УДК 004.7(045)

**Домарєв В. В.,** к.т.н.; **Домарєв Д. В.**; **Гордієнко С. Б.,** к.т.н.
*(Державний університет інформаційно-комунікаційних технологій)*

# ОБГРУНТУВАННЯ ОСНОВНИХ ФУНКЦІЙ СИСТЕМИ УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ

**Домарєв В. В., Домарєв Д. В., Гордієнко С. Б**. **Обгрунтування основних функцій системи управління інформаційною безпекою.** Проведено аналітичний огляд міжнародних та українських нормативних документів для визначення вимог до ефективної системи управління інформаційною безпекою (СУІБ). Приведений перелік обов'язкових документів СУІБ, розглянуті питання реалізації системи управління вмістом для СУІБ, оцінювання інформаційної безпеки і забезпечення внутрішнього аудиту. Виходячи з розглянутих вимог сформульовано перелік функцій ефективної СУІБ.
***Ключові слова:*** ІНФОРМАЦІЙНА БЕЗПЕКА, УПРАВЛІННЯ, СУІБ, ISO27K

**Домарев В. В., Домарев Д. В., Гордиенко С. Б. Обоснование основных функций системы управления информационной безопасностью.** Проведен аналитический обзор международных и украинских нормативных документов для определения требований к эффективной системе управления информационной безопасностью (СУИБ). Приведен перечень обязательных документов СУИБ, рассмотрены вопросы реализации системы управления содержанием для СУИБ, оценивания информационной безопасности и обеспечения внутреннего аудита. Исходя из рассмотренных требований сформулирован перечень функций эффективной СУИБ.
***Ключевые слова:*** ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ, УПРАВЛЕНИЕ, СУИБ, ISO27K

**Domariev V. V., Domariev D. V., Gordienko S. B. Definition of the effective information security management system features.** Analytical overview of international and ukrainian legal documents is performed to define the demands to an effective information security management system (ISMS). The mandatory ISMS documents, content management system for an ISMS, information security metrics and internal audit capabilities are highlighted. The features of an effective ISMS are formulated according to the reviewed demands.
***Keywords:*** INFORMATION SECURITY, MANAGEMENT SYSTEM, ISMS, ISO27K

**Постановка задачі. Актуальність.** Національний банк України запровадив два галузеві стандарти управління інформаційною безпекою (ІБ) [1]. Документи [2, 3] визначають вимоги і правила впровадження системи управління інформаційною безпекою та дублюють міжнародні стандарти управління інформаційною безпекою ISO/IEC 27001 та ISO/IEC 27002.

Тенденція приваблення іноземних інвестицій змушує комерційні організації впроваджувати міжнародні стандарти управління, в тому числі і стандарти управління інформаційною безпекою. Ці факти пояснюють підвищення попиту на впровадження систем управління інформаційною безпекою на українських підприємствах.

Система управління інформаційною безпекою (СУІБ) – частина загальної системи управління, яка ґрунтується на підході, що враховує бізнес-ризики. Загальне призначення СУІБ – розроблення, впровадження, функціонування, моніторинг, перегляд, підтримування та вдосконалення інформаційної безпеки (ІБ) [2].

**Політика інформаційної безпеки.** Під політикою інформаційної безпеки слід розуміти набір законів, правил, обмежень, рекомендацій і т. ін., які регламентують порядок обробки інформації і спрямовані на захист інформації від певних загроз. Термін "політика безпеки" може бути застосовано до підприємства, інформаційної системи, окремого персонального комп'ютера (ПК) і т. ін.

Політика інформаційної безпеки в інфокомунікаційній системі (ІКС) є частиною загальної політики безпеки організації і може успадковувати, зокрема, положення державної політики у галузі інформаційної безпеки. Для кожної ІКС політика безпеки інформації може бути індивідуальною і може залежати від використовуваної технології обробки інформації, , особливостей операційної системи, фізичного середовища і від багатьох інших чинників.

ІКС може реалізовувати декілька різноманітних технологій обробки інформації. Тоді і політика безпеки інформації в такій ІКС буде складеною з частин, що відповідають різним технологіям та іншим особливостям. Очевидно, що для різних ІКС відповідні системи (політики) інформаційної безпеки можуть істотно відрізнятись.

Політика безпеки повинна визначати ресурси ІКС, що потребують захисту, зокрема установлювати категорії інформації, оброблюваної в ІКС. Як складові частини загальної політики інформаційної безпеки в ІКС мають існувати політики забезпечення конфіденційності, цілісності і доступності оброблюваної інформації.

**Обов'язкові документи СУІБ.** Галузеві стандарти України "ГСТУ СУІБ 1.0/ISO/IEC 27001:2010" [2] та "ГСТУ СУІБ 2.0/ISO/IEC 27002:2010" [3] містять певні вимоги до СУІБ. Документ [4] підсумовує ці вимоги.

Головним чином, СУІБ має працювати, спираючись на існуючі політики. В іншому випадку, політики можуть бути розроблені в процесі впровадження або функціонування СУІБ. В [5] пропонуються наступні обов'язкові документи СУІБ:

1. Записи ключових управлінських рішень стосовно СУІБ;
2. Набір політик інформаційної безпеки, у тому числі політика СУІБ і політика ІБ;
3. Опис сфери впливу СУІБ;
4. Опис заходів ІБ;
5. Документація контролів (засобів захисту, які охоплюють політику, заходи, настанови, втілення або організаційні структури [3]);
6. Методи оцінки ризиків;
7. Звіти оцінки ризиків;
8. Інструкції щодо дій відносно ризиків;
9. Оперативні заходи СУІБ;
10. Оцінки ІБ;
11. Звіт відповідності;
12. Заходи з контролю документів;
13. Заходи з контролю записів;
14. Записи ознайомлення з умовами безпеки, навчальні матеріали, а також матеріали ознайомлення з інформаційною безпекою, звіти з оцінками навчання та відгуками;
15. Плани та заходи внутрішнього аудиту СУІБ, а також звіти з аудиту СУІБ, погоджені плани дій і звіти з планових заходів, перевірок, припинення;
16. Заходи з виправлення невідповідностей;
17. Заходи із запобігання невідповідностям.

