МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Київський національний університет будівництва і архітектури

Ю.І. Хлапонін, О.В. Сєлюков

МОНІТОРИНГ ТА АУДИТ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ СИСТЕМ

Конспект лекцій
для студентів спеціальності
125 «Кібербезпека»

Київ 2024

УДК 378.147:004:34.08
Х-55

Рецензент А.М. Котенко, к.т.н., доцент, доцент кафедри Систем інформаційного та кібернетичного захисту Державного університету інформаційно-комунікаційних технологій

Затверджено на засіданні вченої ради факультету автоматизації і інформаційних технологій, протокол №6 від 24 січня 2024 року.

Хлапонін Ю.І.

Х-55 Моніторинг та аудит інформаційно-комунікаційних систем: конспект лекцій / Хлапонін Ю.І., Сєлюков О.В.– Київ: КНУБА, 2024. – 144 с.

Метою даного конспекту є ознайомлення студентів з основними положеннями щодо побудови та функціонування автоматизованої системи управління комплексів засобів захисту розподіленої обчислювальної системи, опанування студентами основних методів та прийомів створення системи моніторингу інформаційної безпеки для забезпечення заданих показників захищеності інформації в розподілених обчислювальних системах. Головна увага приділена розкриттю не стільки глибини, скільки суті тем дисципліни в стислій і доступній для сприйняття формі.

Призначено для студентів спеціальності 125 “Кібербезпека”.

УДК 378.147:004:34.08

ЗМІСТ

ВСТУП

На сучасному етапі розвитку суспільства, пов'язаного з масовим використанням інформаційних технологій і створенням єдиного інформаційного простору, в рамкам якого відбувається накопичення, обробка, зберігання та обмін інформацією, проблеми інформаційної безпеки набувають першорядного значення в усіх сферах суспільної і державної діяльності. Особлива гострота і актуальність цих проблем визначається такими факторами:

- високими темпами зростання парку засобів обчислювальної техніки і зв'язку, розширенням областей використання електронно-обчислювальних машин (ЕОМ), різноманіттям і повсюдним поширенням інформаційно-керуючих систем, які підлягають захисту;
- залученням до процесу інформаційної взаємодії все більшого числа людей і організацій, різким зростанням їх інформаційних потреб;
- підвищенням рівня попиту на автоматизовані системи управління і обробки інформації, використанням їх в критичних ситуаціях;
- ставленням до інформації, як до товару, переходом до ринкових відносин з властивою їм конкуренцією і промисловим шпигунством у сфері створення і надання інформаційних послуг;
- концентрацією великих обсягів інформації різного призначення на електронних носіях, вдосконалення доступу до інформаційних ресурсів;
- наявністю інтенсивного обміну інформацією між учасниками процесу;
- загостренням протиріч між об'єктивно існуючими потребами суспільства в розширенні вільного обміну інформацією і надмірними або навпаки недостатніми обмеженнями на її поширення і використання;
- рівнями втрат (збитків) від знищення, фальсифікації, розголошення абонезаконного тиражування інформації;
- різноманіттям видів загроз і можливих каналів несанкціонованого доступу (НСД) до інформації;
- зростанням числа кваліфікованих користувачів обчислювальної техніки і можливостей по створенню ними програмно-математичних впливів на систему;
- відсутністю достатньої кількості кваліфікованих спеціалістів у сфері захисту інформації.

Процес впровадження нових інформаційних технологій в усі сфери

життя сучасного суспільства, що вступає в постіндустріальний період свого розвитку, який можна назвати інформаційним, неможливий без рішення питань інформаційної безпеки в різних сферах: політичній, військовій, екологічній, природничо-науковій, технічній, соціальній, нормативно-правовій, економічній, фінансовій. Широкомасштабне використання обчислювальної техніки й телекомунікаційних систем, перехід до безпаперової технології, збільшення об'ємів оброблюваної інформації й розширення кола користувачів приводять до якісно нових можливостей несанкціонованого доступу до ресурсів і даних інформаційної системи, до її високої вразливості. В сучасних умовах захист інформації в цілому й захист інформації в автоматизованих інформаційних системах зокрема стає все більш складною проблемою.

На сьогодні достатня кількість підприємств придбаває і впроваджує комп'ютерну техніку або програмне забезпечення, що потребує оцінки безпеки роботи на них з боку спеціалізованих аудиторських підприємств. У числі завдань аудиторських підприємств, в цьому випадку, можуть бути аналіз результатів впровадження, оцінка ефективності різних етапів експлуатації, ступінь відповідності очікуванням керівництва.

Практично кожний підручник з аудиту містить окремий розділ, який присвячений аудиту у комп'ютерному середовищі. Про цікавість до даної проблеми свідчить також і той факт, що значна кількість дисертаційних робіт містить рекомендації щодо удосконалення аудиту в середовищі електронної обробки даних. Питання проведення аудиторських перевірок з використанням комп'ютерної техніки і програмного забезпечення обговорюються на сторінках фахової преси. Проте, незважаючи на постійну увагу до даної проблематики, як з боку науковців так і практиків, все ще залишаються доволі суттєві прогалини, які стосуються, в першу чергу розробок конкретних методик для окремих об'єктів аудиторських перевірок. У конспекті лекцій розглядаються тільки деякі з основних питань, зв'язаних із забезпеченням інформаційної безпеки. Матеріал підготовлений на основі робочої навчальної програми (РНП) з дисципліни "Моніторинг та аудит інформаційно-комунікаційних систем" для студентів зі спеціальності 125 "Кібербезпека". Головна увага приділена розкриттю не стільки глибини, скільки суті тем в стислій і доступній для сприйняття формі.

Дисципліна має метою засвоєння студентами основних положень щодо побудови та функціонування автоматизованої системи управління комплексом засобів захисту розподіленої обчислювальної системи;

опанування студентами основних методів та прийомів створення системи моніторингу інформаційної безпеки для забезпечення заданих показників захищеності інформації в розподілених обчислювальних системах.

Предметом дисципліни є основи побудови системи моніторингу інформаційної безпеки в інформаційно-комунікаційних системах.

В процесі вивчення дисципліни студенти мають бути ознайомленими із сучасними підходами, методиками, засобами та пристроями для системи моніторингу інформаційної безпеки в інформаційно-комунікаційних системах.

Після вивчення дисципліни студенти повинні знати: основні поняття, категорії, визначення і терміни щодо систем моніторингу інформаційної безпеки; складові проблеми особистої інформаційної безпеки; алгоритм організації та проведення аудитів; особливості реалізації агентського перехоплення трафіку; раціональну організацію та методики проведення оперативного контролю; міжнародні стандарти щодо аудиту, принципи системного підходу до управління комплексними системами захисту інформації.

Після вивчення дисципліни студенти повинні вміти: користуватися аудиторським програмним забезпеченням; проводити документовану процедуру внутрішнього аудиту, будувати організаційні структури оперативного контролю.

НАВЧАЛЬНА ДИСЦИПЛІНА В ГОДИНАХ

Курс	Семестр	Лекції	Лабораторні заняття	Всього ауд. годин	Розрахунково-графічна робота	Контрольні роботи	Установ. лекції	Самостійна робота	Всього годин	Екзамен
130	130	30	30	60	1	–	–	70	130 (4,5 кред)	1

1. АУДИТ ІНФОРМАЦІЙНИХ СИСТЕМ І ТЕХНОЛОГІЙ ЯК ІНСТРУМЕНТ СТРАТЕГІЧНОГО УПРАВЛІННЯ ПІДПРИЄМСТВОМ

Сучасний період розвитку ринкової економіки засвідчує ситуацію, у якій все більшої уваги серед вітчизняних суб'єктів господарювання набуває інтерес до ІТ-середовища. Як показує практика, ІТ-середовище виступає джерелом людських, технічних, інформаційних та програмних ресурсів, що необхідні для забезпечення розвитку підприємства. Однак, для ефективного їх використання в діяльності підприємства необхідно регулярно здійснювати перевірку їх застосування, тобто ІТ-аудит.

