (СКЗІ), загрози, потенційні атаки тощо.

Слід зазначити, що відсутня чітка статистична інформація відносно об'єкта, що оцінюється, і навпаки більшість процесів характеризуються невизначеністю. Все це фактично унеможливлює практичне використання точних моделей, які базуються на класичній математичній теорії [3] та її методах. Для вирішення цих проблем зручніше використовувати апарат нечіткої логіки [4], де залежність входів системи та виходів задаються на основі лінгвістичної людської логіки, а не точних цифр, які в даному випадку складно опрацьовувати. Як показали дослідження, показники таких систем набагато вищі, ніж системи на чітких числах. Тому вони все частіше застосовуються у галузі захисту інформації.

Застосування конкретної діагностичної моделі залежить від виду порушення нормального ходу, вхідної інформації, знань та кваліфікації експерта. У зв'язку з цим, для одержання кількісної оцінки, що характеризує ефективність профілю захисту, пропонується використовувати екпертні оцінки, що представляються у вигляді

нечітких множин [3, 4]. Вибір значень елементів множини завжди пов'язаний з ризиком того, що обрані значення показників не забезпечують необхідного (заданого, прогнозованого) рівня безпеки. Наслідком цього є можливість здійснити ефективну атаку на інформаційні ресурси підприємства. Пошук наочного представлення знань приводить до систем на основі нечіткої логіки, яка й забезпечує представлення словесно інтерпретованих знань.

Для забезпечення можливості прийняття рішення при не тільки кількісних, але й якісних характеристик комплексної системи захисту інформації підприємства, доцільне застосування нечіткого ієрархічного дерева, на основі якого здійснюється побудова бази знань СКЗІ. Такий комплексний підхід надає можливість отримати на етапі проектування оптимальний варіант системи інформаційної безпеки підприємства, а також доцільний для застосування у системі [7].

## Список літератури


1. Доренський О.П. Особливості класифікації загроз безпеці інформації сучасної інформаційно-телекомунікаційної системи // Збірник наукових праць Кіровоградського національного технічного університету. – Вип. 20. – Кіровоград: КНТУ, 2008. – С. 155-161.
2. Галатенко В.А. Основы информационной безопасности. – М.: "ИУИТ", 2011. – 208 с.
3. Дудатьев А.В. Проектування системи безпеки інформаційних ресурсів підприємтсва. / Методи та засоби кодування, захисту й ущільнення інформації. – Вінниця: ВНТУ, 2007. – С. 75-76.
4. Домарев В.В. Безопасность информационных технологий. Системный подход. – К.: ООО "Тид "ДС", 2004. – 992 с.
5. Смірнов О.А. Основи захисту інформації: Навч. пос.. / А.О. Смірнов, Л.Г. Віхрова, С.І. Осадчий, В.Ю. Ковтун, Є.В. Мелешко. – Кіровоград: РВЛ КНТУ, 2011. – 322 с.
6. ISO/IEC 15408-1:2009 "Information technology. Security techniques. Evaluation criteria for IT security" [Електронний ресурс]. – Режим доступу: www.iso.org.
7. Загорський Р.М. Програмне забезпечення побудови моделі захисту інформації телекомунікаційної системи. / Загорський Р.М., Доренський О.П. // Матеріали XLIIV наукової конференції студентів та магістрантів КНТУ – Кіровоград: КНТУ, 2011. – с. 78.


# Платформа CLR в середовищі ОС Windows

**О.О. Іванченко**, *студент,*
**В.А. Бісюк**, *викладач*
*Кіровоградський національний технічний університет*

Common Language Runtime (скорочено CLR — «загальне середовище виконання мов») — це компонент пакету Microsoft .NET Framework, віртуальна машина, на якій виконуються всі мови платформи .NET Framework.

CLR транслює початковий код в байт-код на мові IL, реалізація компіляції якого компанією Microsoft називається MSIL, а також надає MSIL-програмам (а отже, і програмам, написаним на мовах високого рівня, що підтримують .NET Framework) доступ до бібліотеки класів .NET Framework, або так званої .NET FCL.

Середовище CLR є реалізацією специфікації CLI (англ. Common Language Infrastructure), специфікації загальномовної інфраструктури, компанії Microsoft.

Віртуальна машина CLR дозволяє програмістам забути про багато деталей щодо конкретного процесору, на якому виконуватиметься програма. CLR також забезпечує такі важливі служби як: керування пам'яттю; керування потоками; обробка виключень; збірка сміття; безпека виконання.