УДК 004.621.37 **Домарєв В.В., Герасименко А. В.**

СИСТЕМНИЙ ПІДХІД У ВИРІШЕННІ ЗАВДАНЬ ПО ОРГАНІЗАЦІЇ РОБОТИ ПІДРОЗДІЛУ ТЕХНІЧНОГО ЗАХИСТУ ІНФОРМАЦІЇ НА ПІДПРИЄМСТВІ

Запропоновано типові завдання, які потрібно вирішити у системі організації роботи підрозділу технічного захисту інформації (ТЗІ) для реалізації системного підходу.

Ключові слова: технічний захист інформації, системний підхід, інформаційна безпека, система управління.

Система - це сукупність взаємозалежних елементів, що утворюють цілісність, яка виконує певну функцію. Елементи системи повинні бути взаємозалежними і обов'язково взаємодіяти один з іншим. Різні частини можуть бути об'єднані в «ціле», але це не система, поки не сформований механізм взаємодії компонентів.

При створенні системи треба опиратися не тільки на існуючі технічні засоби, а і враховувати всі правові аспекти, процес управління персоналом та організацію роботи не тільки підрозділу ТЗІ, а й усього підприємства або організації в цілому.

Будь-яка система може розглядатися як підсистема деякої більшої системи.

Для того щоб зрозуміти, як система виконує свою функцію, необхідно дізнатися, яким чином усі її елементи взаємопов'язані один з одним і як вона пов'язана з зовнішнім середовищем.

Після цілеспрямованого об'єднання елементів за принципом «кожен з кожним», система набуває нових специфічних властивостей, які не були притаманні складовим елементам. При цьому первинного значення набувають ті властивості системи, які визначають якість взаємодії її елементів.

Системний підхід у процесах управління інформаційною безпекою в організації роботи підрозділу ТЗІ - це спосіб мислення й аналізу, згідно з яким система організації роботи підрозділу ТЗІ розглядається як сукупність взаємопов'язаних елементів, що мають спільну мету, - забезпечити безпеку інформації

Системний підхід можна застосовувати за допомогою системи організації роботи ТЗІ - це інформаційно-методичний інструмент, системне рішення, призначене для організації взаємодії керівництва установи, підрозділів комп'ютерних (інформаційних) технологій, служби безпеки, фахівців внутрішнього аудиту та інших підрозділів у процесі управління інформаційною безпекою на підприємстві.

Використовуючи системний підхід з точки зору інформаційної безпеки потрібно координованого використання різних за функціями та складом компонентів, таких як: заходи, методи, засоби, механізми, процедури. Ці компоненти вимагають встановлення жорстких логічних та функціональних обов'язків між собою. Саме це дозволяє зробити інформаційно-методичний інструмент.

Система організації роботи ТЗІ використовується для організації процесів управління інформаційною безпекою відповідно до вимог стандартів та інших нормативних документів, дозволяє самостійно організувати роботу із створення системи інформаційної безпеки і легко адаптується для вирішення конкретних завдань забезпечення ІБ з урахуванням особливостей бізнес-процесів на підприємстві і нових задач. Система організації роботи ТЗІ базується на принципах системного підходу до управління ІБ, вона увібрала в себе знання і кращі практики провідних компаній у сфері забезпечення ІБ.

В процесі експлуатації, списки елементів, класифікації у СУ ТЗІ підлягають змінам, що є нормальною частиною процесу інтеграції СУІБ. Зміни можуть бути спричинені передусім розширенням знань про цільову організацію, або змінами в бізнес-процесах чи в структурі організації.

Системний підхід до розробки нормативно-методичних документів є необхідною умовою створення ефективної СУ ТЗІ. Процес управління інформаційною безпекою представлений у вигляді груп модулів які входять до складу моделі СУ ТЗІ.

Зазначені групи модулів ОСНОВИ, ЕТАПИ та НАПРЯМКИ розглядаються нерозривно.

Функціональні можливості СУ ТЗІ.