**Система управління вмістом для СУІБ.** СУІБ може використовувати систему управління вмістом для забезпечення обміну інформацією, наприклад, висновками аудиту, політиками і т.п. Система управління вмістом має бути обрана з врахуванням особливостей підприємства. Рекомендовано застосовувати метод структурованої специфікації та оцінки (як для вибору методів управління та аналізу ризиків).

Існують безкоштовні (з відкритим вихідним кодом) і комерційні продукти, розроблені для підтримки СУІБ. Їх можна поділити на наступні типи:

1. Системи управління вмістом (Content Management Systems, CMS);
2. Системи управління документами (Document Management Systems, DMS);
3. Системи управління навчанням (Learning Management Systems, LMS);
4. Системи управління політиками (Policy Management System, PMS).

Система управління вмістом є необов'язковою для СУІБ, і обмін інформацією може підтримуватись безпосередньо СУІБ, або виконуватись вручну для відносно малих підприємств чи на рівні вищого керівництва.

**Оцінювання інформаційної безпеки.** Якість ІБ може бути оцінена по різноманітним параметрам – від кількості заблокованих повідомлень спаму до ступеня досягнення стратегічних цілей. Відносно СУІБ, для оцінки ефективності доцільно використувати так звані управлінські категорії: кількість завершених завдань нижчого рівня, умовне значення ризику, який відвернутий заходом безпеки і т.п. Така оцінка забезпечує краще розуміння на рівні вищого керівництва.

**Функції забезпечення внутрішнього аудиту.** Друга найважливіша мета впровадження СУІБ окрім забезпечення прозорого управління підприємством – отримання сертифікату відповідності одному або декільком стандартам ІБ (наприклад, ISO27k, CobiT, PCI DSS).

Процес сертифікації включає зовнішній аудит корпоративної системи інформаційної безпеки для визначення відповідності стандарту(ам). Щоб гарантувати успіх зовнішнього аудиту, підприємство може влаштувати внутрішній аудит безпеки до початку процесу сертифікації.

Оскільки СУІБ зберігає та обробляє найважливішими даними оцінки безпеки, впровадження відповідних функцій може значно полегшити перебіг внутрішнього аудиту.

**Висновок.**

Враховуючи зазначені вимоги до СУІБ, сформульовані наступні необхідні функції програмного продукту для управління інформаційною безпекою: *представлення* для керівників високого рівня завдяки простим інтерфейсам та звітам, орієнтованим на вище керівництво; *відстеження і управління* ризиками ІБ на підприємстві з негайною переоцінкою в разі будь-яких змін в наборах активів чи загроз; *планування* зовнішнього або внутрішнього аудиту, контроль процесу аудиту за допомогою зведених звітів; *реєстрація* порушень, відхилень та зауважень в процесі аудиту шляхом подання потрібної інформації в спеціальному звіті; *використання* шаблонів для політик, описів та інших робочих документів (ці шаблони повинні відповідати державним стандартам України); *створення і зберігання* всіх необхідних настановних та регулюючих документів ІБ (функціональні обов'язки, інструкції, політики безпеки і т.п.) шляхом зберігання, оновлення та включення інформації щодо ІБ в установі безпосередньо до документів; *підтримання* спільних баз знань та методичних матеріалів, архівація для забезпечення управлінських рішень фактичними даними; *проведення* аналізу стану ІБ і створення звітів для правління у вигляді зрозумілих таблиць і діаграм, оскільки представити інформацію щодо ІБ неспеціалістам зазвичай проблематично; *раціональний розподіл* ролей, повноважень і ресурсів між співробітниками та завданнями; *інформативно-аналітична підтримка* рішень правлінням організації відносно управління ІБ, тому що за наявності зрозумілої та об’єктивної інформації приймати раціональні рішення легше; *забезпечення формування вимог* до СУІБ та оцінок її ефективності, що важливо в контролі досягнення встановлених цілей; *оцінка і управління* бюджетом створення і експлуатації СУІБ, щоб контролювати витрати на СУІБ, чи на ІБ організації взагалі; *відстеження* виконання завдань і надання рекомендацій для підвищення загальної продуктивності проектів.

**Література**

1. Про набрання чинності стандартами з управління інформаційною безпекою в банківській системі України ; постанова правління Національного банку України від 28 жовтня 2010 р. № 474. – К.: Національний банк України, 2010.

2. Інформаційні технології. Методи захисту. Система управління інформаційною безпекою. Вимоги (ISO/IEC 27001:2005, MOD). ГСТУ СУІБ 1.0/ISO/IEC 27001:2010. – К.: Національний банк України, 2010. – 49 с.

3. Інформаційні технології. Методи захисту. Звід правил для управління інформаційною безпекою (ISO/IEC 27002:2005, MOD). ГСТУ СУІБ 2.0/ISO/IEC 27002:2010. – К.: Національний банк України, 2010. – 163 с.

4. ISO/IEC 27000 series FAQ – ISO27k Forum [Електронний ресурс]. – Режим доступу: http: // www.iso27001security.com/ html/ faq.html.

5. Salah O. Mandatory Information Security Management System Documents Required for ISO/IEC 27001 Certification [Електронний ресурс] / O. Salah, G. Hinson. – Режим доступу: http: // www.iso27001security.com/ ISO27k_mandatory_ISMS_documents.rtf.