УДК 004.43

Руда О.І., к.е.н., доцент, (olharuda@gmail.com) ©
Львівський державний університет внутрішніх справ
Руда І.І., викладач, (ir.artprint@gmail.com)
Львівський державний університет внутрішніх справ
Борецька І.Б., асистент, (iryna-boretska@mail.ru)
Національний лісотехнічний університет України

ЗАХИСТ ІНФОРМАЦІЙНИХ СИСТЕМ ПІДПРИЄМСТВ АПК НА БАЗІ АУДИТУ БЕЗПЕКИ

Пропонується класифікування послуг різних видів аудиту інформаційної безпеки, обґрунтовано особливості та головні критерії раціонального вибору і застосування аудиту інформаційної безпеки. Розроблено організаційно-правову структуру аудиту інформаційної безпеки, яка формується відповідно до рекомендацій міжнародних стандартів та з дотриманням вимог чинного законодавства України.

***Ключові слова**: інформаційна система, інформаційна безпека, аудит інформаційної безпеки, захист інформації.*

Постановка проблеми. На поточний момент, коли обсяги інформації, що циркулює, обробляється та накопичується у сучасних інформаційних системах (ІС), стрімко збільшуються, питання захисту інформації стає особливо актуальним. В умовах розвитку та впровадження технології систем з відкритою архітектурою, яка вирізняється складною взаємодією ІС різного походження (інтероперабельність), наявністю проблем перенесення прикладних програм між різними платформами (мобільність) та іншими особливостями, питання захисту інформації набуває все більшої ваги.

Аналіз останніх досліджень. На даний момент ще не сформовано усталеного визначення аудиту інформаційної безпеки (ІБ). У подальшому ми пропонуємо під поняттям аудиту ІБ розуміти системний процес отримання об'єктивних якісних і кількісних оцінок заходів безпеки, процесів та процедур відповідно до визначених критеріїв та показників безпеки, вимог міжнародних стандартів, чинного законодавства України, відомчих нормативно-правових актів.

Процедура аудиту ІБ дозволяє керівництву отримати об'єктивну інформацію про стан захищеності ІС. Однак, як показує практика, керівництво і працівники найчастіше розуміють суть цієї послуги по-різному.

На думку авторів, поза увагою дослідників залишилося питання розроблення організаційно-правової структури аудиту інформаційної безпеки, яка визначить стратегію і тактику системи безпеки ІС.

Метою публікації є детальне класифікування послуг різних видів аудиту, обґрунтування особливостей та головних критеріїв раціонального вибору і застосування різних видів аудиту ІБ. Формування організаційно-правової

структури аудиту інформаційної безпеки, яка розробляється відповідно до рекомендацій міжнародних стандартів та з дотриманням вимог чинного законодавства України.

Виклад основного матеріалу. З огляду на згадані обставини керівництву підприємств АПК необхідно звернути особливу увагу на проблеми ІБ у ІС, ймовірність виникнення яких є неминучим у процесі функціонування довільної ІС. Єдиним правильним, з пункту бачення захищеності ІС, рішенням у такій ситуації є **аудит інформаційної безпеки**, який проведуть фахівці у галузі захисту інформації.

Основними цілями проведення робіт з аудиту ІБ є: ідентифікування загроз та виявлення імовірних каналів витоку службової інформації у ІС; розроблення політики безпеки [1] та супровідних документів; інвентаризування інформаційних активів ІС та їх подальше категоріювання; розроблення та запровадження системи управління ризиками ІБ; забезпечення відповідності прийнятих технічних рішень вимогам чинного законодавства та галузевих норм [2]; незалежне оцінювання поточного стану захищеності інформаційної структури ІС та мінімізування збитків від інцидентів безпеки.

Одним з найпоширеніших видів аудиту є активний аудит. Це дослідження стану захищеності ІС з точки зору зловмисника, що володіє високою кваліфікацією в області сучасних інформаційних технологій (ІТ). Найчастіше послугу активного аудиту іменують інструментальним аналізом захищеності ІС, щоб виокремити цей вид аудиту від інших.

