

Левшенко О. С.¹

Комолаєва Т. М.¹

Пустовіт С. С.²

Рибидайло А. А. к.т.н., с.н.с.¹

Уварова Т. В.¹

¹- Центр воєнно-стратегічних досліджень Національного університету оборони України імені Івана Черняхівського, Київ;

²- Державне підприємство “Антонов”, Київ

Організаційний аспект проведення аудиту електронних ресурсів Збройних Сил України

Резюме. У статті розглянуто питання проведення аудиту електронних ресурсів установ Збройних Сил України, за результатами якої отримуються відомості щодо стану інформації, що є їх власністю.

Ключові слова: електронні ресурси, інформаційні ресурси, аудит, інвентаризація, реєстр, класифікація.

Постановка проблеми. Розвиток інформаційних технологій веде до істотного відновлення складу електронних інформаційних ресурсів, враховуючи їх вплив на усі сфери діяльності установи: наукову, суспільну, економічну тощо.

На сьогодні представляється важливим знання про те, якою інформацією, в якому обсязі і в яких місцях зберігання знаходяться інформаційні ресурси, якими володіє установа (відомство).

За визначеннями, які наведені в [1, 2], *електронний ресурс* – це інформаційні ресурси, які керуються комп'ютером, потребують використання периферійного пристрою, підключеного до комп'ютера. Електронними ресурсами є електронні дані, електронні програми або їх об'єднання.

Згідно з міжнародними стандартами, серед яких ISO 17799 “Інформаційна технологія. Методики безпеки. Практичне керівництво для інформаційного управління безпеки” [14], виділяють наступні категорії ресурсів:

інформаційні ресурси – бази і файли даних, системна документація, дослідницька документація тощо;

програмні ресурси – прикладне, системне, інструментальне програмне забезпечення та утиліти;

фізичні ресурси – комп'ютерне обладнання, засоби зв'язку, змінні носії й інше обладнання;

сервіси – обчислювальні служби та засоби зв'язку, служби загального призначення.

На початку 2000-х років гостро встало питання щодо необхідності захисту й обліку ресурсів, у тому числі електронних ресурсів (ЕР),

інформаційних ресурсів (ІР), інформаційних електронних ресурсів (ІЕР) як таких.

Інформаційний ресурс – сукупність документів в інформаційних системах (бібліотеках, архівах, банках даних тощо).

Електронний інформаційний ресурс – інформація, апаратні, програмні та інші засоби, що можуть бути надані користувачеві (файл-сервером або базою даних).

Виникла проблема контролю за неправомірним використанням інформації ЕР обмеженого доступу і пов'язані з цим проблеми витоків та інших небажаних дій, що потребує проведення перевірки, аудиту з метою аналізу та безпеки зберігання, у тому числі і в установах Збройних Сил (ЗС) України.

Це зв'язане, у першу чергу, з еволюційним переходом інформації (у тому числі й обмеженого доступу) в електронний вид. При цьому системи (ERP, CRM, електронний документообіг, електронна пошта), у яких ця інформація циркулює, створювалися для надання максимально швидкої доступності інформації, зневажаючи на її цілісність та конфіденційність.

Ступінь розробленості проблеми і аналіз останніх досліджень і публікацій. З питання розвитку системи аудиту ЕР, удосконалення їх техніко-технологічного інструментарію, теоретико-методологічних основ управління обліково-інформаційною діяльністю є чимало ґрунтовних досліджень, які суттєво вплинули на саму концепцію аудиту, що є необхідним підґрунтям та базою щодо вдосконалення процедур проведення аудиту ЕР, ІР, ІЕР [5-8].

З метою підвищення якості проведення аудиту ЕР провідні IT-компанії розробили та готові запропонувати замовникам комплексне рішення аудиту, що включає в себе ідентифікацію, рубрикацію та категорювання ІР. Запропоноване рішення засноване на застосуванні спеціалізованих програмних продуктів класу управління знаннями (Knowledge Management), призначених для обробки різнорідних інформаційних масивів, наприклад: Autonomy IDOL Server, Convera Retrievalware, Opendext Knowledge Management & Concept Builder й інших [8, 13]. Усі перераховані вище програмні комплекси належать до групи найбільш функціональних і широко визнаних інформаційно-аналітичних систем корпоративного рівня.

