проводится безотносительно к области применения. Характерными примерами являются измерения коэффициента экранирования экранного сооружения или коэффициента затухания сетевого фильтра. В этих случаях значения параметров затухания измеряются независимо от того, какое дальнейшее назначение изделия: для защиты устройств от внешних непреднамеренных помех или для защиты информации от утечки по техническим каналам. Вместе с тем в настоящее время в Украине существует два вида разрешения на проведение деятельности такого рода – лицензия на право проведения проверок средств ТЗИ и аккредитация Госстандарта Украины. Для чисто физических измерений, пример которых приведен выше, такой двойственный подход не допустим. С другой стороны, целый ряд специальных проверок и исследований включает особые требования, которые не могут быть предусмотрены Госстандартом. К этим особенностям относятся специальные начальные условия, отличные от лабораторных, режимы работы и тесты исследуемой аппаратуры, специальный порядок обработки результатов измерений, нормированные значения эффективности защиты и многое другое. Поэтому было бы неправильно противоставлять аккредитацию испытательных лабораторий и лицензирование в области ТЗИ.

Эти два направления должны разумно сочетаться. Для измерений общефизического характера, необходимо и достаточно иметь аккредитацию органов Госстандарта, не зависимо от назначения и функций предмета испытаний. Другое дело проведение специфических для защиты информации исследований и аттестаций. Они требуют специальных знаний и навыков, наличия нормативно-методической документации и т.д. Однако, и в этом случае, если эти работы сопровождаются измерениями, - они должны проводиться только аккредитованными в органах Госстандарта лабораториями.

Проблема нормирования труда при проведении типовых измерений и испытаний является актуальной так же, как при проведениии лицензионных и сертификационных работ.

Выводы:

1. Необходимо определить задачи и место измерений при проведении работ в области ТЗИ.
2. Определить перечень работ, содержащих измерения и испытания.
3. Провести расчет средних трудозатрат на выполнение основных операций при проведении измерений и испытаний в ходе выполнения работ различного назначения в области ТЗИ.

УДК 681.528.54

ПРОБЛЕМА ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ЕКСПЕРТНИХ СИСТЕМ

Володимир Тарасенко, Антон Михайлюк, Дмитро Воробей
Національний Технічний Університет України «КПІ»

Анотація: **У доповіді надані рекомендації щодо особливостей забезпечення інформаційної безпеки експертних систем (ЕС). Розглянуто фактори, що визначають ці особливості, та наведено узагальнену класифікацію засобів інформаційної атаки на експертну систему. Запропоновано елементи структури системи безпеки, яка була б спроможна подолати нестандарті атаки на експертну систему.**

Summary: **The report provides recommendations concerning provisions of information security to the expert systems. The causes of such features have been considered and summarized in the classification of attack methods on expert system. The report presents the structural elements of such security system, which would enable the system to resist nonstandard attacks on it.**

Ключові слова: **експертна система, засоби інформаційної атаки, система безпеки,евристичний аналізатор.**

І Необхідність створення нової системи безпеки ЕС

В більшості існуючих ЕС реалізовані методи захисту програмного забезпечення (ПЗ) без урахування огляду на специфіку ЕС. Тобто застосовуються традиційні методи захисту, а саме, верифікація користувачів, створення резервних копій тощо.

Безперечно, така система безпеки (СБ) частково вирішує проблему захисту ЕС, але робить вона це з одним припущенням – атака на ЕС повинна бути ззовні. Це припущення може дорого коштувати ЕС, оскільки, атака може бути здійснена і власними засобами ЕС.

Інтелектуальні властивості ЕС є безперечним досягненням і перевагою над іншими системами, але з точки зору безпеки це одночасно є її ахіллесовою п’ятою. Тому виникає потреба в створенні нової СБ ЕС, яка б забезпечила надійну роботу з врахуванням особливостей ЕС.

ЕС містить в собі знання багатьох експертів, а також робить власні висновки. Як знання експертів, так і зроблені на їх основі висновки є інтелектуальною власністю і потребують захисту від руйнування, несанкційованого доступу та використання. По-перше, ЕС потребує захисту від пошкодження внаслідок навмисного чи випадкового введення до неї помилкових знань. Особливістю ЕС є здатність до навчання, тому, на відміну від звичайного ПЗ, експертну систему можна пошкодити її власними засобами з її власного інтерфейсу. Це може зробити як експерт, так і користувач. По-друге, ЕС потребує захисту від викрадення її у цілому. На жаль, це теж можна здійснити засобами її власного інтерфейсу шляхом простого перебору бази знань (БЗ) у ході експлуатації.

Таким чином, функції СБ ЕС можна умовно поділити на два основних напрями, кожний з яких запобігає спробі викрадення або спробі пошкодження ЕС (див. рисунок 1).