Суть активного аудиту полягає у тому, що за допомогою спеціального програмного забезпечення (у тому числі систем аналізу захищеності) і спеціальних методів здійснюється збір інформації про стан системи захисту зовнішнього периметру корпоративної мережі ІС підприємства.

При здійсненні даного виду аудиту на систему захисту зовнішнього периметру корпоративної мережі з віддаленим доступом моделюється якомога більша кількість мережевих атак, які може здійснити зловмисник. При цьому аудитор штучно ставиться, властиво, у такі умови, в яких працює зловмисник, – йому надається мінімум інформації, тільки та, яку можна отримати з відкритих джерел.

Активний аудит умовно можна поділити на два види – ″зовнішній″ і ″внутрішній″. При ″зовнішньому″ активному аудиті фахівці моделюють атаки на зовнішній периметр корпоративної мережі і окремі вузли досліджуваної ІС ″зовнішнього″ зловмисника. У даному випадку проводяться такі процедури: визначення доступних з зовнішніх мереж IP-адрес корпоративної мережі досліджуваної ІС; сканування даних IP-адрес з метою визначення активованих сервісів, а також призначення відсканованих хостів; визначення версій сервісів сканованих хостів; вивчення трафіку до хостів корпоративної мережі; збір інформації про систему безпеки ІС з відкритих джерел; аналіз отриманих даних з метою подальшого реалізування загроз.

Однак, всупереч поширеним уявленням, загрози зовнішньому периметру корпоративної мережі не є найбільш критичними для безпеки інформаційних активів ІС. Інсайдерські загрози (загрози, які виходять від своїх же працівників) є на порядок вищими, ніж загрози зовнішні.

″Внутрішній″ активний аудит за складом робіт аналогічний до ″зовнішнього″ і проводиться з використанням спеціальних програмних засобів моделювання загроз від ″внутрішнього″ зловмисника.

З огляду на специфіку функціонування ІС підприємств АПК у ході активного аудиту необхідно виконувати ряд додаткових досліджень, безпосередньо пов'язаних з оцінюванням стану системи безпеки, зокрема – проведення спеціальних досліджень. Це пов’язано з використанням спеціалізованого програмного забезпечення (ПЗ) призначеного для вирішення спеціальних завдань. Подібне ПЗ унікальне, тому готових засобів і технологій для аналізу їх захищеності не існує.

Експертний аудит можна умовно подати як порівняння стану системи захисту ІС з ″ідеальним″ описом. Ключовий етап експертного аудиту – аналіз системи захисту ІС, топології корпоративної мережі та технології оброблення інформації, у ході якого виявляються недоліки існуючої системи захисту, які знижують рівень захищеності ІС [3]. За результатами робіт даного етапу пропонуються зміни в існуючій ІС і технології оброблення інформації, спрямовані на усунення виявлених недоліків.

Наступний етап – аналіз інформаційних потоків. На даному етапі визначається критичність інформаційних потоків ІС та використовуються методи забезпечення ІБ, що відображають рівень захищеності інформаційного потоку.

На підставі результатів даного етапу робіт пропонується захист або підвищення рівня захищеності тих компонент ІС, які беруть участь у найбільш важливих процесах передавання, зберігання та оброблення інформації. Застосування аналізу рівня критичності інформаційних потоків дає можливість реалізувати систему захисту, яка відповідає принципу розумної достатності.

Особлива увага на етапі аналізу інформаційних потоків надається визначенню повноважень і відповідальності конкретних осіб за забезпечення ІБ різних ділянок ІС. Повноваження і відповідальність повинні бути закріплені положеннями організаційно-розпорядчих документів. Організаційно-розпорядчі документи оцінюються на предмет достатності та несуперечності декларованим цілям і заходам ІБ.

Аудит на відповідність стандартам. Суть даного виду аудиту найбільш наближена до тих формулювань, які існують у фінансовій сфері. При проведенні даного виду аудиту стан системи захисту ІС порівнюється з прийнятим абстрактним описом, який подається у стандартах.

