що до помилок, підбиття підсумків опитування). Оскільки програми призначені для працівників, які найчастіше не-мають досвіду роботи з комп'ютером, то інтерфейс програм передбачено максимально простим. Є режим автоматичного «програвання» інформаційного блоку програми як «слайдфільму».

Комп'ютерний самоконтроль знань також організований гранично просто, аби зафіксувати увагу працівника зосереджено лише на змістову частину запитань і не відволікалася для осмислення того, як йому запровадити свою відповідь в комп'ютер. Використовується найпростіша схема відповідей, що передбачає вибір з представленого списку варіантів відповідей шляхом вказівки мишею. Програми видають оперативні повідомлення, правильність кожної відповіді і пояснюють, у чому помилка. Отже, незалежно від рівня початкових знань, кожна людина зможе успішно "дійти" кінця програми розвитку й отримати правильні відповіді на всі питання. Досвід застосування комп'ютерних програм із серії «Наочна безпека продукції та охорона праці» на багатьох підприємствах свідчить, що муль-тимедійні комп'ютерні технології навчання з питань охорони праці та про-мислової безпеки зацікавили працівників, а в цілому цей напрям є досить перспективним. Найголовнішим результатом впровадження цих розробок, як сподіваються автори, є зниження виробничого травматизму.

к.т.н., доц. Тітова В.Ю. (ХмНУ)
д.т.н., проф. Андрощук О.С.(ХмНУ)
Даценко В.С.(ХмНУ)

Застосування нейронних мереж у виявленні вторгнень

В даний час в різних галузях науки і техніки підвищується інтерес до використання штучних нейронних мереж. На даний момент не існує альтернативи до даної системи на основі правил. Мережеві атаки постійно змінюються, тому постійно мінливий характер мережевих атак вимагає гнучку захисну систему, яка здатна аналізувати величезну кількість мережевого трафіку за методом, який менш структурований ніж той, що заснований на побудові певних правил.

Перевагами у використанні нейронної мережі у виявленні вторгнень є:

1. Гнучкість - яку надає ця мережа.
2. Швидкість - властива нейронним мережам.
3. Навчання - нейронна мережа може бути навчена розпізнавати відомі підозрілі події з високим ступенем точності.

Відстежуючи подальші виникнення цих подій, система буде здатна поліпшити аналіз подій і, можливо, провести захисні заходи, перш ніж атака буде вдало виконана.

Недоліками систем виявлення вторгнень на основі нейронних мереж є:

1. Вимоги до навчання нейронної мережі - здатність до ідентифікації ознак вторгнення повністю залежить від правильного навчання системи, дані для навчання і методи навчання.

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.