- Інформаційно-аналітична підтримки рішень керівництва щодо управління процесом забезпечення ТЗІ;
- Оптимізація розподілу ролей і повноважень;
- Розробка і ведення всіх необхідних розпорядчих і регламентних документів ТЗІ: функціональних обов'язків, інструкцій, політик безпеки;
- Проведення аналізу стану ТЗІ та формування звітів для керівництва у вигляді таблиць і графіків;
- Моніторинг ризиків з питань ТЗІ;
- Планування контрольних перевірок;
- Координація діяльності та розподіл ресурсів;
- Контроль виконання завдань та рекомендацій;
- Використання шаблонів методик, описів і робочих документів;
- Забезпечення формування вимог (Матриця вимог) і показників оцінки ефективності СУ ТЗІ (Матриця оцінок).

Структура інформаційно-методичний інструменту «СУ ТЗІ» наведена на рисунку 1.

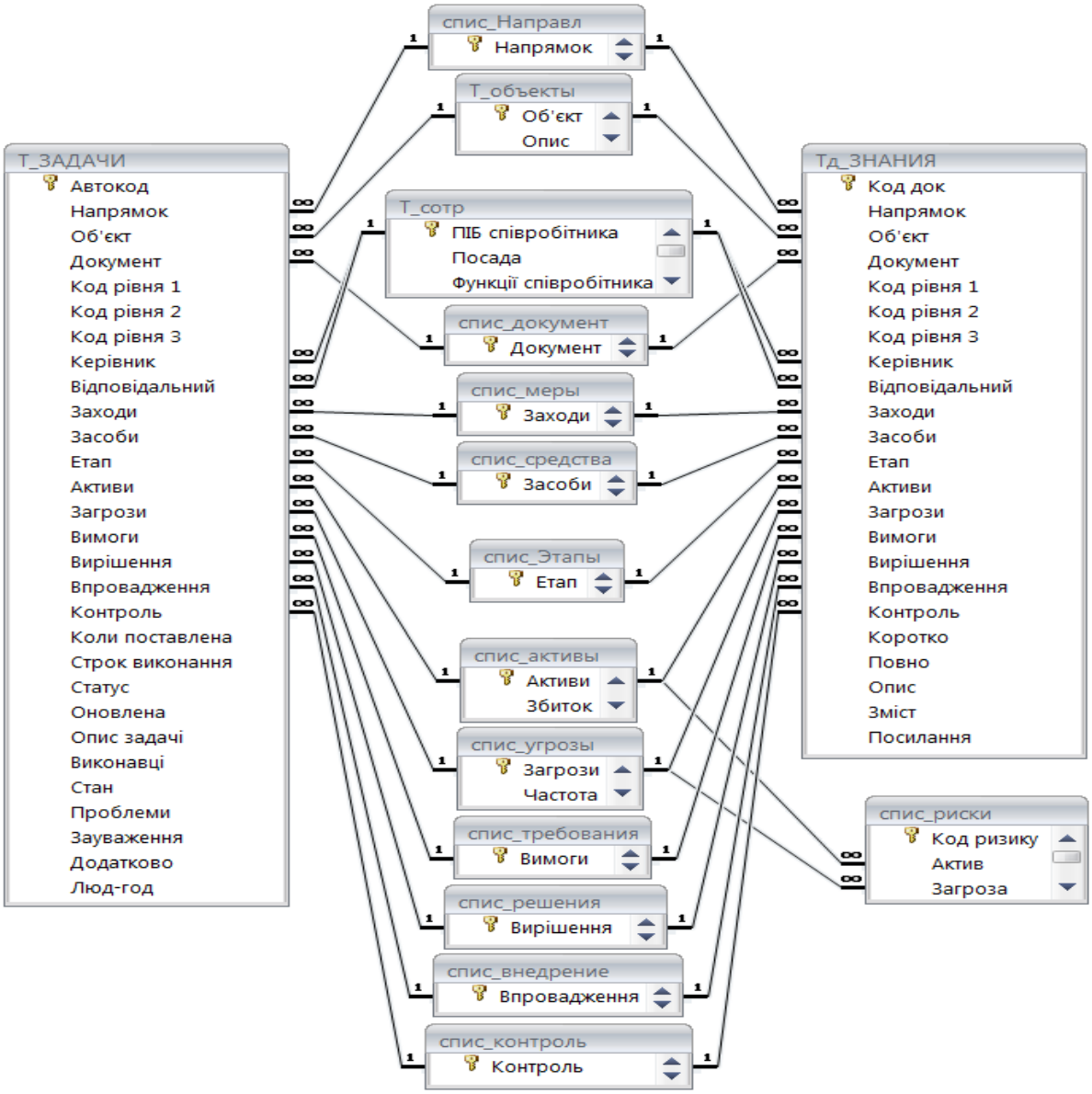

Рис. 1. Структура інформаційно-методичний інструменту «СУ ТЗІ»