Виходячи із того, що ви вивчали за іншими предметами, можна стверджувати, що:

1) під інформаційною технологією слід розуміти систему методів і способів збору, передачі, накопичення, опрацювання, зберігання, подання і використання інформації.

2) інформаційні технології на підприємствах поділяються на:

- технології автоматизації офісу;
- інформаційні технології обробки даних;
- інформаційні технології управління;
- інформаційні технології підтримки прийняття управлінських рішень;
- інформаційні технології експертних систем.

3) інформаційні технології підприємства (забезпечувальні, функціональні) спільно із інформаційними ресурсами, технічними засобами та програмним забезпеченням формують систему інформаційного забезпечення прийняття управлінських рішень (поточних, перспективних).

4) ІТ-аудит (аудит інформаційних технологій) – це незалежна перевірка (експертиза) аудитором (компетентним фахівцем або групою фахівців) ІТ-середовища підприємства з метою отримання повної та об'єктивної інформації (достовірних фактів, якісних і кількісних оцінок) про його поточний стан (даної підсистеми підприємства), формування об'єктивного аудиторського висновку, а також надання рекомендацій щодо удосконалення ІТ-середовища. Отже, ІТ-аудит являє собою процес формування висновків у аудитора та надання їх замовнику (підприємству) стосовно стану тої інформаційної системи, яка виступає об'єктом аудиту. Внаслідок отриманих під час аудиторської перевірки даних формуються рекомендації по удосконаленню ІТ-середовища, у якому функціонує замовник (підприємство).

Практика показує, що аудит інформаційних систем поділяється на декілька напрямків, зокрема:

1) аудит технічного стану (націлений на скорочення витрат, що спричинені збоями);

2) аудит інформаційної безпеки (дозволяє сформувати оптимальну систему захисту інформації, що відповідатиме цілям та меті діяльності підприємства);

3) оціночний аудит програмного забезпечення (спрямований на встановлення рівня економічної ефективності від упровадження та експлуатації програмного забезпечення);

4) оціночний аудит інформаційних систем (передбачає виявлення відхилень фактичних результатів від очікуваних);

5) аудит проектів упровадження і реінжинірингу (націлений на оцінку ризиків упровадження чи реінжинірингу інформаційної системи);

6) аудит ефективності інформаційної системи (дозволяє оцінити сумарну вартість оволодіння інформаційною системою підприємством та порівняти її з показниками лідерів, що функціонують у цьому конкурентному середовищі).

Окрім того, IT-аудит поділяється на внутрішній аудит та зовнішній аудит. Основними елементами внутрішнього IT-аудиту виступають об'єкти інформаційної системи внутрішнього аудиту та персонал, що його здійснюватиме, а зовнішнього IT-аудиту – об'єкти інформаційної системи 28 зовнішнього аудиту та персонал, що його здійснюватиме. Ключовою особливістю IT-аудиту у системі управління підприємством виступає те, що за результатами його проведення можна чітко отримати інформацію про те, яку роль інформаційні технології відіграють у загальній організаційній структурі підприємства. Поряд з тим, отримана інформацію дозволить визначити рівень адекватності IT-стратегії у відповідності до загальної стратегії підприємства, а також рівень зрілості IT-процесів та рівень управління IT-ризиками. Практика засвідчує, що великі та середні аудиторські компанії, які спеціалізуються на наданні аудиторських послуг у IT-сфері, являють собою союзи професіоналів, основними професійними обов'язками яких виступають формування та супровід стандартів IT-аудиту переважно закритого типу. Натомість стандарти відкритого типу аудиту інформаційних систем представлені у діяльності таких провідних компаній, як асоціація ISACA (англ. The Information Systems Audit and Control Association) тобто Асоціація аудиту і контролю інформаційних систем.

Перед тим, як проводити IT-аудит, необхідно першочергово зібрати

інформацію про такі факти, як: вид діяльності та рівень ефективності функціонування підприємства; стан цільового ринку підприємства, взаємовідносини із споживачами та клієнтами; рівень управління організаційною культурою підприємства; стратегічні цілі та майбутнє бачення діяльності.

Алгоритм проведення аудиторської перевірки охоплює п’ять етапів:

1) етап попередньої діагностики, яка необхідна для встановлення видів, термінів здійснення та вартості ІТ-аудиту (передбачає збір інформації про підприємство, на основі якої встановлюються ключові проблеми у ІТ-сфері та представляються пропозиції щодо їх вирішення);

2) етап аудиту ІТ-інфраструктури, який необхідний для одержання точної та правдивої інформації щодо поточного стану інфраструктури упроваджених інформаційних технологій на підприємстві (передбачає визначення сильних та слабких сторін інфраструктури упроваджених інформаційних технологій, рівня ефективності функціонування, що дозволять виділити та представити професійні рекомендації стосовно удосконалення ІТ-інфраструктури підприємства);

3) етап аудиту ІТ-підрозділу, який необхідний для одержання точної та правдивої інформації щодо поточного стану підрозділу, який спеціалізується на управлінні інформаційними технологіями (передбачає виявлення сильних та слабких сторін підрозділу, що відповідає за управління інформаційними технологіями, які дозволять виділити та представити професійні рекомендації стосовно удосконалення ІТ-підрозділу підприємства);

4) етап ІТ-безпеки, який необхідний для одержання точної та правдивої інформації щодо стану інформаційної безпеки підприємства, його сильних та слабких сторін, рівня ефективності функціонування з метою розроблення та впровадження рекомендацій удосконалення ІТ-безпеки підприємства;

5) етап контролю за впровадженням рекомендацій ІТ-аудиту (проводиться із метою забезпечення контролю і підтримки упровадження результатів, отриманих за рахунок здійснення ІТ-аудиту його замовником). Результати доводять, що аудиторський висновок дає можливість оцінити поточний рівень та стан діяльності підприємства, визначити недоліки та встановити ризики із перспективою їх подальшого усунення.

Виходячи із зазначеного, рекомендації стосовно проведеного ІТ-аудиту стосуються таких основних напрямків, як:

1) рекомендації щодо розроблення системи інформаційного забезпечення робочих місць;

2) рекомендації щодо розроблення алгоритмів обміну інформацією;
3) рекомендації щодо контролю за функціонуванням програмного забезпечення і користувачами цього забезпечення;
4) рекомендації щодо проведення повторного контролю за функціонуванням програмного забезпечення і користувачами цього забезпечення;
5) рекомендації по заходах із збереження конфіденційності інформації. Для проведення ІТ-аудиту звично розробляється модель комп'ютерної аудиторської програми, що передбачає проведення аудиту резервів та забезпечень підприємства. Дана модель містить такі елементи: імпорт даних, аналітичне обстеження, систематизацію та аудиторський висновок.

Встановлено, що застосування моделі комп'ютерної аудиторської програми дозволяє отримати ряд переваг для підприємства, зокрема:
1) примножити рівень аудиторської вибірки інформації стосовно резервів та забезпечень підприємства;
2) підвищити рівень контролю за 29 аудиторськими діями;
3) підвищити рівень ефективності аудиту;
4) встановити відхилення фактичних значень від нормативних;
5) порівняти фактичні дані із даними, отриманими у результаті аудиту.

