2. Розроблена СКБД дозволяє зручно оперувати даними, що стосуються структури квартир у будинку і розташування датчиків та приладів у квартирах, які використовують системи «розумного» будинку. СКБД спрощує процес редагування параметрів об'єктів даних за допомогою використання розробленого візуального інтерфейсу користувача. Функція емуляції станів сенсорів і приладів зменшує фінансові та часові затрати під час розробки систем «розумних» будинків за рахунок відкидання потреби у придбанні та налаштуванні реальних приладів та сенсорів, емулюючи їхні стани за допомогою розробленої системи.

1. *Meulen R.* Gartner Says 8.4 Billion Connected "Things" Will Be in Use in 2017, Up 31 Percent From 2016 [Електронний ресурс] / Rob Meulen // Gartner. – 2017. – Режим доступу до ресурсу: https://www.gartner.com/en/newsroom/ press-releases/2017-02-07-gartner-says-8-billion-connected-things-will-be-in-use-in-2017-up-31-percent-from-2016.
2. *Kazarian A., Teslyuk V., Tsmots I., Mashevska M.* Units and structure of automated "smart" house system using machine learning algotithms // Proceeding of the 14 th International Conference "The Experience of Designing and Application of Cad Systems in Microelectronics", CADSM'2017, 21-25 February 2017, Polyana, Lviv, Ukraine. 2017. – P. 364 – 366.
3. *Kazarian A., Tsmots I., Teslyuk V.* "Intelligent house as a service and his practical usage for home energy efficiency", in Proc. of the XII-th Intern. Conf. of Computer Science; Information Technologies 2017 (CSIT; 2017). – Lviv, 2017. – P. 220 – 223.
4. *Пасічник В. В.* Організація баз даних та знань / В.В. Пасічник, В.А. Резніченко. – К.: Видавнича група BHV, 2006. 384 с.

Поступила 17.09.2018р.

УДК 004.451.36:681.5

В. І.Сабат, П.І. Шепіта, Львів

ФУНКЦІОНАЛЬНА МОДЕЛЬ СИСТЕМИ ЗАХИСТУ АВТОМАТИЗОВАНОЇ СИСТЕМИ ДОКУМЕНТООБІГУ

Анотація. У статті запропоновано методи створення функціональної моделі системи захисту в автоматизованих системах документообігу (АСДО) та проаналізовано взаємозв'язки між основними структурними елементами дослідженої моделі.

Ключові слова: системи документообігу, системи захисту, функціональна модель.

Вступ. Надійне функціонування будь-якої інформаційної системи (ІС) безпосередньо пов'язане із впровадженням заходів безпеки та захисту такої системи від зовнішніх атак і несанкціонованих вторгнень.

Для захисту від загроз інформаційній безпеці АСДО і зменшення ризиків необхідно реалізувати низку захисних заходів на етапах проектування і впровадження АСДО у виробництво, а також тих, що стосуються безпосередньої роботи АСДО. Важливість таких заходів очевидна, бо неможна передбачити усіх загроз системи захисту, не перевіривши їх у процесі практичної реалізації. Тому для більш наближеного аналізу необхідно вдаватись до моделювання, моніторингу, тестування та аудиту системи захисту і, відповідно, корекції та вдосконалення таких систем.

Методи функціонального IDEF0-моделювання дозволяють вирішувати багато проблем в роботі ІС завдяки аналізу взаємозв'язків між структурними елементами та блоками досліджуваної області і вносити відповідні корективи у процесі функціювання таких систем. [1]

Основна частина. При дослідженні та створенні АСДО, можна виділити три основних етапи обігу документів, на яких необхідно розробити план та стратегію захисних дій та засобів. До таких етапів функціонування АСДО можна віднести:

— проектування документів;
— робота з документами;
— архівування документів.