Реалізовані в цих продуктах технології автоматизації інформаційно-аналітичної діяльності дозволяють проводити аудит та автоматизовану класифікацію інформаційних масивів по тематичним групам (рубрикам).

Метою дослідження є узагальнення світового досвіду та обґрунтування організаційних аспектів проведення аудиту електронних ресурсів у ЗС України.

Виклад основного матеріалу. Під аудитом розуміють оцінку систем, процесів, підприємств, проектів або продуктів. В Україні цей термін внаслідок впливу англомовних джерел також застосовується в галузі управління проектами, оцінки та перевірки електронних ресурсів (ЕР), інформаційно-електронних ресурсів (ІЕР) та відповідність їх вимогам законів України, положень (стандартів) обліку або інших правил [3, 4].

Головною метою перевірки та аудиту ЕР є забезпечення контролю за достовірністю інформації, що надається у звітності.

У Міністерстві оборони (МО) України для проведення перевірки матеріальних ресурсів створено Департамент внутрішнього аудиту, що є структурним підрозділом апарату МО України, призначеним для здійснення внутрішнього контролю діяльності підконтрольних суб'єктів, до яких належать структурні підрозділи МО України та Генерального штабу (ГШ) ЗС України, військові частини, військові навчальні заклади, установи та організації ЗС України, організації, державні підприємства та об'єднання підприємств, що належать до сфери управління МО України та ГШ ЗС України.

Основними завданнями Департаменту є надання МО України об'єктивних і незалежних висновків і рекомендацій (пропозицій) щодо:

функціонування системи внутрішнього контролю в МО України, ГШ ЗС України, інших підконтрольних суб'єктах та її вдосконалення;

удосконалення системи управління фінансовими та матеріальними ресурсами МО та ЗС України;

запобігання фактам незаконного, неефективного та нерезультативного використання МО України, ГШ ЗС України, іншими підконтрольними суб'єктами фінансових та матеріальних ресурсів;

запобігання виникненню помилок чи інших недоліків у діяльності МО України, ГШ ЗС України, інших підконтрольних суб'єктів;

функціонування системи контролю за електронними ресурсами.

Згідно з міжнародними стандартами й практиками, серед яких ISO 17799 "Інформаційна технологія. Методики безпеки. Практичне керівництво для інформаційного управління безпеки", виділяють наступні категорії ЕР:

інформаційні ресурси (бази і файли даних, системна документація, дослідницька документація, настанови користувачів тощо);

програмні ресурси (прикладне, системне, інструментальне програмне забезпечення та утиліти);

фізичні ресурси (комп'ютерне обладнання, засоби зв'язку, змінні носії та інше обладнання);

сервіси (обчислювальні служби та засоби зв'язку, служби загального призначення).

Проведення аудиту ЕР підтверджується формулюванням двох із переліку основних принципів безпеки захисту інформації: "Знай те, чим володієш" і "Захищай те, чим володієш". Аудит дозволяє вирішити ряд важливих завдань для побудови ефективної системи забезпечення діяльності установи та забезпечення інформаційної безпеки.

При виконанні аудиту ЕР вирішуються наступні завдання:

визначення обсягів проведення перевірок, тобто які ЕР будуть розглянуті і які завдання вони виконують;

визначення і класифікація ЕР (наприклад, за видом інформації – вхідна, вихідна, така, що зберігається та обробляється);

визначення власників ресурсів та їх повноважень;

категорювання ЕР за критеріями інформаційної безпеки (наприклад, загальна інформація, інформація обмеженого користування, державна або комерційна

таємниця тощо) – це дозволяє виділити найбільш критичні ресурси, порушення інформаційної безпеки, яких може привести до збитку;

визначення суб'єктів ЕР, тобто користувачів, яким надається доступ до інформації, що захищається (розмежування доступу і повноважень);

регламентація способів зберігання і захисту критичних ЕР, а також безпечної роботи з ними у разі надзвичайних ситуацій;

аналіз поточного стану і форми організації інформаційного захисту ЕР у МО України;

закріплення прав матеріальної та/або інтелектуальної власності;

документування процесу аудиту та інвентаризації ресурсів, включаючи інвентаризаційні описи.

