АНАЛІЗ ПЕРСПЕКТИВНИХ СТАНДАРТІВ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Айвазова К.Б.[1], Мацків О.І.[2], к.е.н.
1 - Одеська державна академія технічного регулювання та якості,
2 – Одеський національний економічний університет,
м. Одеса

У доповіді, опираючись на зарубіжні публікації, проведено огляд нормативних та законодавчих документів, які регулюють технології аудиту інформаційної безпеки організацій. Показано, що закони продовжують розроблятися та удосконалюватися. Визначено, що актуальним питанням є вимоги до практичних дії зі сторони організацій щодо контролю за дотриманням вимог до інформаційної безпеки. Відзначено, що актуальним питанням є порядок визначення, чи виконують організації всі необхідні заходи з інформаційної безпеки. Приділено увагу бібліотеці інфраструктури ITIL, про що йде мова нижче.

Корисним інструментом, який може використовуватися для вдосконалювання системи інформаційної безпеки (ІБ), є бібліотека інфраструктури ІТ (*IT Infrastructure Library* – ITIL) – набір оптимальних методів та принципів, які визначають інтегрований, заснований на процесах підхід з управління ІТ. Зацікавленість у застосуванні ITIL постійно росте по усьому світу.

ITIL рекомендує впровадження ефективних заходів в області ІБ на стратегічному, тактичному та операційному рівнях. Забезпечення ІБ розглядається як циклічний процес з фазами планування, впровадження, оцінки та підтримки. ITIL оперує такими поняттями в області ІБ, як політики, процеси, процедури та інструкції. З деякими особливостями аналогічні підходи прослідковуються в COBIT, а також у вітчизняних нормативних та законодавчих актах. Хоча в ITIL відсутні безпосередні спеціалізовані стандарти оцінки відповідності, він є близьким до британського стандарту BS 15000, який присвячений управлінню ІТ-сервісами та методам їх оцінки.

Оцінку якості аудиторів, відповідно до BS 15000, здійснює Британське агентство акредитації (United Kingdom Accreditation Service – UKAS). UKAS встановлює основні вимоги відносно аудиторів у частині навчання, кваліфікації, наявності досвіду роботи у сертифікаційних компаній. Крім того, UKAS регулярно проводить аудит сертифікаційних компаній з метою переконатися, що вони можуть документально підтвердити свою компетентність по проведенню сертифікаційних аудитів. BS 15000 містить докладні керівництва для організацій, які бажали б отримати сертифікацію, і вимоги відносно аудиторів.

В 2005 році стандарт BS 15000 був представлений в ISO і по завершенню прискореної та спрощеної процедури він був прийнятий, як ISO/IEC 20000.

Ще одним широко обговорюваним стандартом в області безпеки, є стандарт ISO/IEC 15408 «Загальні критерії ІБ ІТ», який був гармонізований, наприклад, у Росії, як державний стандарт Р ИСО/МЭК 15408. Цей стандарт технічний і іноді важкий для сприйняття бізнесом. Він корисний для постачальників та покупців продукції ІБ, для того щоб визначити, наскільки достатнім є механізм захисту в продукції, що випробовується. На жаль, він не

допомагає керівництву розібратися, чи правильно воно діє, забезпечуючи той чи інший рівень ІБ.

Область застосування ISO/IEC 15408 з метою відповідності регулюючим вимогам, є досить обмеженою. Однак існують виключення, зокрема в області процесінгу платіжних карт, де певні технічні вимоги стандарту зустрічаються, наприклад, у програмах перевірки на відповідність вимогам в області безпеки з боку платіжної системи Mastercard.

Найбільш відомими та широко використовуваними стандартами управління ІБ, а також доказом дотримання нормативних актів та законодавства, є міжнародні стандарти серії ISO/IEC 2700X по управлінню ІТ. Беручи свій початок від первісних Британських стандартів серії 7799 (далі – ISO/IEC 17799 та ISO/IEC 27001), ці стандарти конкретно та чітко визначають технології ефективного впровадження систем управління ІТ. Є кілька причин, чому ці стандарти настільки популярні. Не останньою з них є та, що в них чіткі вказані методи проведення аудиторських перевірок на відповідність, а також можливість сертифікації по ISO/IEC 27001.

ISO/IEC 17799 та ISO/IEC 27001 допомагають відповістити на запитання: «як довести, що в організації забезпечений необхідний рівень безпеки?» і переконати регулювальні органі, що «усе виконується правильно» та «належним чином».

