УДК 004.056

ОСНОВИ ПРОВЕДЕННЯ АУДИТУ СИСТЕМИ УПРАВЛІННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Павленко В.В., Горицький В.М.
Інститут телекомунікаційних систем, КПІ ім. Ігоря Сікорського, Україна
E-mail: pavlenkov1996@gmail.com

Basic concepts of conducting audit of information security management system

Considered the main stages of conducting audit of information security management system such as analysis for compliance documentation management system implementation, planning, preparation and improvement.

Проблема створення ефективних систем управління інформаційної безпеки (СУІБ) з метою забезпечення стабільного розвитку сучасної організації та успішної протидії загрозам в умовах жорсткої конкуренції добре відома. Дану систему необхідно піддавати повноцінному аудиту на відповідність вимогам інформаційної безпеки, наприклад стандартам серії ISO 27k [1,2]. Тому важливість проведення якісної перевірки СУІБ важко переоцінити.

Під інформаційною безпекою зазвичай розуміється захищеність інформації та підтримуючої її інформаційної системи від випадкових і навмисних впливів природного або штучного характеру, що завдають шкоди власникам або користувачам цієї інформації і самій підтримуючій її інформаційній системі [1].

Аудит СУІБ дозволяє визначити найбільш вразливі місця в захисті компанії, допомагає оцінити ефективність діючих організаційно-технічних заходів щодо захисту інформаційної системи організації [3]. Рівень забезпечення інформаційної безпеки різниться в залежності від конкретної компанії, але повинен відповідати деякому мінімальному набору вимог безпеки. Сьогодні існує ряд стандартів в області інформаційної безпеки, найбільш відомий - міжнародний стандарт ISO/IEC 27001: 2013, що містить вимоги щодо створення СУІБ компанії [2].

Основним завданням аудиту є підтвердження конфіденційності, цілісності і доступності інформації, що обробляється в корпоративній системі підприємства.

Аудит на відповідність вимогам інформаційної безпеки - це комплексний, циклічний процес, який складається з наступних етапів:

- планування аудиту;
- планування заходів по аудиту (розробка, узгодження і затвердження планів заходів);
- перевірка на відповідність групі вимог (наприклад, на відповідність стандарту ISO/IEC 27001: 2013);
- систематизація результатів обстеження і формування звітності.

Ці чотири етапи складають життєвий цикл аудиту [4].

Найбільш складним етапом, звичайно, є практичне проведення аудиту. Безпосередньо перед проведенням аудиту аудиторська група повинна мати чітко сформульовані завдання аудиту і його область, критерії аудиту, документи різних рівнів (політики, процедури, інструкції, стандарти організації та ін.), перелік процесів і активів компанії, що підлягають перевірці, узгоджену програму аудиту від об'єктів аудиту, підтвердження проведення аудиту.

Аудит починається зі вступної наради з представниками організації, на якому обговорюється порядок денний, програма аудиту. Після цього аудитори починають перевіряти організацію. Спочатку перевіряються документи верхнього рівня: політика інформаційної безпеки або концепція інформаційної безпеки, приватні політики, стандарти організації. Перераховані документи повинні відображати не тільки ідеологію організації в цілому в області інформаційної безпеки, але і відображати розподіл відповідальності між співробітниками і керівництвом організації. Обов'язково необхідно перевіряти обізнаність про зміст цих документів у співробітників організації і розуміння цілей, принципів і зобов'язання щодо захисту активів компанії.

Аудитор повинен по черзі пройти кожний заявлений в програмі підрозділ і перевірити виконання необхідних вимог. В ході перевірки може бути використано інтерв'ювання, часткова перевірка процесу, перевірка з допомогою вибірки (перевірка виконання в певні проміжки часу), або повна перевірка всіх складових процесу. При цьому логічним буде виглядати аналіз та перевірка:

- вразливості політики безпеки;
- вразливості організаційних заходів;
- вразливості класифікації і контролю ресурсів;
- вразливості процедур, пов'язаних з персоналом;
- вразливості фізичної безпеки;
- вразливості експлуатації систем;
- вразливості контролю доступу;
- вразливості обслуговування і розробки систем;
- уразливості інцидентів інформаційної безпеки [4].

В процесі аудиту важливим фактором є збір фактів і свідчень для подальшого аналізу і звіту. Дані завжди повинні бути об'єктивними, аудитор не повинен використовувати власну фантазію для отримання картини, що відбувається. Відомості можуть бути отримані за допомогою спостереження, вимірювання, випробування або будь-яким іншим розумним способом. Хорошою практикою вважається відкритість аудитора і вміння ставити правильні питання, які мотивують розповісти про процес або пояснити необхідні деталі.

Відомості аудиту використовуються для опису невідповідностей, формування висновків і рекомендацій. Так як при перевірці часто аналізуються

результати попередніх аудитів, то зібрані свідчення про невідповідності повинні бути простежені і легко відновлюваними для аудиторів в одній області.

Після перевірки всіх необхідних процесів, заявлених у програмі аудиту, представляється звіт за виявленими невідповідностями. У ньому відбиваються всі відмінності, будь-яка двозначність неприпустима. Він деталізований: всі зібрані факти по кожному процесу або пункту стандарту повністю відображені. Звіт про невідповідності повинен бути ретельно перевірений на наявність помилок і неточностей, і, по можливості, не мати великих обсягів.

Далі складається комплексний звіт по проведеному аудиту. Він може вміщувати рекомендації щодо усунення невідповідностей і календарний план робіт щодо поліпшення СУІБ.

Завершити аудит рекомендується заключною нарадою, на якій підводяться підсумки аудиту, обговорюються спірні питання, що виникли в ході проведення перевірки, узгоджуються терміни усунення зауважень. Важливо отримати підтвердження розуміння необхідності поліпшення СУІБ і узгодити терміни початку і завершення робіт щодо усунення недоліків [5].

Аудит інформаційної безпеки в сучасних умовах є одним з найбільш ефективних інструментів отримання незалежної і об'єктивної оцінки поточного рівня захищеності будь-якого економічного суб'єкта як від існуючих, так і потенціальних загроз. Результати аудиту інформаційної безпеки дозволяють сформувати стратегічні установки розвитку, що відповідають сучасним викликам системи забезпечення інформаційної безпеки для вказаного суб'єкта. Однак слід розуміти, що застосування на практиці аудиту інформаційної безпеки має бути не епізодичним, а регулярним, що дозволяє не тільки виявити вже доконаний факт, а й передбачити потенційні загрози [6].

Література

1. ISO/IEC 27007:2011 «Information technology-Security techniques-Guidelines for information security management systems auditing».
2. Цвілій О.О. «Безпека інформаційних технологій: сучасний стан стандартів ISO27k системи управління інформаційною безпекою» - Науковий журнал «Телекомунікаційні та інформаційні технології», - 2014. – № 2. – с. 73-79.
3. Цвілій О.О. Системи управління інформаційною безпекою: гармонізація з міжнародними стандартами, правилами та процедурами. - Перша всеукраїнська науково-практична конференція «Перспективні напрями захисту інформації». 2015. Збірник тез, с. 107-11.
4. Агафонова М.Е., Шахалов И.Ю. К вопросу о проведении внутреннего аудита системы менеджмента информационной безопасности //Вопросы кибербезопасности №3 – 2013. – 6 с.
5. Ситнов А. А., Уринцов А. И. Аудит информационных систем: монография для магистров. М.:Юнити-Дана – 2014. 239 с.
6. Ситнов А. А. Организация аудита информационной безопасности. – 2016. – 9 с.