Коцюба О.В., магістрант, гр. АТ-21-2м,
Науковий керівник – Чепюк Л.О., к.т.н., доцент,
Житомирський державний технологічний університет

АВТОМАТИЗОВАНА СИСТЕМА ПІДТРИМКИ ПРИЙНЯТТЯ РІШЕНЬ ЕКСПЕРТОМ З АУДИТУ ЗАХИЩЕНОСТІ КОМП'ЮТЕРНОЇ МЕРЕЖІ ПІДПРИЄМСТВ

Для сучасного етапу розвитку суспільства характерний неперервний процес інформатизації і вдосконалення інформаційних технологій. Середовище впровадження телекомунікаційної і обчислювальних систем постійно розширюється, залучаючи усе нові сторони життя суспільства. У зв'язку з цим важливою задачею є забезпечення достатньої міри захищеності цих систем для їх ефективного функціонування в умовах прояву інформаційних загроз, для чого, у свою чергу, необхідно наявність адекватного методологічного аналізу і управління інформаційними ризиками.

Загрози інформаційної безпеки мають імовірнісний характер і змінюються в процесі функціонування комп'ютерних мереж (КМ), тому ризик необхідно розглядати як деяку імовірнісну категорію, асоційовану з поняттям збитку від успішної реалізації загроз, а в якості базової моделі взяти імовірнісну модель атак на інформаційно-телекомунікаційну систему, в котрій об'єктивні співвідношення виражені в термінах теорії імовірності та математичної статистики.

Ефективне забезпечення захисту комп'ютерних мережах можливе тільки на основі комплексного використання всіх відомих методів та підходів до вирішення даної задачі. Концепція такого комплексного захисту має задовольняти наступній сукупності вимог. По-перше, мають бути розроблені й доведені до рівня регулярного використання всі необхідні механізми гарантованого забезпечення необхідного рівня захищеності інформації. По-друге, мають існувати механізми практичної реалізації необхідного рівня захищеності інформації. Побудова системи захисту інформації (СЗІ) полягає в тому, щоб для заданої КМ створити оптимальні механізми забезпечення захисту й управління ними.

Розробка такого роду програмного продукту дасть змогу керівникам підприємств одержати реальну оцінку засобів та заходів захисту від безпосереднього та віддаленого доступу до елементів комп'ютерної мережі, організаційних та програмно-технічних засобів захисту.

В процесі розробки потрібно вирішення наступних *задач*:

- аналіз методів, засобів та технологій побудови системи підтримки прийняття рішень (СППР);
- аналіз методів, засобів та технологій побудови систем захисту КМ;
- моделювання системи підтримки прийняття рішень експерта з аудиту захищеності КМ;
- розробка структурної схеми системи підтримки прийняття рішень експерта з аудиту захищеності комп'ютерної мережі;
- програмна реалізація СППР експерта з аудиту захищеності КМ.

Аналіз дає можливість зробити висновок, що велика група методик оцінки захищеності систем інформаційних технологій базується на наявності певного набору засобів та механізмів захисту, способів виготовлення, експлуатації й тестування та дозволяють віднести той або інший пристрій або систему інформаційних технологій до одного з рівнів захищеності .

Системний підхід до проектування багаторівневої моделі СЗІ відображається на змісті етапів життєвого циклу системи інформаційної безпеки.

На першому етапі формується коректна інформаційно-безпечна КМ, тобто формується загальне інформаційне поле захищеної системи.

Метою другого етапу життєвого циклу є коректне виконання системою заданих функцій. Використовується механізм адаптації для регулювання на зміну зовнішніх чинників – відбувається збільшення, самонавчання й зміна загального інформаційного поля КМ та СІБ .

На третьому етапі відбувається згортання прикладних функцій системи КМ

При коректній роботі СІБ. Багаторівнева модель інформаційної безпеки системи КМ містить накопичений досвід нейтралізації механізмами захисту вразливості системи та характеризується максимально повною множиною відомих загроз.

Основними механізмами реалізації адаптивних СІБ є: нечіткий логічний висновок, який дозволяє використовувати досвід експертів в області інформаційної безпеки у вигляді системи нечітких предикативних правил для попереднього навчання системи, здатність адаптивних СІБ до класифікації й кластеризації та здатність адаптивного розподіленого поля системи до накопичення знань в процесі навчання, адаптивна модель СІБ.