Комплекс захисних заходів узгоджується з цілями і завданнями системи безпеки АСДО і визначається в процесі проектування таких систем. Для більш адекватного визначення рівня безпеки доцільно періодично проводити моніторинг системи захисту, при цьому основна увага приділяється аудиту та аналізу загроз і вразливостей, що у своїй сукупності формують поняття ризику. Завдяки процесу оцінювання рівнів ризику на усіх етапах функціонування АСДО встановлюється і загальний рівень безпеки для ІС.

Для більш наочного відображення функціональних зв'язків між основними структурними блоками, які входять в систему захисту (СЗ), а також визначення місця СЗ у загальній моделі АСДО, скористаємось поширеним на сьогодні IDEF0-моделюванням. Узагальнену модель системи захисту для АСДО можна представити у вигляді функціональної моделі верхнього рівня (рис. 1).

Рис. 1. Функціональна модель системи захисту АСДО верхнього рівня

Для управління системою захисту (СЗ) на етапі проектування АСДО розробляється політика безпеки, у якій визначаються цілі і завдання безпеки на усіх етапах документообігу. Прописані в політиці безпеки завдання для організації, у якій планується впровадження АСДО, реалізуються у вигляді окремих положень, інструкцій та процедур. Кожна процедура має розділ, що описує її сферу призначення. Наприклад, процедури політики технічної безпеки застосовуються до всіх комп'ютерних і мережних систем. Інформаційна політика містить перелік процедур та інструкції, які застосовуються до всіх службовців та користувачів. При цьому визначається секретна інформація всередині організації і способи її захисту. Політика розробляється так, щоб охопити всю існуючу інформацію. Кожен службовець відповідає за безпеку секретної інформації, з якою він стикається в роботі. Документи можуть бути представлені на паперових носіях або у вигляді файлів на комп'ютері, тому в описаних процедурах повинен передбачатись захист для всіх форм представлення інформації.

Реалізацію механізмів управління СЗ для АСДО здійснює спеціально навчений персонал системи безпеки (СБ) через служби безпеки, моніторингу та адміністрування системи захисту. Необхідність функціонування таких служб, навчання персоналу СБ та груп моніторингу проводиться згідно з регламентованими у політиці безпеки інструкціями та процедурами. Від фахового рівня персоналу СБ залежить надійність функціонування системи захисту у будь-якій організації, яка працює з секретними документами. Тому механізмам управління СЗ приділена особлива увага на етапі розробки політики безпеки і зокрема в процесі її функціонування.

Вхідними даними функціональної моделі СЗ є:

— вхідні дані від користувачів, які ініціюють процес створення нових документів (заявки, службові записки, скарги, вимоги тощо);
— зовнішні атаки — зловмисні та незловмисні дії та акти, які можуть призвести до негативних наслідків роботи АСДО та СЗ і, відповідно, до збитків для відновлення вказаних систем;
— оновлення даних — інформація, що оновлюється для санкціонованих програмних продуктів, передбачених політикою безпеки (операційна система, прикладні програми, антивірусний захист тощо);
— інформація про зміни системи захисту — нормативні акти, положення Законів України, відомості, які регламентують процеси проектування та вдосконалення систем захисту для підприємств і організацій [2].

На виході функціональної моделі СЗ є:

— вихідні дані для реалізації процесу створення нового документу, після перевірки автентичності замовника з бази даних (БД), або визначення його статусу як «новий користувач» з введенням його відповідних реквізитів у БД;
— інформація на відновлення АСДО після інциденту. Якщо на початку реалізації атаки її не можна було локалізувати та нейтралізувати засобами системи захисту, і в результаті чого ІС перейшла в аварійний

стан роботи, тоді служба захисту видає план дій для усунення наслідків після інциденту, передбачений політикою безпеки;

— дані оперативного оновлення — інформація про оновлення сертифікованих програмних продуктів АСДО, яка перевіряється системою захисту на автентичність і цей процес фіксується у реєстраційному журналі системного адміністратора;

— зміни в політиці безпеки — інформація про необхідність вдосконалення політики безпеки підприємства, що виникає внаслідок зовнішніх змін регламентованих для СЗ а також в результаті моніторингу і виявлення нових загроз та вразливостей АСДО.