Об'єктами аудиту є система ЕР МО України, органів військового управління усіх рівнів, військових частин, структурних підрозділів, закладів, установ та організацій, що забезпечують їх формування, використання та захист інформації в них.

Аудит ЕР є точкою відліку у процесі побудови системи інформаційної безпеки. Саме необхідність мати актуальні відомості щодо власних ресурсів виявляє необхідність проведення аудиту та інвентаризації в установі і проводиться за типами ресурсів, враховуючи категорії їх конфіденційності, здійснюється на підставі документів, де можуть мати місце невиявлені помилки в облікових записах. Усе це обумовлює можливість невідповідності між даними обліку і фактичної наявності ресурсів і для виявлення та усунення такої невідповідності проводиться аудит й інвентаризація.

Інвентаризація – це перевірка в натурі наявності та стану матеріальних цінностей та вкладень, звірка фактичної наявності з даними обліку, протягом якої виявляються корисні інформаційні залишки, визначаються

інструменти та технології оптимізації інформаційних процесів.

Теперішнє стрімке та мало контрольоване зростання інформаційного масиву зумовлене не менш динамічним розвитком інформаційних технологій, які вимагають нового ставлення до обслуговування інформації, а саме, вивели на перше місце потребу в аудиті та інвентаризації інформації.

Інвентаризація ЕР входить до концепції управління інформацією, яка зосереджена на процесах її створення, обслуговування, передавання, архівації та утилізації.

У цей час характерним як для великих, так і відносно невеликих установ є відсутність яскраво вираженої структури ЕР саме в плані конфіденційності інформації, відсутній або не відповідає дійсності перелік конфіденційних документів [13]. Найчастіше без належної уваги до змісту залишається весь інформаційний масив, створюваний, збережений, одержуваний, пересилаємий співробітниками, що не входять в управлінське коло установи – їх робочі документи, повідомлення електронної пошти, у яких можуть утримуватися відомості, які підлягають захисту.

Слід зазначити і той факт, що більшість усіх корпоративних ІР є неструктурованими – це інформація у файлах, повідомленнях електронної пошти, замітках, доповідях і планах, створена в різних форматах і збережена в різних системах. Це вказує на необхідність проведення спеціального комплексу заходів – аудиту та інвентаризації ІР.

З позиції найбільш загального представлення процесу аудиту доцільно виділяти наступні етапи (табл. 1).

Таблиця 1

Етапи проведення аудиту

№	Етап	Процедура
1.	Підготовчий	Визначення основних напрямів перевірки
2.	Початковий	Здійснення поглибленої оцінки системи обліку та внутрішнього контролю
3.	Основний	Фізична перевірка активів установи та документальна перевірка рахунків бухгалтерського обліку, звітності
4.	Заключний	Складання звіту про проведену аудиторську перевірку та аудиторський висновок про достовірність перевіреної звітності

У загальному вигляді порядок проведення аудиту ЕР установ ЗС України можна подати наступним чином:

ідентифікація ЕР, що припускає визначення фізичного місцезнаходження ІР (власні сервери зберігання, орендовані сервери), типи зберігання ІР (файлові системи, СУБД і т.д.), формати зберігання (текстові файли, файли презентацій, графічні зображення, записи БД);

виділення ІР, доступних для обробки;

рубрикацію ІР, що включає в себе:

– побудову (розроблення) структури рубрик;

– автоматизовану рубрикацію ІР;

– інтерпретацію результатів рубрикації;

категорювання ІР установи на основі прийнятої політики інформаційної безпеки, яке проведене за результатами рубрикації ІР;

внесення змін або перегляд переліку конфіденційних документів.

На етапі ініціювання процедури аудиту ЕР повинні бути вирішені наступні організаційні питання:

права та обов'язки аудиторів повинні бути чітко визначені і документально закріплені в посадових інструкціях, а також у положенні про внутрішній (зовнішній) аудит;

визначення границь проведення обстеження;

аудитором повинен бути підготовлений і погоджений з керівництвом план проведення аудита.

План і границі проведення аудита обговорюються на загальних зборах, у яких беруть участь аудиторів, керівництво установи та керівники структурних підрозділів.

У положенні про внутрішній аудит повинне бути закріплене, зокрема, що співробітники установи зобов'язані сприяти аудиторів і надавати всю необхідну для проведення аудита інформацію.