Висновки та рекомендації. Використання системного підходу та програмного забезпечення СУ ТЗІ дозволяє вирішувати такі завдання щодо організації роботи підрозділу ТЗІ:

- проводити періодичний аналіз стану технічного захисту інформації підприємства з метою виявлення існуючих недоліків та проблем;
- здійснювати оцінку негативних впливів та загроз технічного захисту інформаці на підприємстві;
- проводити аналіз та узагальнення законодавчих та нормативних актів з метою розробки внутрішніх нормативно-методичних документів щодо організації технічного захисту інформації на підприємстві;

У більшості випадків загрози в галузі ТЗІ реалізуються за рахунок недбалості або незнанням. Для того щоб запобігти цьому, кожен співробітник повинен бути навчений правилам безпеки відповідно до типових завдань:

Створення свідомості ІТ-безпеки. Кожен співробітник повинен бути обізнаним про завдання ІТ-безпеки, які його стосуються.

Розподіл обов'язків і ресурсів. Необхідно надати інформацію про заходи безпеки, яких необхідно дотримуватися щодо розподілу функцій між виконавцями.

Виконання заходів безпеки додатків і систем. Необхідно надати інформацію про заходи безпеки, властиві специфічному продукту.

Дії при виявленні комп'ютерного вірусу в ПК. Співробітники повинні бути проінструктовані про те, як обробити комп'ютерні віруси.

Використання паролів. Необхідно забезпечувати правильне використовування паролів.

Резервування даних і його реалізація. Регулярне резервування даних — один із важливих елементів ІТ-безпеки. Співробітники повинні бути проінструктовані щодо відсутності централізованих функцій резервування даних ПК і про завдання, які за необхідності повинні здійснюватись кожною особою (де дублювання даних доручено кожному користувачу індивідуально).

Захист конфіденційності даних. Персонал повинен бути ознайомлений з вимогами законодавства, заходів, що вживаються, по захисту конфіденційності і транспортуванню (внесення/винесення) даних за межі підприємства.

Заходи у разі позаштатних ситуацій. Усі співробітники (включаючи осіб, не пов'язаних безпосередньо з ІТ) повинні бути проінформовані про встановлені заходи у разі аварійних ситуацій. Це включає інформацію про маршрути виходу/евакуації, правила поведінки на випадок пожежі тощо.

Запобігання витоку інформації через публічні комунікації. Персонал повинен бути проінструктований про небезпеку спілкування відкритими телекомунікаціями (звичайний і мобільний телефон, Інтернет тощо). Типові приклади спроб отримати конфіденційну інформацію - звернення від імені клієнтів або посадовців різних відомств. Персонал повинен бути проінструктований про те, що необхідно перевірити ідентичність партнерів комунікації і не надавати конфіденційну інформацію, зокрема за телефоном.

ЛІТЕРАТУРА

1. Домарев В.В. Защита информации и безопасность компьютерных систем / В.В. Домарев. – К.: ДиаСофт, 1999. - 480с.

2. Домарев В.В. Безопасность информационных технологий. Методология создания систем защиты / В.В. Домарев. – К.: ТИД Диа Софт, 2002. – 688 с.

3. Домарев В.В. Безопасность информационных технологий. Системный поход / В.В. Домарев. – К.: ООО ТИД Диа Софт, 2004. – 992 с.

4. Домарєв В.В. Управління інформаційною безпекою в банківських установах. Теорія і практика впровадження стандартів серії ISO 27k / В.В. Домарєв, Д.В. Домарєв. –Донецьк: Велстар,2012. - 143с.

5. Домарєв В.В. Організація захисту інформації на об'єктах державної та підприємницької діяльності: під. для ВНЗ / В.В. Домарев, С.О. Скворцов. – К: Європейський університет, 2006. - 165с.

Надійшла: 18.03.2013 р.

Рецензент: д.т.н., проф. Розорінов Г.М.