Після декомпозиції функціональної моделі системи захисту АСДО можна проаналізувати взаємозв'язки між основними структурними блоками інформаційної системи (рис. 2).

На рис. 2 представлено такі основні функціональні блоки моделі системи захисту:

— система управління доступом — базується як на фізичному так і на технічному доступі до інформації що міститься в документах, а також до самих документів. Успішна робота цієї системи залежить від служби ідентифікації і автентифікації користувачів та службовців. Секретність інформації, як було вищезазначено, визначається у політиці безпеки організації, а система управління доступом встановлює рівні доступу до неї для усіх суб'єктів АСДО;

— база даних АСДО — містить інформацію про користувачів та службовців системи, масив документів та інформацію з рівнями доступу до них, архівні дані тощо. При виявленні нових користувачів і проходженні процедур реєстрації, їхні дані також вносяться в базу даних, про що інформується система управління доступом;

— технічні та інформаційні засоби безпеки — включають технічні засоби захисту різноманітних активів підприємства (апаратної та програмної частини ПК, мережного обладнання, устаткування тощо) а також інформаційну складову засобів безпеки;

— політика безпеки АСДО — встановлюються на етапі проектування СЗ з врахуванням інформаційних, технічних та соціальних правил, прав та обов'язків усіх суб'єктів ІС. Описується на рівні процедур та інструкції і поширюється на всю систему захисту. В процесі функціонування і розширення ІС політика безпеки може змінюватись та вдосконалюватись.

— служби безпеки — базові компоненти системи захисту. Основне їхнє призначення — це протидія зовнішнім та внутрішнім атакам на ІС [3];

— служби моніторингу — виконують функцію сканування системи на наявність вразливих місць та загроз. До них також входить аудит системи захисту. При наявності слабких місць в системі захисту служби можуть ініціювати підвищення рівня безпеки і зміни в політиці безпеки.

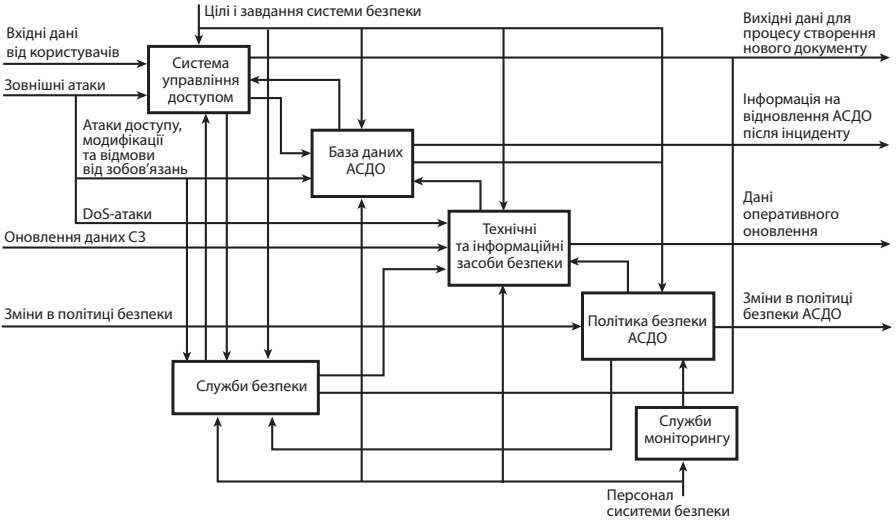

Рис. 2. Функціональна модель системи захисту АСДО другого рівня

Аналізуючи функціональну модель системи захисту (рис. 2), можна простежити напрямки основних атак на АСДО. Насамперед це атаки доступу модифікації та відмову від зобов'язань, які спрямовані на систему управління доступом. Протидіяти таким атакам можуть відповідні служби інформаційної безпеки: служба конфіденційності, служба цілісності і служба ідентифікації. До атак на базу даних АСДО можна віднести: атаки доступу, атаки модифікації та атаки на відмову від зобов'язань. Захист баз даних також здійснюється через відповідний контроль та відслідковування вищевказаних служб.