Дослідженнями з'ясовано, що ІТ-аудит доцільно застосовувати у випадку, коли: проводиться використання інформаційних систем і ІТ-аудиту з метою організації діяльності суб'єкта аудиту; ведеться перевірка і оцінювання стану комп'ютерних інформаційних систем; він використовується як специфічний елемент проведення аудиту.

Дослідження засвідчують, що ІТ-аудит охоплює такі сфери перевірки: комп'ютерно-інформаційна система; стан архівування та зберігання інформації; рівень контролю комп'ютерної обробки інформації; співставність здійснюваних алгоритмів нормативній документації; гнучкість реагування на зміну законодавчого регулювання програмного забезпечення; можливість збільшення масштабів комп'ютерно-інформаційних систем; стан інформаційної безпеки; стан інформаційної політики; рівень розвитку інформаційних технологій.

У ході ІТ-аудиту використовують аудиторське програмне забезпечення, яке складається із пакета програм, програм спеціального призначення та програм-утилітів. Для того, щоб якісно здійснити ІТ-аудит, необхідно мати досконало опрацьовані схеми перевірки, а також ефективний рівень контролю за виявленням і виправленням помилок. Окрім того, якість ІТ-аудиту залежить професіоналізму аудиторів та послуг, які вони надають.

Найчастіше на практиці під час здійснення IT-аудиту керуються стандартами COBIT Control Objectives for Information and related Technology), розробленими незалежною міжнародною асоціацією ISACA (The information Systems Audit and Control Association). Відтак, ці стандарти націлені на ефективне і раціональне удосконалення усіх взаємопов'язаних бізнес-процесів підприємства. Результати від застосування стандартів COBIT передбачають отримання інформації про поточний технічний стан підприємства та проведення комплексної інвентаризації програмного забезпечення і обладнання. Як засвідчує практика функціонування вітчизняних підприємств, однією із причин утримання або відтермінування IT-аудиту виступає вартість послуг, якщо підприємство використовуватиме послуги зовнішніх аудиторів. Однак, що стосується внутрішнього аудиту, то тут можливо є такий варіант, коли підприємство чекає на нового працівника чи вже його залучило, оскільки стовідсотково довіряє йому проведення внутрішнього аудиту. Як наслідок, одержується інформація про стан IT-структури підприємства та представляються рекомендації по його модернізації.

Послуги у сфері IT-аудиту нині надають такі організації (міжнародні, професійні чи державні), як:

- Міжнародна організація бухгалтерів (IFAC);
- Міжнародна організація вищих органів фінансового контролю (INTOSAI);
- Міжнародна організація зі стандартизації– (ISO);
- Фундація аудиту і контролю інформаційних– систем (ISACF);
- Інститут стратегічного управління інформаційними технологіями (ITGI);
- Інститут внутрішніх аудиторів (IIA) та багато– інших менш відомих.

Таким чином, внаслідок проведеного IT-аудиту отримується інформація про рівень ефективності функціонування IT-середовища, а також його основних складових частин.

Результати проведеного огляду та аналізу існуючих публікацій засвідчують, що IT-аудит виступає складовою частиною процесу стратегічного управління підприємством. З'ясовано, що з року в рік все більшої популярності набуває використання послуг IT-аудиту серед вітчизняних суб'єктів господарювання. Встановлено, що IT-аудит дозволяє формувати висновки про реальний стан захисту IT-ресурсів, а також рівень їх здатності протистояти внутрішнім та зовнішнім загрозам, що виникають у середовищі функціонування.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Астахова М. М. Використання комп'ютерних інформаційних систем при проведенні аудиту резервів і забезпечень підприємства / М. М. Астахова // Наукові праці Кіровоградського 30 національного технічного університету. Економічні науки: збірник наукових праць – 2007. – Вип. 12, Ч. 1. – С. 319–324. – URI: http://dspace.kntu.kr.ua/jspui/handle/123456789/873 (дата звернення 13.05.2023).
2. Бенько М. М. Інформаційні технології як фактор інтеграції внутрішнього і зовнішнього аудиту / М. М. Бенько, В. В. Сопко // Економічний форум. – 2015. – № 1. – С. 254–262. – URL: http://nbuv.gov.ua/UJRN/ecfor_2015_1_44 (дата звернення 13.05.2023).
3. Голяш І. Д. Аудит безпеки підприємства у сфері застосування інформаційних технологій / І. Д. Голяш, С. І. Саченко // Бухгалтерський облік, контроль і аналіз. – 2012. – С. 90–95. – URL: http://dspace.tneu.edu.ua/handle/316497/22636 (дата звернення 13.05.2023).
4. Гребешков О. М. Стратегічний інформаційний аудит як інструмент розробки інформаційної стратегії підприємства / О. М. Гребешков // Вісник Національного університету "Львівська політехніка". – 2010. – № 683. – С. 202–205. – URL: http://ena.lp.edu.ua:8080/bitstream/ntb/20292/1/41- 202-205.pdf (дата звернення 13.05.2023).
5. Гужва В. М. Інформаційні системи і технології на підприємствах: [навч. посібник] / В. М. Гужва. – К.: КНЕУ, 2001. – 400 с. – URL: http://www.dut.edu.ua/uploads/l_1366_68707543.pdf (дата звернення 13.05.2023).
6. Данилюк І. IT- аудит: проблеми та перспективи / І. Данилюк // Модернізація національної системи управління державним розвитком: виклики і перспективи. – 2016. – Ч. 2. – С. 75–77. – URL: http://econf.at.ua/publ/konferencija_2016_12_8_9/sekcija_5_ekonomichni_ nauki/it_audit_problemi_ta_perspe ktivi/61-1-0-1467 (дата звернення 13.05.2023).
7. Денисенко М. П. Інформаційне забезпечення ефективного управління підприємством / М. П. Денисенко, І. В. Колос // Економіка та держава. – 2006. – № 7. – С. 19–24. – URL: http://dspace.nuft.edu.ua/jspui/handle/123456789/2214 (дата звернення

13.05.2023).
8. Івахненков С. В. Поняття комп'ютерного контролю та аудиту / С. В. Івахненков // Менеджмент: збірник наукових праць. – 2009. – Вип.11. – 225 с. – С. 24– 38. – URL: http://ekmair.ukma.edu.ua/bitstream/handle/123456789 /644/Ivakhnenkov_Poniattia%20kompiuternoho.pdf (дата звернення 13.05.2023).
9. Москаленко Ф. І. Проблемні питання проведення аудиту інформаційних систем у сучасних умовах / Ф. І. Москаленко // Таврійський науковий вісник. Економічні науки. – 2013. – № 84. – С. 327–332. – URL: http://irbis-nbuv.gov.ua/cgibin/irbis_nbuv/cgiirbis_64.exe?C21COM=2&I21DBN =UJRN&P21DBN=UJRN&IMAGE_FILE_DOWNLOAD=1&Image_file_name=PDF/Tavnv_2013_84_66.pdf (дата звернення 13.05.2023).
10. Нога І. М. Діагностика ефективності застосування інформаційних технологій в управлінні підприємствами / І. М. Нога, Р. М. Скриньковський, Г. Павловські // Бізнес Інформ. – 2016. – № 9. – С. 241–245. – URL: http://www.businessinform.net/export_pdf/business-inform-2016-9_0-pages-241_245.pdf (дата звернення 13.05.2023).
11. Огнева А. М. Аудит інформаційних систем і технологій / А. М. Огнева // Вісник Хмельницького національного університету. Серія: Економічні науки. – 2009. – № 6, Т. 1. – С. 229–232. – URL: http://journals.khnu.km.ua/vestnik/pdf/ekon/2009_6_1/pdf/229-232.pdf (дата звернення 13.05.2023).
12. Pawlowski, G., Skrynkovskyy, R., Shpak, O., & Vizniak, Y. (2017). Development of the Model of the System of Managerial Diagnostics of the Enterprise on the Basis of Improvement of Diagnostic Purposes. Path of Science, 3(11), 4010-4020. doi: http://dx.doi.org/10.22178/pos.28-9 (дата звернення 13.05.2023).
13. Письмаченко Л. М. Сучасні інформаційні технології обліку та аудиту в управлінні підприємством / Л. М. Письмаченко, В. Г. Васильєва, І. В. Яковенко // Інвестиції: практика та досвід. – 2010. – № 9. – 43– 47. – URL: http://nbuv.gov.ua/UJRN/ipd_2010_9_14 (дата звернення 13.05.2023).
14. Пугаченко О. Б. Особливості аудиту інформаційних систем і технологій / О. Б. Пугаченко // Наукові праці Кіровоградського національного технічного університету. Економічні науки. – 2009. –