Переваги використання пропонованої методики аудиту ІР:

можливе застосування методики як у складі комплексу заходів аудиту інформаційної безпеки у цілому, так і самостійно – як окремої послуги;

ефективна обробка більших обсягів (сотні гігабайт) текстової інформації – проведення автоматичного аналізу змісту документів, анотування документів;

ЕР установи стають її інтелектуальними активами. Інтелектуальні активи можна представити як вид ЕР, які установа змогла визначити, описати та занести до конкретного реєстру.

Прикладами інтелектуальних активів є:

програмне забезпечення, розроблені і формалізовані в установі бізнес-процеси та методології, бази і масиви даних, звіти та описи тощо;

автоматична класифікація корпоративних ІР по тематичним групам; виділення конфіденційної інформації із загального масиву;

можливість автоматизованої аналітичної обробки ЕР з метою виявлення тематичної спрямованості вмісту, автоматизоване структурування ІР;

пошук інформації, що не явно відноситься до типу “конфіденційна”;

можливості аналізу інформації, збереженої у файлових системах, на Web-Сайтах, СУБД, в Microsoft Exchange, Lotus Notes та ін.

Установа, що одержує ЕР переробляє їх у продукти своєї діяльності. При цьому вони породжують специфічне внутрішнє середовище, яке формується сукупністю структурних підрозділів, персоналом, технічними засобами та технологічними процесами, відносинами як усередині самої установи, так і у взаємодії з іншими.

Усередині установи інформаційні потоки надходять у відповідні модулі інформаційно-аналітичної системи для структурування, систематизації, обробки, аналізу і практичного використання. Більша частина цієї інформації є вільно використовуваною в процесі реалізації діяльності державної або комерційної установи, однак залежно від особливостей внутрішньої діяльності та взаємодії зі сторонніми організаціями частина інформації може мати грифи обмеження доступу.

Після проведення аудиту складається звіт, який містить:

відомості про об'єкти аудита;

опис інформаційних систем, що входять в область аудита;

опис складу та класифікацію інформації, оброблюваної в установі (у рамках області аудита);

результати аналізу організаційно-розпорядчої документації в області захисту інформації;

результати оцінки реалізації організаційних і технічних заходів захисту та висновки і рекомендації з підвищення рівня захищеності.

Електронні ресурси підлягають обов'язковому внесенню до Реєстру електронних інформаційних ресурсів Міністерства оборони України [11, 12], метою створення якого є:

побудова та розвиток інформаційного простору МО України;

забезпечення реєстрації й обліку існуючих, придбаних або переданих на законних підставах ЕІР, які є у розпорядженні МО України;

забезпечення оперативного доступу до відомостей, які занесені в Реєстр: їх наявність, структура, зміст, власники (постачальники) ЕІР, а також умови їх отримання зацікавленими користувачами (споживачами) ЕІР.

Відповідно до грифу інформації ЕІР Реєстр включає три реєстри:

з відкритою інформацією (даними);
зі службовою інформацією (з ЕІР, які містять службову та конфіденційну інформацію);
з таємною інформацією.

Сам Реєстр складається з еталонного, робочого, страхового та інформаційного фондів.

ЕІР МО України інтегрується з Єдиною автоматизованою системою управління ЗС України та системи електронної взаємодії державних ЕІР.

Власником Реєстру є Міністерство оборони України, а загальне керівництво здійснює Міністр оборони України.

ЕІР класифікуються за напрямками діяльності структурних підрозділів МО України, структурних підрозділів ГШ ЗС України, видів ЗС України, їх з'єднань, військових частин, військових навчальних закладів, установ та організацій, що не належать до видів ЗС України.

Обов'язковою умовою включення відомостей про ЕІР до Реєстру є його документування на матеріальних носіях із реквізитами, що дозволяють його ідентифікувати.

Визначений структурний підрозділ (військова частина), який здійснює системне адміністрування Реєстру один раз на рік проводить повний аудит та інвентаризацію зареєстрованих ЕІР та за її результатами звітує перед державною установою з питань електронного урядування України через уповноважений структурний підрозділ МО України.

Висновки. Аудит електронних ресурсів має бути організований таким чином, щоб повно, точно, оперативно та наочно представити перелік видів, типи, категорії ресурсів, порядок організації та їх ефективного використання, обслуговування і захист.