На технічні та інформаційні активи АСДО можливі зовнішні атаки на відмову в обслуговуванні (DoS-атаки). Для протидії таким атакам зазвичай використовують служби доступу та ідентифікації. DoS-атаки особливо поширені через мережні технології і найбільш непрогнозовані та важко контрольовані системами захисту при функціонуванні ІС. Тому важливо при проектуванні систем захисту для ІС враховувати засоби протидії таким атакам (мережні шлюзи, міжмережні екрани, комутатори і т.д.).

Відстежування (моніторинг) мережі АСДО на предмет наявності підозрілої активності є необхідною і обов'язковою дією. Ця дія включає як аудит, так і моніторинг мережі і системи у реальному часі. Зазвичай таке відстеження розділяється на аудит і виявлення вторгнень.

Висновок. На етапі проектування системи захисту АСДО доцільно провести функціональний аналіз її структурних компонентів і визначити їхнє місце в інформаційній системі організації. Надійне функціонування будь-якої організації буде залежати від проведеного аналізу та прийнятих заходів та засобі безпеки, які обумовлюються в політиці безпеки. Для такого аналізу найбільш підходить використання графічних функціональних моделей.

1. Знакомство с нотацией IDEF0 и пример использования. Блог компании Trinion [з мережі] 28.02.2017 р. https://habr.com/company/trinion/blog/322832/
2. Закон України «Про інформацію» [з мережі] http://zakon.rada.gov.ua/laws/show/2657-12/ed20110106.
3. *Сабат В. І.* Особливості захисту інформації в автоматизованих системах документообігу / В. І. Сабат. // Збірник наукових праць, випуск 70, ІПМЕ ім. Г. Є. Пухова НАН України. — К., 2014. — С. 119–123.

Поступила 10.09.2018р.

УДК 004.65: 004.5

В.Я.Коваль, асистент кафедри ІСТ, ІППТ, НУ “Львівська політехніка”,
М.А.Вовчок, магістр кафедри САП НУ “Львівська політехніка”,
Р.В.Чубінський, магістр кафедри САП НУ “Львівська політехніка”,
В. М.Теслюк, д.т.н., проф. кафедри ІСТ, ІППТ, НУ “Львівська політехніка”.

СТРУКТУРНА МОДЕЛЬ ТА ІНФОРМАЦІЙНЕ ЗАБЕЗПЕЧЕННЯ СИСТЕМИ ТЕХНОЛОГІЧНОЇ ПІДГОТОВКИ ПОЛІГРАФІЧНОГО ВИРОБНИЦТВА

Abstract. The structural scheme and the database of the system of technological preparation of polygraphic production have been developed. The model was constructed on the basis of theory of Petri nets. Model used to study the dynamics of the system of technological preparation of polygraphic production.

Анотація. Розроблено структурну схему та базу даних системи технологічної підготовки поліграфічного виробництва. Побудовано модель на основі теорії мереж Петрі, яка використовується для дослідження динаміки роботи системи технологічної підготовки поліграфічного виробництва.

Актуальність

Гострою проблемою сучасних поліграфічних підприємств є вдосконалення управління виробництвом на основі застосування сучасних інформаційних технологій. Досвідчені фахівці поліграфічної галузі обґрунтовують можливість підвищення рівня управління шляхом створенням інтегрованої системи, здатної до поєднання різних інформаційних потоків на підприємстві та оперативного опрацювання достовірних даних для прийняття оптимальних управлінських рішень [1].

У зв’язку з ростом складності та інтенсивним розвитком технологій, зокрема на операціях складання, верстки, спуску сторінок, інформаційні технології вже тривалий час використовуються у технологічних процесах поліграфічного виробництва. Автоматизація поліграфічного обладнання,