Вип. 16(2). – С. 223–228. – URL: http://nbuv.gov.ua/UJRN/Npkntu_e_2009_16%282%2 9__38 (дата звернення 13.05.2023).
15. Редченко К. І. Інформаційні технології та аудит: стратегічний контекст / К. І. Редченко // Вісник Національного університету "Львівська Політехніка". Менеджмент та підприємництво в Україні: етапи становлення і проблеми розвитку. – 2012. – № 722. – С. 386–389. – URL: http://ena.lp.edu.ua:8080/bitstream/ntb/12529/1/74_386-389_Vis_722_menegment.pdf (дата звернення 13.05.2023).
16. Ус Р. Л. Аудит інформаційних технологій – новий вид аудиту організацій / Р. Л. Ус // Формування ринкових відносин в Україні. – 2013. – № 1. – С. 81–86. – URL: http://nbuv.gov.ua/UJRN/frvu_2013_1_21 (дата звернення 13.05.2023).
17. Ус Р. Л. Аудит інформаційних технологій як складова системи аудиту організацій / Р. Л. Ус // Формування ринкових відносин в Україні. – 2011. – № 1. – С. 163–168. – URL: http://nbuv.gov.ua/UJRN/frvu_2011_1_40 (дата звернення 13.05.2023).
18. Чумаченко Г. В. Організація управління малими та середніми підприємствами з використанням інформаційних технологій: автореф. дис. ... канд. екон. наук: 08.06.02 – підприємництво, менеджмент та маркетинг / Г. В. Чумаченко; Східноукраїнський державний університет. – Луганськ, 1999. – 20 с.
19. Янчев А. Питання управління та оцінки інформаційних технологій / А. Янчев // Економіст – 31 вересень, 2011. – № 9. – С. 50–52. – URL: http://nbuv.gov.ua/UJRN/econ_2011_9_13 (дата звернення 13.05.2023).
20. Buchanan S. The information audit: An integrated strategic approach / S. Buchanan, F. Gibb // International Journal of Information Management. – February 1998. – Volume 18, Issue 1. – Pages 29–47. – URL: https://doi.org/10.1016/S0268-4012(97)00038-8 (дата звернення 13.05.2023).
21. Kim H.-J. Information technology acceptance in the internal audit profession: Impact of technology features and complexity / Hyo-Jeong Kim, Michael Mannino, Robert J. Nieschwietz // International Journal of Accounting Information Systems. – December 2009. – Volume 10, Issue 4. – Pages 214–228. – URL: https://doi.org/10.1016/j.accinf.2009.09.001 (дата звернення 13.05.2023).
22. Robson K. Transforming audit technologies: Business risk audit

methodologies and the audit field / Keith Robson, Christopher Humphrey, Rihab Khalifa, Julian Jones // Accounting, Organizations and Society. – May–July 2007. – Volume 32, Issues 4–5. – Pages 409–438. – URL: https://doi.org/10.1016/j.aos.2006.09.002 (дата звернення 13.05.2023).
23. Janvrin D. An Examination of Audit Information Technology Use and Perceived Importance / Diane Janvrin, James Bierstaker, D. Jordan Lowe // Accounting Horizons. – March 2008. – Volume 22, No. 1. – Pages 1–21. – URL: https://doi.org/10.2308/acch.2008.22.1.1 (дата звернення 13.05.2023).
24. IT-аудит – инструмент стратегического управления компанией: Матеріали української компанії “Baker Tilly in Ukraine”. – URL: http://www.bakertilly.ua/media/IT_audit_russ.pdf (дата звернення 13.05.2023). (дата звернення 13.05.2023)
25. Матвіюк Р. IT-аудит: для кого і для чого? / Роман Матвіюк // Журнал “Незалежний аудитор” – URL: http://nauditor.com.ua/uk/component/na_archive/309?view=m aterial (дата звернення 13.05.2023).

Контрольні запитання

1. Назвіть нарямки, на які поділяється аудит інформаційних систем.
2. Які етапи охоплює проведення аудиторської перевірки?
3. Які сфери перевірки охоплює IT-аудит?
4. Розкажіть про аудиторське програмне забезпечення, яке використовується у ході IT-аудиту.
5. Назвіть міжнародні організації, які надають послуги у сфері IT-аудиту.

2. ВНУТРІШНІЙ АУДИТ ЗА ВИМОГАМИ ISO/IEC 27001 ТА ISO 19011

Процес внутрішнього аудиту є необхідним для будь-якої системи менеджменту. Планування та проведення внутрішніх аудитів вимагається стандартами ISO 9001, ISO 14001, OHSAS 18001 та іншими. Стандарт ISO/IEC 27001, що висуває вимоги для Системи менеджменту інформаційної безпеки (СМІБ), також містить обов'язкову вимогу щодо проведення внутрішнього аудиту. При проведенні аудиту СМІБ важливо дотримуватися усіх принципів, описаних в ISO 19011, які відносяться до аудиту систем менеджменту. В усіх питаннях, пов'язаних з аудитом СМІБ, аудитор має бути незалежним від об'єкта аудиту. Функція аудиту в організації повинна бути незалежною від ділянки, що перевіряється, для отримання об'єктивних результатів. Інформаційна безпека є сферою, яка динамічно розвивається. У цьому зв’язку важливо, щоб аудитори інформаційної безпеки (ІБ) були постійно в курсі сучасних загроз, уразливостей і ситуації в організації (бізнес-процесів, технологій, стосунків).

2.1. Загальна характеристика внутрішніх аудитів СМІБ

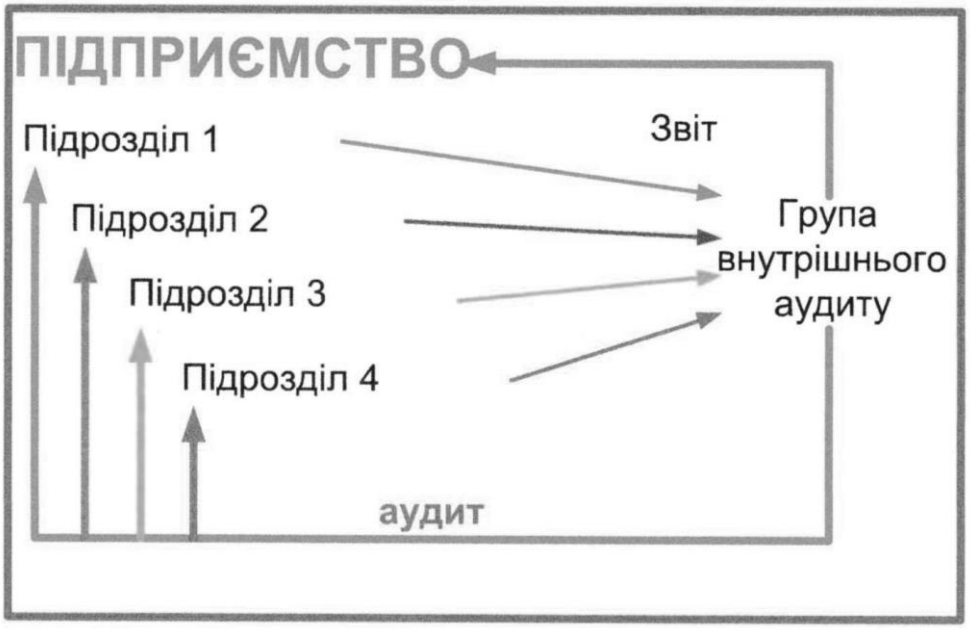

Рис. 2.1. Аудит внутрішній (аудит першої сторони, внутрішня перевірка)