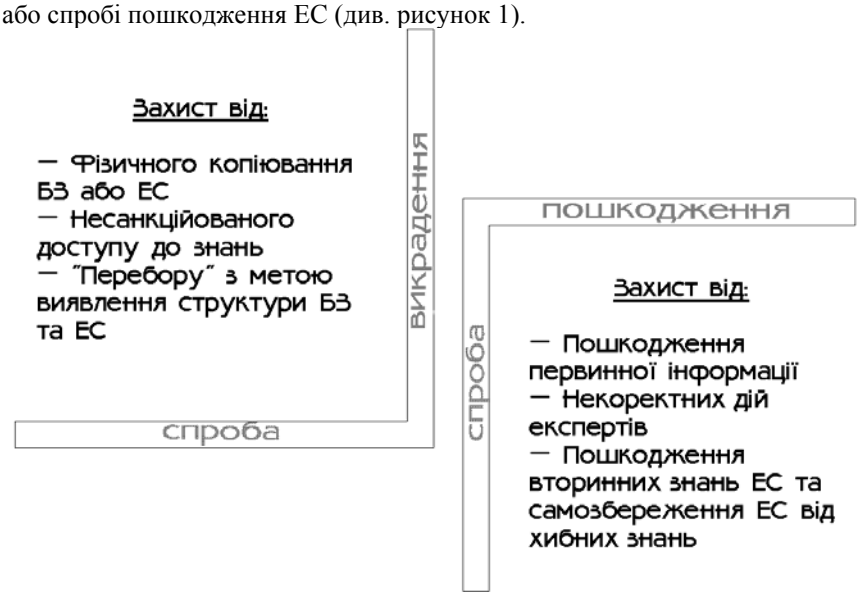

Рисунок 1 – Класифікація можливих атак на ЕС за кінцевою метою

II Формування системи безпеки, що враховує особливості ЕС

Перш за все визначимо, які у ЕС є канали порушення інформаційної безпеки та як можна завдати по них удару. Розглянемо ті випадки, коли атаки на ЕС здійснюються засобами самої ЕС, тобто через її власний інтерфейс. Інші випадки, коли робляться спроби атакувати ЕС на фізичному рівні або на рівні даних, залишимо на фізичну СБ та СБ бази даних (БД) відповідно.

Основною відмінністю роботи з ЕС від роботи із звичайним ПЗ є те, що на результати її роботи впливає не тільки той, хто створює ЕС, але й користувач. Тобто на висновки ЕС впливають знання не з одного джерела, а знання різних експертів, які необхідно зводити разом, та попередній досвід від роботи з іншими користувачами.

Зрозуміло, що небезпеку становлять тільки ті елементи в ЕС, які викликають операції по її оновленню. В свою чергу виклик цих операцій не виникає з нізвідки. Так чи інакше вони ініціюються внаслідок отримання (обміну) інформації ззовні. Якщо припустити, що адміністратор ЕС є фахівець, який ніколи не помиляється, то як потенційна загроза залишиться тільки експерт та користувач. Будь-яка робота з ЕС, направлена на модифікацію БЗ або ЕС повинна проходити під контролем СБ.

БЗ складається з великої кількості знань, отриманих від різних експертів. Крім того БЗ може поповнюватись експертами в ході експлуатації. Якщо прийняти знання первинної БЗ аксіоматичними (первинна БЗ може бути й порожньою), то будь-які додаткові знання, що вносить експерт, можуть бути хибними та завдати шкоди роботі ЕС. Причин хибності знань, отриманих від експерта, може бути дві: помилка та навмисна дезорієнтація. Обидві причини цілком можливі, та до них треба ставитись як до штатних ситуацій, оскільки експерт може помилятися або заплановано ушкоджувати систему. Якщо БЗ ЕС велика, то в разі збою знайти, що було його причиною, дуже важко, а якщо з БЗ працює кілька експертів, то ще складніше.

Для покращання функціонування ЕС в процесі роботи з користувачами створює спеціальний кеш та здобуває власні знання. Будемо називати такі знання знаннями другого рівня. Кожна сесія з користувачем впливає на подальшу роботу ЕС з іншими користувачами, та, разом з тим, одна сесія не здійснює суттєвого впливу на знання другого рівня. Тобто ЕС неможливо дезорієнтувати за одну сесію, але цілком можливо за певну кількість сеансів. Ушкодження кешу та знань другого рівня може найбільш відобразитись на системах реального часу. Якщо звичайна ЕС ще в змозі подолати проблеми з кешем та частково обійти хибні знання другого рівня за

умови відсутності обмеження у часі, то для ЕС реального часу це означатиме повну катастрофу, оскільки за умови таких перешкод ЕС може не встигнути розглянути правильну гілку та прийняти вірне рішення.