ISO/IEC 17799 та ISO/IEC 27001 охоплюють всі основні сфери вимог, які пропонуються законодавством та нормативними актами, згаданими вище. Наріжним каменем відповідності стандартам є розуміння того, які інформаційні активи має організація, і впровадження необхідного рівня заходів контролю, заснованого на оцінці ризиків.

ISO/IEC 17799 та ISO/IEC 27001 – це просто та доступно написані стандарти, що надають корисні методики з заходів контролю, які організація захоче впровадити. При цьому стандарти зрозумілі як фахівцям в області ІБ, так і керівництву. Вони допомагають подолати комунікаційний бар'єр між обома сторонами, забезпечивши тим самим розуміння керівництвом, що робиться та чому. Керівництво розглядається стандартом як ключова ланка при постановці цілей в області ІБ.

Для того щоб бути сертифікованою по ISO/IEC 27001, організація повинна довести, що в неї існують процедури по ідентифікації законів та нормативних актів, що стосуються її з погляду захисту інформації. Крім того, у неї повинна існувати програма по дотриманню цих нормативних вимог. Тоді сертифікація по ISO/IEC 27001, якщо вона проведена належним чином, гарантувала б, що організація на ділі дотримує всі законодавчі та нормативні вимоги, які регулюють її діяльність.

Додаток А стандарту ISO/IEC 27001 містить перелік заходів контролю, які повинні бути впроваджені в організації, яка бажає пройти сертифікацію. Однак, слід зазначити, не всі заходи контролю з даного списку обов'язково повинні бути впроваджені, якщо з цього питання існує документально підтверджене рішення керівництва, засноване на оцінці ризиків. Багато компаній використовують ISO/IEC 27001 як засіб самооцінки, оскільки методик по проведенню оцінки безпеки недостатньо. Деякі компанії прагнуть пройти офіційний сертифікаційний аудит в акредитованих незалежних аудиторських

організаціях. Аналогічно BS 15000, описаному вище, організації, які проводять сертифікаційний аудит, повинні бути акредитовані відносно стандарту BS 7799 (част. 2) органом UKAS у Великобританії. У міру приведення британських стандартів у статус міжнародних (ISO), акредитація також стає можливою через органи ISO.

В документі ЕА-7/3 «Акредитація організацій, що займаються сертифікацією систем управління ІБ» Європейської комісії з акредитації, перераховані основні вимоги в області незалежності, кваліфікації та внутрішньої системи контролю якості відносно таких організацій. Ці вимоги до якості процесу сертифікації та кваліфікації аудиторів обумовлені необхідністю довіри до результатів сертифікації.

Сертифікація по стандартах також вимагає проведення регулярних аудиторських перевірок з метою забезпечення та підтримки відповідності виконання вимог, та для того, щоб процес управління безпекою функціонував належним чином. Це скорочує розрив, який у даний момент існує в більшості законодавчих актів: як довести регулювальним органам, що організація постійно дотримує вимог законодавства?

Сертифікація полегшує співробітникам служби безпеки отримання фінансування на підтримку програми управління безпекою, і не тільки на сам сертифікаційний аудит, але й на весь комплекс заходів в області безпеки.

У деяких країнах дотримання ISO/IEC 17799/BS 7799:2 у ряді галузей економіки є обов'язковим (наприклад, у Японії).

Регулювальні органи опираються на процес сертифікації по стандарту, як на достатню умову задоволення потреб галузі в захисті інформації. Можливо, інші країни будуть наслідувати цей приклад завдяки тому, що стандарт широко використовується як інструмент впровадження безпеки; він зрозумілий, а механізми його виконання (сертифікація) чітко встановлені.

Зазвичай, керівництво підприємства прагне знати, наскільки воно «розумно» діє в області ІБ. Керівництво також повинне могти забезпечити впровадження рішень, які б відповідали потребам бізнесу з погляду складності, організації робіт та витрат. Багато із законодавчих актів, яких необхідно дотримуватися, вимагають підходу, заснованого на оцінці ризиків, і не пропонують до застосування конкретні технології. Втім, інтуїтивно зрозумілим є той факт, що гарний стандарт не повинен пропонувати ту або іншу технологію або конкретні процедури контролю: він повинен бути досить гнучким, щоб дозволити будь-якій компанії дотримуватися вимог стандарту. Він повинен ґрунтуватися на оцінці ризику та повинен враховувати те, що завдання організації – це не забезпечення безпека, а ведення комерційної діяльності: у більшості випадків – заробляння грошей. Тому стандарт повинен забезпечувати гнучкість керівництву в прийнятті рішень, пов'язаних з безпекою, з урахуванням вимог бізнесу. Не все, що ризиковано, повинне бути заборонене: просто повинно бути більше різноманітних заходів контролю, що компенсують ризики. Т.ч., гарний стандарт повинен відображати потреби підприємств у розвитку.