Внутрішній аудит (рис. 2.1) – це самоперевірка, тобто аудит власних процесів силами самого підприємства. Цей процес є ключовим для СМІБ. Внутрішній аудит – основний інструмент вищого керівництва для реалізації політики і цілей системи менеджменту. В рамках даного процесу підприємство має можливість побачити реальну ситуацію, оцінити реальний рівень забезпечення ІБ і здійснювати постійну підтримку СМІБ. Метою

проведення внутрішніх аудитів є перевірка того, що система менеджменту:
а) відповідає встановленим вимогам;
б) результативно впроваджена і підтримується в робочому стані.

Результат внутрішнього аудиту, як правило у формі звіту, необхідний для виконання аналізу СМІБ з боку вищого керівництва. Проведення такого аналізу є також обов'язковою вимогою стандарту ISO/IEC 27001.

Розглядаючи вимоги ISO/IEC 27001 щодо організації процесу внутрішнього аудиту складно детально і поетапно уявити собі цей процес. Для організації адекватного процесу варто розглянути розділ 6 стандарту ISO/IEC 27001 і стандарт ISO 19011 (рис. 2.2). Рекомендації щодо організації процесу аудиту містяться в ISO/IEC 19011 «Керівні вказівки для аудиту систем менеджменту».

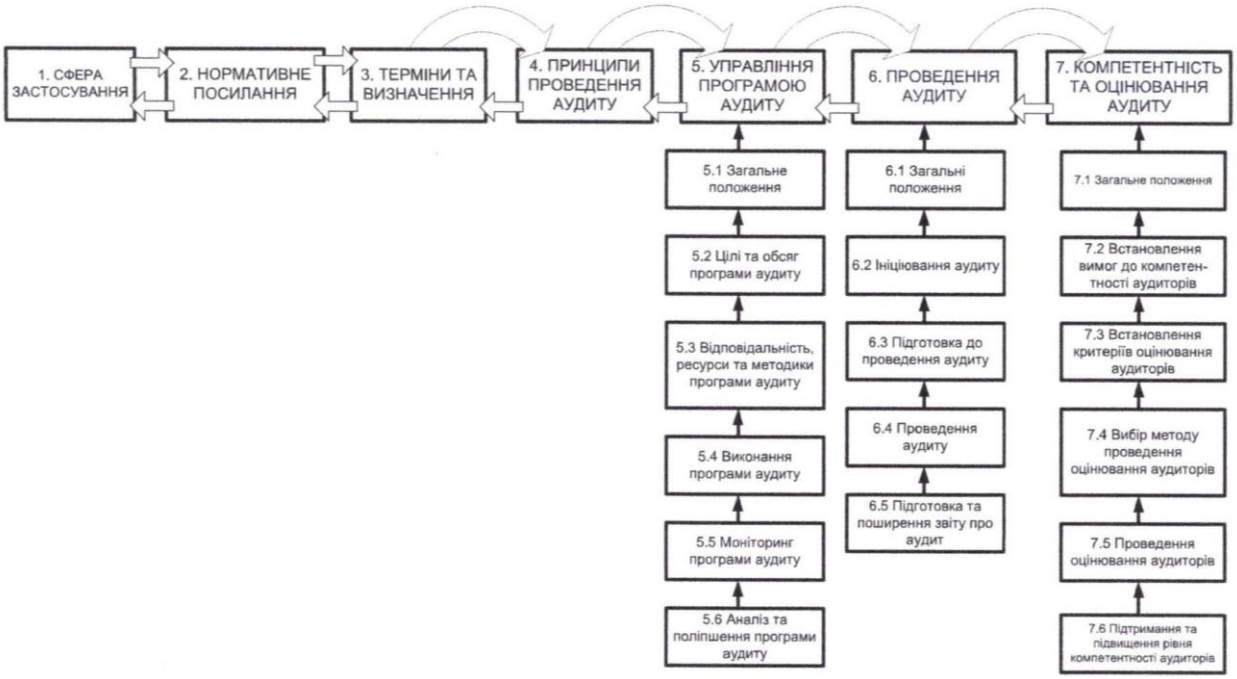

Рис. 2.2. Структура стандарту ISO 19011-2011 «Керівні вказівки для аудиту систем менеджменту»

Дані рекомендації застосовуються при проведенні перевірок усіх систем менеджменту, наприклад, якості (ISO/IEC 9001), інформаційної безпеки (ISO/IEC 27001), професійної безпеки та охорони праці (на відповідність OHSAS 18001), систем управління безпеки харчових продуктів (HACCP), безпеки морського судноплавства (ISM Code) тощо.

Ґрунтуючись на положеннях цих стандартів, а також на практичному досвіді, варто відзначити той факт, що деталі процесу внутрішнього аудиту можуть відрізнятися в залежності від специфіки та внутрішньої організації

кожного підприємства. Для ознайомлення з таким процесом розглянемо типовий приклад його реалізації (рис.2.3).

Рис. 2.3. Модель процесу внутрішнього аудиту

Алгоритм організації та проведення внутрішніх аудитів (рис. 2.4.):

0) РОЗРОБКА ПРОЦЕДУРИ ВНУТРІШНІХ ПЕРЕВІРОК СМІБ. Стандарт ISO/IEC 27001 вимагає наявності документованої процедури внутрішніх аудитів. Цей документ повинен відображати всі правила й етапи процесу внутрішнього аудиту. У ньому може бути відображений алгоритм організації та проведення внутрішніх аудитів, а також опис кожного етапу алгоритму. Крім того, гарною 36 практикою вважається підкріплення даної процедури бланками протоколів, необхідних для реалізації процесу.

1) ПІДБІР І НАВЧАННЯ КОМАНДИ АУДИТОРІВ. Для проведення внутрішнього аудиту необхідні кваліфіковані кадри. Внутрішні аудитори повинні володіти знаннями як мінімум у двох сферах: знати вимоги стандарту ISO/IEC 27001 і знати процес внутрішнього аудиту. Крім того, внутрішньому аудитору вкрай необхідно знати ділянку, що перевіряється, виробничі процеси і розуміти призначення тих чи інших інформаційних активів у підрозділах. Корисним може виявитися навчання внутрішніх аудиторів СМІБ на спеціалізованих курсах в сертифікаційних або консультаційних компаніях. Однак це не є вимогою стандарту ISO/IEC 27001. Спеціалісти підприємства можуть самостійно отримати необхідні знання шляхом самоосвіти та самопідготовки. У цьому випадку варто

потурбуватися про те, щоб провести атестацію внутрішніх аудиторів і документально підтвердити факт відповідності внутрішніх аудиторів власним вимогам підприємства.