Затребуваність аудиту інформаційних ресурсів походить з необхідності забезпечення інформаційної безпеки та має здійснюватися, виходячи з видів та категорій інформації. Установа може визначити, яка інформація повинна бути оброблена та захищена, тобто

забезпечити задані рівні захисту використовуваних електронних ресурсів.

Електронні ресурси та інформаційні системи Збройних Сил України підлягають обов'язковому обліку в державному Реєстрі.

Подальше дослідження планується здійснювати, виходячи із затребуваності удосконалення інструментарію інформаційно-аналітичних ресурсів.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Закон України від 13.09 2001 р. N 2684 "Про Національну програму інформатизації".
2. Антоненко І., Баркова О. Електронні ресурси як об'єкт каталогізації: історія питання, термінологія, форматне забезпечення // Бібл. вісн. - 2004. - N 2. - С. 11-22. - Режим доступу до статті: <http://sas1.at.ua/publ/8-1>
3. Закон України «Про аудиторську діяльність» від 22.04.1993 р. №3125-ХІІ.
4. Рішення АПУ від 30.11.2006 №168/7 "Про застосування Міжнародних стандартів аудиту видання 2006 року".
5. Пушкар, А.И. Теоретико-методологические основы управления информационной деятельностью предприятия / А.И. Пушкар // Сучасні проблеми управління підприємствами: теорія та практика: матеріали міжн. наук.-практ. конференції 8 – 9 листопада 2012 р. – Х.: ФОП ВД «ІНЖЕК», 2012.
6. Назаренко В.В., В. Укріплюємо безпеку бізнесу: комерційна таємниця і конференційна інформація /В.В. Назаренко // Баланс. – 2011.
7. Писаревська Т.А. Інформаційні системи обліку та аудиту: Навч. посібник. – К.: КНЕУ, 2004. – 369 с.
8. Джарратано Д., Гайли Г. Экспертные системы. Принципы разработки и программирования. – М.: Издательский дом «Вильямс», 2007.
9. Розпорядження КМ України від 05.05.2003 р. N 259-р "Про затвердження Концепції формування системи національних електронних інформаційних ресурсів"
10. Наказ Міністра оборони України від 17.09.2014 року № 650 "Про затвердження Концепції інформатизації Міністерства оборони України".
11. Постанова КМ України від 17 03. 2004 р. N 326 "Про затвердження Положення про Національний реєстр електронних інформаційних ресурсів".
12. Наказ Міністра оборони України від 01.04.2015, № 147 "Про затвердження Реєстру електронних інформаційних ресурсів Міністерства оборони України".
13. Васильев М. Аудит и инвентаризация информационных ресурсов. Журнал Информационная безопасность", №4, 2009
14. ISO/IEC 17799:2005 "Информационная технология. Методики безопасности. Практическое руководство для информационного управления безопасности".

Левшенко А. С.¹

Комолаева Т. Н.¹

Пустовит С. С.²

Рыбыдайло А. А. к.т.н., с.н.с.¹

Уварова Т. В.¹

¹- Центр военно-стратегических исследований Национального университета обороны Украины имени Ивана Черняховского, Киев;

²- Государственное предприятие “Антонов”, Киев

Организационный аспект проведения аудита электронных ресурсов Вооруженных Сил Украины

Резюме. В статье рассмотрены вопросы проведения аудита электронных ресурсов учреждений Вооруженных Сил Украины, результатом которого являются сведения о состоянии информации, являющейся собственностью организации.

Ключевые слова: электронные ресурсы, информационные ресурсы, аудит, инвентаризация, реестр, классификация.

A. Levshenko;

T. Komolaeva;

S. Pustovit;

A. Rybydajlo;

T. Uvarova

Organizational aspect of realization for audit of electronic resources of the Armed Forces of Ukraine

¹- Center for Military and Strategic Studies National Defence University of Ukraine named after Ivan Chernyhovskij, Kyiv;

²- National enterprise “Antonov”, Kyiv

Resume. In the article the questions of the audit of electronic resources of the Armed Forces of Ukraine, the result of which is the status information is information owned by the organization.

Keywords: information resources, inventory, audit, management, classification.