Література

1. Казакова Н. Ф. Міжнародна регламентація правового регулювання та стандартизації аудиту інформаційної безпеки [Текст] / Н. Ф. Казакова,

Е. А. Плешко, К. Б. Айвазова // Вісник Східноукраїнського національного університету імені Володимира Даля. – 2013. – № 15(204). – Т. 1. – С. 172-181.

2. Удосконалення принципів та методів інформаційного забезпечення, інформаційної та фінансово-економічної безпеки підприємств та організацій сфери економіки, бізнесу та фінансів [Звіт про НДР] : (проміжн.) / О. О. Скопа, Н. Ф. Казакова, О. В. Орлик, Ю. В. Щербина, А. О. Петров, С. Л. Волков, О. І. Мацків, О. Г. Єсіна, А. Ю. Вакула, О. О. Фразе-Фразенко, А. В. Мінін, О. О. Йона, Є. В. Вавілов, К. Б. Айвазова // ОНЕУ ; кер. О. О. Скопа. – 0112U007713. – Одеса, 2013. – 236 с.
3. Petrov A. Analiza stanu bezpieczeństwa ekonomicznego w sferze nowoczesnej ekonomii i biznesu [Текст] / Anton Petrov, Mikołaj Karpiński, Nadiya Kazakova // Zeszyty Naukowe Wyższej Szkoły Finansów i Prawa. – Bielsko-Biała : Wyższa Szkoła Finansów i Prawa. – 2013. – № 4. – S. 27-38.
4. Зеленцова Ж. Ю. Конвергенция глобальной сети как новый этап развития: обзор инфраструктурных решений и технологий с целью нахождения решений для повышения безопасности обработки данных при облачных вычислениях [Текст] / Ж. Ю. Зеленцова, Н. Ф. Казакова // Інформаційна безпека. – 2013. – № 4 (12). – С. 23-40.
5. Зеленцова Ж. Інфраструктурні рішення та технології підвищення безпеки обробки даних при хмарних обчисленнях [Текст] / Ж. Зеленцова, Н. Казакова // Захист інформації і безпека інформаційних систем : ІІІ міжнар. наук.-техн- конф., 5-6 червня 2014 р. : матер. конф. – Львів, НУ «Львівська політехніка. – С. 58-59.
6. Казакова Н. Ф. Принципи побудови захищених інтелектуальних мереж [Текст] / Н. Ф. Казакова // Вісник ДУІКТ. – 2009. – № 4. – Т. 7. – С. 381-388.
7. Казакова, Н. Ф. Доповнення до концепції інформаційної безпеки [Текст] / Н. Ф. Казакова // Сучасна спеціальна техніка. – 2010. – № 3(22). – С. 74-80.
8. Казакова, Н. Ф. Проблеми правового забезпечення захисту баз даних [Текст] / Н. Ф. Казакова, Ю. В. Щербина // Інформаційна безпека. – 2012. – № 2(8). – С. 73-76.
9. Йона О. О. Світові тенденції боротьби з кіберзлочинністю [Текст] / О. О. Йона, Н. Ф. Казакова // Вісник Східноукраїнського національного університету імені Володимира Даля. 2013. – № 15(204). – Т. 1. – С. 59-62.
10. Казакова, Н. Ф. Автоматизація процесу адаптації інформаційних систем до інцидентів інформаційної безпеки [Текст] / Н. Ф. Казакова, Є. В. Вавілов // Інформаційна безпека. – 2013. – №4 (12). – С. 49-56.
11. Орлик О. В. Економічна безпека підприємства: властивості, стратегія та методи забезпечення [Текст] / О. В. Орлик // Економічна безпека в умовах глобалізації світової економіки : [колективна монографія у 2 т.]. – Дніпропетровськ : «ФОП Дробязко С.І.», 2014. – Т. 2. – С. 176-182.
12. Вавілов Є. В. Фактори впливу на показники якості інформаційно-комунікаційних мереж [Текст] / Є. В. Вавілов, Г. В. Васильченко // Гармонізація суспільства – новітній напрямок розвитку держави : щорічн. студ. конф. ОНЕУ, 25 березня 2014 р. : матер. конф. Одеса, ОНЕУ. – С. 7-10.