2. "Чорний ящик" нейронної мережі - вага зв'язку і передавальні функції різних мережевих вузлів, заморожуються після того, як мережа досягла прийнятного рівня успіху в ідентифікації подій. "Проблема чорного ящика" переслідує нейронних мереж в ряді додатків. Це постійна область досліджень в нейронних мережах.

Основними реалізаціями нейронних мереж в системах виявлення вторгнень є:

1. Включення їх в експертні системи. В той час, як нейронна мережа розширила свої можливості для виявлення нових атак, експертну систему необхідно буде оновити для того, що б вона так само розпізнавала ці загрози.

2. Нейронні мережі як автономні системи виявлення вторгнень, будуть отримуватись дані з мережевого потоку і аналізувати інформацію на наявність вторгнення.

Список використаних джерел:

1. Круглов в. в., Борисов В.В. штучні нейронні мережі. - М.: Гаряча лінія-Телеком, 2002.

2. Каллан р. основні концепції нейронних мереж.: Пер. з англ. - М.: Вільямс, 2003.

***к.пед., доц. Толок І.В. (ВІКНУ)***
***к.т.н., доц. Кльоц Ю.П. (ХмНУ)***
***к.ф.-м.н., доц. Рамський А.О. (ХмНУ)***
***Рикун В.В (ХмНУ)***

## Дослідження характеристик надійності та інформаційної безпеки вузлів комп'ютерної мережі

Так як системи зв'язку досить важливі для правильного функціонування організації, вони стають пріоритетом для злочинців. Впливаючи на мережу, організовуються атаки, спрямовані на різні характеристики інформації. Загроза інформаційної безпеки - це сукупність умов і факторів, які створюють потенційну або фактичну загрозу інформації. При атаках зловмисників існує небезпека втрати, перекручення, блокування, копіювання, поширення інформації, а також інших несанкціонованих дій з нею.

Незалежно від конкретних типів загроз необхідно забезпечити наступні основні властивості: цілісність, конфіденційність і доступність. Доступність – це можливість за прийнятний час одержати необхідну інформаційну послугу.

Під цілісністю мається на увазі актуальність і несуперечність інформації, її захищеність від руйнування і несанкціонованої зміни.

Конфіденційність – це захист від несанкціонованого доступу до інформації.

Завдання цілісності і конфіденційності успішно вирішується за рахунок використання криптографічного захисту інформації. У роботі запропоновано метод оцінки ефективності функціонування вузла зв'язку корпоративної мережі з врахуванням інформаційної безпеки. Це дає можливість вжити заходи щодо їх нейтралізації та оцінити ефективність їх використання.

Головним завданням цього дослідження є об’єднання в єдину математичну модель характеристик надійності та інформаційної безпеки. Для моделювання характеристик надійності та інформаційної безпеки можна використовувати марківські процеси і експоненціальний розподіл можливих подій. Як показник, що безпосередньо характеризує властивості системи, доцільно використовувати коефіцієнт готовності. Класичним підходом до моделювання мережі є приведення її до деревовидного графу. Одним з підходів є нормування коефіцієнту готовності ліній зв'язку та мереж передачі даних, але існуючі правила не застосовуються до корпоративних мереж передачі даних, побудованих поверх Інтернету, оскільки мережа, сформована таким чином, частково абстрагується від певного постачальника послуг.

З врахуванням вищесказаного, розробка методу оцінки ефективності функціонування вузла зв'язку корпоративної мережі з врахуванням інформаційної безпеки є актуальним науково-технічним завданням.

***д.т.н., проф. Лєнков С.В. (ВІКНУ)***
***к.т.н., доц. Тітова В.Ю. (ХмНУ)***
***к.т.н., доц. Муляр І.В. (ХмНУ)***
***Дацюк Р.М. (ХмНУ)***

## Аналіз стеганографічних алгоритмів

Актуальність вивчення стеганографії постійно зростає, оскільки з поширенням персональних комп’ютерів, і особливо Інтернету, можливість конфіденційно передавати інформацію привертає увагу значної кількості людей. Переважна більшість теоретичних та практичних досліджень у галузі стеганографії присвячена розробці нових та вдосконаленню існуючих методів приховування даних. Кількість останніх постійно зростає з часом, але в сучасній науковій літературі відсутня чітка класифікація таких методів, що ускладнює пошук і не дозволяє повною мірою оцінити рівень існуючих досягнень для їх подальшого ефективного використання.

Аналізуючи процес розвитку комп’ютерної стеганографії, можна сказати, що в найближчі роки інтерес до розробки її методів буде дедалі більше зростати. Актуальність проблеми інформаційної безпеки постійно зростає і стимулює пошук нових методів захисту інформації. З іншого боку, швидкий розвиток інформаційних технологій дає можливість впроваджувати ці нові методи захисту.

Стеганографічні методи поряд із криптографічними займають важливе місце серед методів захисту інформації. Але якщо в криптографії наявність зашифрованого повідомлення саме по собі привертає увагу зловмисника, то в стеганографії прихований зв’язок залишається невидимим, що робить організацію цього процесу досить актуальною.

Загальною особливістю стеганографічних методів є те, що приховане повідомлення або додаткова інформація вбудовується в якийсь нешкідливий, непомічений об’єкт або контейнер, в результаті чого з’являється приховане повідомлення, яке потім відкрито транспортується до одержувача за каналом