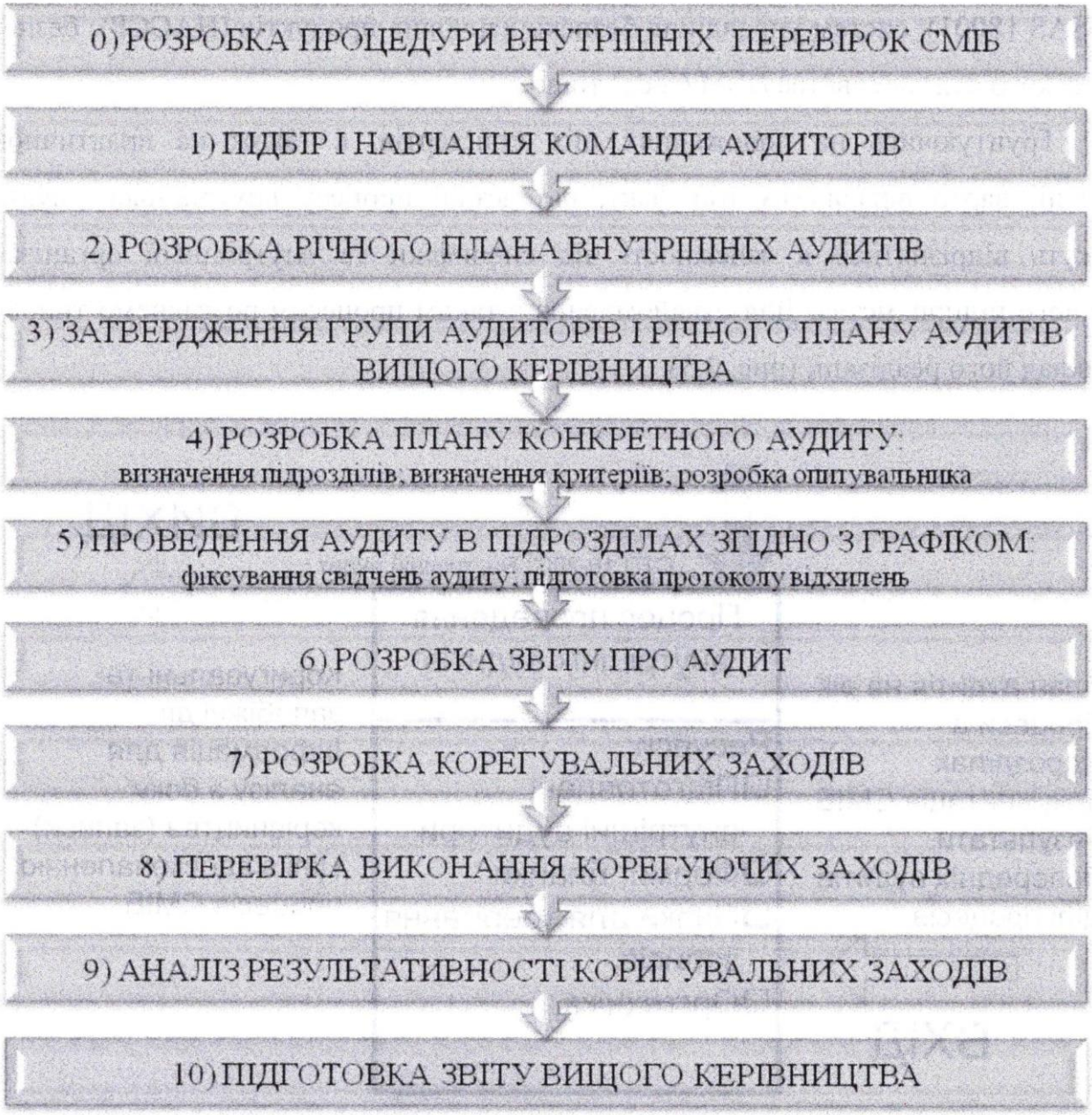

Рис. 2.4. Алгоритм проведення внутрішніх аудитів

З точки зору вимог ISO/IEC 27001, на підприємстві повинен бути як мінімум один внутрішній аудитор. З практичної точки зору, необхідну кількість аудиторів варто визначати, виходячи з їх здатності реалізувати річну програму аудитів. Відомі випадки, коли внутрішні аудити підприємства проводять за допомогою сторонніх організацій. Це не заборонено стандартом. Однак це не виключає необхідності планування і

фіксації висновків за результатами аудитів. Як приклад, можна привести організацію процесу внутрішнього аудиту СМІБ в одному з регіональних відділень великого банку, кількість персоналу в якому становить трохи більше 500 осіб. Банк має три внутрішні аудитори, які є співробітниками служби ІБ. Близько 40% аудитів проводять сторонні організації. Зокрема аудит ІС проводять представники консалтингової компанії, що працює у сфері ІБ. Також залучаються окремі фахівці для реалізації тестів на вторгнення. Для аудиту питань фізичної безпеки залучаються фахівці охоронної фірми. Розглянемо інший приклад – виробниче підприємство, на якому працюють більше 2000 осіб. Задіяні два штатних внутрішніх аудитора СМІБ. Крім того, до групи аудиту в різний час підключаються близько двадцяти аудиторів тільки на момент аудиту підрозділів підприємства. Важливо при підборі команди аудиторів забезпечити об'єктивний і неупереджений процес внутрішнього аудиту.

2) РОЗРОБКА ПРОГРАМИ ВНУТРІШНЬОГО АУДИТУ НА РІК. При проведенні внутрішніх аудитів систем менеджменту найчастіше обмежуються плановими аудитами. Ці аудити плануються заздалегідь, представники підрозділів, які підлягають аудиту, заздалегідь сповіщаються про дати його проведення. Незважаючи на відсутність раптовості, саме такий підхід надає внутрішньому аудиту результативності. Аудитор у цьому випадку стає помічником у виявленні слабких місць. При такому підході підрозділи стають активними співучасниками процесу перевірки. Аудит перестає бути схожим на перевірку податковою інспекцією. Однак, при цьому, не варто забувати про те, що контролю потребує уся система безпеки. А це означає, що проблеми в одному з напрямків можуть призвести до того, що всі роботи в рамках СМІБ виявляться марними. Наприклад, порушення правил по роботі з комерційними пропозиціями можуть призвести до втрат, зіставних із річним доходом підприємства. Тому, поряд з плановим аудитом, при аудиті СМІБ часто використовують й інші види аудитів. Серед цих видів варто виділити такі три: позаплановий внутрішній аудит, пошук загроз та моделювання загроз. Розглянемо дані види аудиту у контексті необхідності їх використання в тому чи іншому випадку.

Позаплановий внутрішній аудит дуже схожий на плановий за одним виключенням. Представників підрозділу, що перевіряється, не попереджають про прихід внутрішніх аудиторів. Цей вид аудиту застосовують у тому випадку, коли існують побоювання, що персонал приховує факти при планових аудитах. При цьому внутрішні аудитори не здатні це довести в

рамках планових аудитів. Також позаплановий аудит може бути проведений при виникненні небезпечних ризиків у певний момент часу. Наприклад, у зв'язку з ремонтом пропускного пункту на підприємстві застосовується тимчасова схема, що використовує нестандартні правила. Зловживати позаплановими аудитами не варто. Це може призвести до того, що персонал буде бачити в цьому процесі тільки негатив. Внутрішнім аудиторам припинять показувати реальні проблеми, перестануть бачити в них помічників, здатних вирішувати нагальні проблеми. В результаті цінність усього процесу внутрішнього аудиту може бути втрачена.