Отже запропонуємо структуру СБ ЕС, яка була б у змозі подолати описані проблеми.

Будь-які дії з ЕС, які проводяться через інтерфейс самої ЕС та викликають, як наслідок, оновлення БЗ або ЕС, повинні зберігатися у вигляді окремих операцій у спеціальному журналі транзакцій. Так, наприклад, якщо будь-яке знання змінювалося декілька разів, то повинна зберігатися вся історія змін. Це, безумовно, надлишково з точки зору компактності БД, але це єдина можливість у разі необхідності провести розслідування. Ведення журналу по зміні БЗ дозволить відключити певну групу знань та промоделювати процес без неї. У випадку встановлення хибності знань неважко буде знайти, хто їх ввів до БЗ. Щодо зберігання всіх сеансів з користувачем, тут інша ситуація. Сеанси роботи з користувачем необхідно зберігати, але який термін – це вже залежить від конкретної ЕС. Спеціальний евристичний аналізатор ЕС повинен з певною мірою вірогідності відрізняти серію атак від звичайної роботи.

Під евристичним аналізатором будемо розуміти підсистему, що має набір функцій аналізу, робота яких спрямована на виявлення порушень в роботі користувачів з ЕС. Так, наприклад, якщо атака направлена на ушкодження знань другого рівня, то для її подолання в евристичному аналізаторі передбачена спеціальна функція, яка порівнюється з максимальним допустимим рівнем навчання.

Описане вище є тільки внутрішньою СБ ЕС. Крім цього ЕС потребує ще й захисту від несанкційного доступу. Тобто треба забезпечити захист ЕС не тільки від ушкодження. Як не прикро, але це теж можна зробити з терміналу ЕС її ж засобами. Досвідчений користувач в змозі за n сеансів перебрати всі варіанти розвитку подій в ЕС – обійти все дерево знань та тим самим отримати знання ЕС. Завдяки тому, що всі сесії з користувачем зберігаються в журналі, евристичний аналізатор ЕС з певною мірою вірогідності повинен відрізнити перебір БЗ від звичайної роботи.

Таким чином, будь-яка робота/операція з ЕС, направлена на модифікацію БЗ або ЕС повинна реєструватися у журналі операцій. Ведення такого журналу дозволить уникнути не тільки спроби викрасти або пошкодити ЕС, але й суттєво збільшує шанс на локалізацію власних помилок та робить БЗ більш надійною і прозорою.

III Висновки щодо особливостей створення системи безпеки ЕС

ЕС, як будь-яке інше ПЗ, потребує наявності розвиненої специфічної СБ. Ведення протоколів роботи з ЕС дозволяє не тільки знайти та вірно відреагувати на хибні знання, введені експертом, а й не припустити зміни висновків системи внаслідок певної кількості сесій, спрямованих на агресію. Введення в СБ ЕС евристичного аналізатора дозволяє розв'язати питання, які не зачіпаються звичайною СБ. Будь-який розвинений захист можливий тільки за умов постійного аналізу самої ЕС та протоколів роботи з нею. Для того, щоб надійно захистити інтелектуальну систему, необхідна інтелектуальна система захисту. Питання безпеки ЕС потребує глибшого розгляду та розвитку порівняно із звичайним ПЗ.

УДК 681.518.54

МАТЕМАТИЧНИЙ АПАРАТ ДЛЯ ОБГРУНТУВАННЯ ЕКОНОМІЧНОЇ ДОЦІЛЬНОСТІ ВИКОРИСТАННЯ ЕКСПЕРТНИХ СИСТЕМ ПРИЙНЯТТЯ РІШЕНЬ ДЛЯ ЗАХИСТУ ІНФОРМАЦІЇ

Володимир Тарасенко, Антон Михайлюк, Андрій Петрашенко
Національний Технічний Університет України "КПІ"

Анотація: **Співвідношення між ефективністю та вартістю системи захисту інформації може бути розглянуто як критерій її оцінки. За цим методом математична модель аналізує ефективність застосування експертних систем прийняття рішень у галузі захисту інформації, порівнюючи її з традиційним підходом – залученням експертів.**
Summary: **Correlation between effectiveness and cost of information security systems can be served as a criterion for evaluation. Using this method mathematical model analyze effectiveness of expert systems application in branch of guarding, comparing it with traditional approach – attraction of experts.**
Ключові слова: **математична модель, експерт, експертна система.**

При проектуванні і реалізації систем захисту інформації вагоме значення приділяється економічним аспектам проблеми. Одним із критеріїв оцінки доцільності застосування подібної системи може служити співвідношення