Організаційно-правова структура інформаційного аудиту системи ІБ у ІС формується відповідно до рекомендацій міжнародних стандартів та з дотриманням положень чинного законодавства України. Такими стандартами є: ISO/IEC 27002:2005 Інформаційні технології. Методи захисту. Кодекс практики для управління інформаційною безпекою; ISO/IEC 27003:2010 Інформаційні технології. Методи захисту. Керівництво з застосування системи менеджменту захисту інформації; ISO/IEC 27004:2009 Інформаційні технології. Методи захисту. Вимірювання; ISO/IEC 27005:2008 Інформаційні технології. Методи забезпечення безпеки. Управління ризиками інформаційної безпеки; ISO/IEC

27006:2007 Інформаційні технології. Методи забезпечення безпеки. Вимоги до органів аудиту і сертифікування систем управління ІБ.

Офіційний звіт, підготований у результаті проведення даного виду аудиту, включає наступну інформацію: ступінь відповідності ІС обраним стандартам; ступінь відповідності власним внутрішнім вимогам в області ІБ; кількість і категорії отриманих невідповідностей і зауважень; настанови з побудови або модифікування системи ІБ, що дозволяють привести її у відповідність з даним стандартом; докладне посилання на основні документи, включаючи політику інформаційної безпеки, опис процедур забезпечення ІБ, додаткові обов'язкові і необов'язкові стандарти і норми, які запроваджені у ІС [4].

Як **висновок** відзначимо, що при плануванні перевірки стану системи ІБ важливо не тільки точно вибрати вид аудиту, виходячи з потреб і можливостей, але і не помилитися з вибором виконавця.

Література

1. Рудий Т.В. Захист інформаційних систем підрозділів МВС / Т.В. Рудий, Я.Ф. Кулешник, О.В. Омельяненко, О.О. Логінова / Проблеми застосування інформаційних технологій, спеціальних технічних засобів у діяльності ОВС, навчальному процесі, взаємодії з іншими службами // Матеріали науково-практичної конференції 14 грудня 2011 р. – Львів: ЛьвДУВС, 2011. – С.58-64.

2. Рудий Т.В. Управління безпекою в інформаційних системах МВС / Т.В. Рудий, Я.Ф. Кулешник, І.М. Ганич, І.В Бичинюк / Науковий вісник ЛьвДУВС, №1(47), – Львів: ЛьвДУВС, 2011. – С. 382-392.

3. Рудий Т.В. Принципи організації системи захисту інформаційних систем підрозділів МВС / Т.В. Рудий, О.В. Захарова, О.І. Зачек, А.Т. Рудий / Науковий вісник ЛьвДУВС. Серія юридична / головний редактор М.М. Цимбалюк. – Львів: ЛьвДУВС, 2012. – Вип. 2 (2). – С. 309-316.

4. Когут В.В. Порядок атестування систем технічного захисту інформації / В.В. Когут, Т.В. Рудий, Я.Ф. Кулешник, А.Т. Рудий / Проблеми діяльності кримінальної міліції в умовах розбудови правової держави // Матеріали науково-звітної конференції факультету кримінальної міліції ЛьвДУВС 12 березня 2010 р. –Львів: ЛьвДУВС, 2010. – С.90-97.

Summary

Olha Ruda, *Lviv State University of Internal Affairs*
Iryna Ruda, *Lviv State University of Internal Affairs*
Iryna Boretska, *Ukrainian National Forestry University*

PROTECTION OF INFORMATION SYSTEMS ENTERPRISES AIC BASED SECURITY AUDIT

Proposed classifying services of various types of auditing information security, reasonable features and the main criteria for rational selection and application of auditing information security. The organizational and legal structure of auditing information security which is formed in accordance with the recommendations of international standards and in compliance with the current legislation of Ukraine.

Key words: *information systems, information security, audit information security, information security.*

Рецензент – д.е.н., професор Музика П.М.