Наступний вид аудиту – пошук загроз. Найчастіше даний вид аудиту базується на реєстрі активів і ризиків. Пошук загроз застосовується в двох випадках:

1) існують важливі або складні активи. Відповідальний за СМІБ не володіє об'єктивними даними про ці активи та ризики для них. Прикладом такого активу може бути велика інформаційна система класу ERP (Enterprise resource planning), яка обслуговує все підприємство.

2) існують активи, ризики для яких не достатньо зрозумілі. Можливо, також є сумнів в адекватності проведеної оцінки ризиків. Прикладом може бути така ситуація. У приміщенні зберігається архів з конструкторською документацією. Протягом довгого часу надходять скарги про відсутність необхідних папок. Служба ІБ у повному обсязі реалізує заплановані заходи для усунення даної проблеми. Однак результатів це не приносить. Для реалізації пошуку загроз найчастіше вдаються до послуг сторонніх організацій. Серед них - постачальники певного активу, консультаційні компанії та ін.

Найбільш екстремальний вид аудиту – моделювання загроз. Даний аудит проводять для практичного виявлення можливих наслідків відомих ризиків, а також для визначення невідомих ризиків. При цьому внутрішній аудитор самостійно реалізує ризик і відстежує наслідки даної дії. Наведемо приклади. Іноді може бути корисним відключити електричне живлення в серверній, приховано вилучити важливу папку з документами, цілеспрямовано ввести в ІС завідомо неправдиві дані і т.д. Важливо перед реалізацією моделювання загроз узгодити даний процес з керівництвом підприємства, оцінити можливі наслідки і попередити при необхідності задіяні підрозділи. Хоча моделювання загроз може бути вкрай корисним, зловживати ним не варто. Це може завдати серйозної шкоди підприємству.

Важливо пам'ятати, що незалежно від обраного виду аудиту необхідно

повністю дотримуватися документованої процедури внутрішнього аудиту. Тому у випадку, якщо будуть використовуватися додаткові види аудиту, їх обов'язково необхідно описати в процедурі внутрішнього аудиту. Також обов'язково ці аудити необхідно відобразити в усьому ланцюжку документації процесу внутрішнього аудиту. При розробці програми аудитів на рік (рис.2.5) найкраще використовувати шаблон, який зручно змінювати. Підприємство – це живий механізм, тому часто виникає необхідність внесення змін до програми протягом року. Запропонована форма програми аудитів має два позитивних моменти: зручність внесення змін і наочність. Завдяки наочності представлення даних, виключається можливість пропустити той чи інший елемент СМІБ. Вкрай важливо затвердити річну програму у вищого керівництва. Це дозволить уникнути розбіжностей при узгодженні і проведенні кожного виду аудиту в підрозділах.

ВАТ "XYZ"
Програма аудитів на _____ рік

Версія 2.3 від ____.____ 2014

Затверджую
Голова правління
ВАТ "XYZ"

_____ Мороз І.І.
___.___ 2014

Критерії / Підрозділи	Внутрішні вимоги СМІБ	4	5	6	7	8	A5	A6	A7	A8	A9	A10	A11	A12	A13	A14	A15	Місяць
Служба IT	П				П		П	П	П	В		М	У				П	1
Відділ постачання	П			П		П												2
Технічний відділ		П				П									В		П	2
Служба якості	П	П			П	П			М		П					П		4
Служба діловодства	П				П								П					5
Ділянка синтезу	П				П	П							П					8
Ділянка пакування	П				П	П								У				11
Склади	П																	2
Вище керівництво	П		П			П	П								П			1

Вид аудиту	Скорочення
* Плановий внутрішній аудит	П
* Позаплановий внутрішній аудит	В
* Пошук загроз	У
* Моделювання загроз	М

Погоджено: _____ підпис _____ Уповноважений СМІБ _____ дата

Розроблена: _____ підпис _____ Головний аудитор СМІБ _____ дата

Рис. 2.5. Приклад програми аудитів на рік

3) РОЗРОБКА ПЛАНУ АУДИТУ ПРОТЯГОМ РОКУ. При впровадженні та підтримці СМІБ в якості критеріїв найчастіше використовують:
- стандарт ISO/IEC 27001;
- внутрішні процедури та інструкції;
- плани з обробки ризиків.

Такий набір критеріїв у процесі становлення і зростання системи, як правило, залишається незмінним. Змінюється тільки роль кожного критерію. При першому внутрішньому аудиті найбільше приділяють увагу вимогам стандарту ISO/IEC 27001. Результати аудиту за даним критерієм можуть з великою часткою впевненості сказати нам про результативність всієї роботи з впровадження СМІБ. На другому і третьому році життя найбільший інтерес в якості основного критерію складають внутрішні правила і процедури. У цей момент приходить усвідомлення того, що саме виконання власних внутрішніх норм дозволить забезпечити належний рівень безпеки. За умов адекватно працюючої системи, коли виконуються вимоги внутрішніх норм, на перше місце як критерій виходять плани з обробки ризиків. У цьому випадку основний об'єкт внутрішнього аудиту – заходи, зафіксовані в плані з обробки ризиків. Необхідно переконатися, що заплановані заходи виконані і їх реалізація принесла очікуваний результат. Стандарт ISO/IEC 27001 вимагає адекватного розподілу сил при проведенні внутрішнього аудиту: «Програма аудитів повинна бути спланована з урахуванням статусу та важливості процесів і ділянок, які необхідно перевіряти, а також результатів попередніх аудитів». Для реалізації даної вимоги необхідно розуміти критерії збільшення тривалості аудиту того чи іншого процесу (рис. 2.6). Система СМІБ обумовлює необхідність розподілу зусиль за допомогою ризиків. Тому перед початком розробки річної програми аудитів варто провести облік активів і повний аналіз ризиків. Відштовхуючись від результатів аналізу ризиків, доцільно збільшувати частоту і тривалість кожного аудиту протягом року в тих місцях, де існують найбільш високі ризики. Таким чином, ризики – це перший критерій для збільшення тривалості внутрішнього аудиту. Другий за важливістю критерій пов'язаний із необхідністю усунення відхилень, які були виявлені під час попередніх аудитів. На деяких підприємствах у процесі багаторазових внутрішніх аудитів виявляються одні й ті ж проблеми. Це свідчить про те, що система менеджменту та процес внутрішнього аудиту працюють не адекватно. Саме внутрішні аудитори повинні робити все для усунення повторюваних проблем. Третій критерій – масовість інформаційних активів. Найчастіше при аудиті СМІБ велику кількість активів зосереджено на двох процесах: паперовому і електронному документообігу. Скупчення активів в одному процесі або в одному приміщенні має змусити нас приділити більше уваги пошуку існуючих і потенційних проблем.

Рис. 2.6. Критерії, що впливають на тривалість внутрішнього аудиту

Важливість перерахованих трьох критеріїв збільшення тривалості внутрішнього аудиту різна. Найбільш значущим критерієм завжди повинен залишатися перший, пов'язаний з високими ризиками. Менш значущим – останній критерій, пов'язаний з високим скупченням активів. Натомість, переглядаючи плани кількох підприємств, доводиться спостерігати з року в рік одну і ту ж помилку. Велику частину часу і сил внутрішні аудитори витрачають у службі діловодства та службі ІТ, зосереджуючи увагу на великому скупченні паперових документів, папок, файлів, баз даних і т.д. Згідно з річною програмою аудитів складаються окремі плани для кожного аудиту (рис. 2.7). Ці плани мають бути конкретними і детальними. Розробка плану є важливим елементом як для групи внутрішніх аудиторів, так і для підрозділів, що перевіряються.

План проведення аудиту ВАТ "XYZ"

Вид аудиту: плановий

Керівник аудиту Мороз І.І.	Група аудиторів Петров П.П.,Сідоров С.С.	Дата аудиту: 01.02.2014	Критерії: ISO/IEC 27001, процедури СМІБ
Час	Підрозділ	Учасники аудиту	Елементи перевірки
9.00 - 9.30	Відділ постачання	Начальник відділу	4, А5-А15, процедури СМІБ
9.30 - 11.30	Відділ постачання	Зам. начальника відділу	5, 6, 7, процедури СМІБ
11.30 - 13.30	Відділ постачання	Старший менеджмер	5, А8, процедури СМІБ
14.30 - 15.30	Технічний відділ	Начальник відділу	А9, процедури СМІБ
15.30 - 17.00	Технічний відділ	Зам. начальника відділу	А7, А9-А15, процедури СМІБ

Розроблено: _____ підпис _____ _____ дата
Головний аудитор СМІБ

Погоджено: _____ підпис _____ _____ дата
Відділ постачання

Погоджено: _____ підпис _____ _____ дата
Технічний відділ

Затверджено: _____ підпис _____ _____ дата
Уповноважений з СМІБ

Рис. 2.7. Приклад складання плану внутрішнього аудиту

У кожному плані необхідно вказати: вид аудиту, групу аудиторів, дату і час аудиту, критерії, перелік підрозділів, що перевіряються, та елементи перевірки. У випадку проведення планових аудитів плани направляються у підрозділи, що підлягають аудиту, заздалегідь (зазвичай за 10-20 днів). За цей період група аудиту повинна погодити план з урахуванням специфіки виробництва, наявності фахівців на місцях і логістичних особливостей.

4) РОЗРОБКА АНКЕТ ВІДПОВІДНО ДО КРИТЕРІЇВ АУДИТУ. Стандарт ISO/IEC 27001 не вимагає наявності підготовлених опитувальників для внутрішніх аудиторів. Тобто перелік вимог, виконання яких перевіряє внутрішній аудитор, може міститися в голові аудитора. Також критеріями можуть слугувати 44 стандарт ISO/IEC 27001 або внутрішні процедури підприємства. Однак все ж рекомендується заздалегідь підготувати чіткі і зрозумілі опитувальники для проведення внутрішнього аудиту. Такі опитувальники надають можливість перевірити усі можливі вимоги, не випустивши з уваги аудиторів ніяких моментів. Крім того, самостійна підготовка опитувальника допоможе детально вивчити вимоги, описані в критеріях. Саме цей крок є одним з найдієвіших для вивчення і розуміння стандарту. Підготовка опитувальників – досить простий для розуміння процес. Його суть полягає в тому, щоб скласти перелік питань відповідно до критеріїв внутрішнього аудиту. Необхідно пункт за пунктом пропрацювати

весь стандарт або внутрішню процедуру. Приклад опитувальника, складеного за окремим пунктом стандарту ISO/IEC 27001 наведено в табл. 2.1.

Таблиця 2.1

Приклад опитувальника для проведення внутрішнього аудиту

	Питання	**Тип питання**
1.	Чи задокументовані функції Вашого відділу та обов'язки співробітників?	Закрите
2.	Назвіть цілі Вашого відділу у сфері забезпечення безпеки?	Відкрите
3.	Як Ви розумієте свою роль у Політиці інформаційної безпеки?	Відкрите
4.	Якими документами з безпеки керується підрозділ у роботі?	Відкрите
5.	Чи існує їх перелік?	Закрите
6.	Як збігається конструкторська і технічна документація?	Відкрите
7.	Хто має право входити в архів з документацією?	Відкрите
8.	Чим це регламентовано?	Відкрите
9.	Які проблеми з документацією у Вас існують?	Відкрите
10.	А в електроному вигляді?	Відкрите
11.	Як давно Вам змінювали пароль на вхід до системи?	Відкрите
12.	Ви проходили навчання з інформаційної безпеки?	Закрите

При підготовці опитувальника можна використовувати відкриті й закриті питання. Закриті питання припускають відповіді «Так» або «Ні». Відповіді на відкриті питання заздалегідь передбачити неможливо. Важливо розуміти, що використання закритих питань робить опитувальник дуже визначеним, сам процес аудиту стає схожим на експрес-тест. Закриті питання мають свої переваги та недоліки. Великий мінус закритого питання в тому, що в самому питанні міститься відповідь. Також досить складно за допомогою закритих питань отримати від респондента повний ланцюжок фактів. Кращим способом є комбіноване застосування закритих і відкритих питань. При цьому рекомендується значно збільшити частку відкритих питань.

5) ПІДГОТОВКА ДО ПРОВЕДЕННЯ АУДИТУ НА МІСЦІ. Для того, щоб аудит міг принести адекватні результати, необхідно добре знати ділянку, що

перевіряється, і мати в руках необхідний пакет інструментів. Для вивчення ділянки, що перевіряється, необхідно ознайомитись зі звітом про аудит в даному підрозділі за минулий період, переліком активів і звітом про оцінку ризиків, процедурами та інструкціями підрозділів. Крім того, необхідно озброїтися засобами для фіксації фактів. Отже, стандартний пакет аудитора може виглядати таким чином:

1) стандарт ISO/IEC 27001.
2) звіти про аудити за минулий період з чітким зазначенням виявлених відхилень.
3) реєстр активів з розбивкою по підрозділах або процесах.
4) реєстр ризиків з розбивкою по підрозділах або процесах.
5) процедури та інструкції підрозділів.

Канцелярія:

1) бланки для ведення рукописних записів (блокнот).
2) бланки для реєстрації невідповідностей (відхилень).
3) планшет для зручності ведення записів на виробництві.
4) дві кулькових ручки.
5) візитні картки.

Проведення аудиту в підрозділах зручно починати зі вступної наради. На даній нараді вкрай бажаною є присутність першого керівника. Під час наради оголошуються критерії аудиту, графік аудиту, представляється група аудиторів, і висвітлюються їх повноваження. Крім того, оголошується порядок визначення невідповідностей та процес апеляції за виявленими невідповідностями. Опитування респондентів у підрозділах зручно проводити вдвох. Це дає можливість одному аудитору зосередитися на опитуванні, а другому – фіксувати виявлені факти. Гарною практикою вважається фіксація всіх виявлених фактів, у тому числі позитивних. Це дасть можливість детально проаналізувати не тільки слабкі, але й сильні місця СМІБ. Для фіксації фактів зручно використовувати заздалегідь заготовлений бланк (рис. 2.8). Використання таких бланків дає можливість у будь-який час, в тому числі після аудиту, звернутися до фактів з чіткою ідентифікацією.

Виявлені у процесі аудиту проблеми називають відхиленнями або невідповідностями. Розглянемо, що може бути відхиленням.

Відхилення:

- це умова, що впливає або може мати шкідливий вплив на інформаційні активи;

- втрата одного або декількох властивостей ІБ;

- це пряме або непряме порушення вимог СМІБ, тобто вимог стандарту ISO/IEC 27001 чи внутрішніх процедур СМІБ.

ВАТ "XYZ" **Рукописні записи** Аудитори:	Лист _____ из _____ Дата:	
Найменування підрозділу, що перевіряється	Пункт стандарту (процедури)	П*
Текст, Текст, Текст, Текст, Текст, Текст, Текст, Текст Текст, Текст, Текст, Текст, Текст, Текст, Текст, Текст Текст, Текст, Текст, Текст, Текст, Текст, Текст, Текст		
* номер протоколу відхилення		

Рис. 2.8. Приклад бланків для фіксації результатів внутрішнього аудиту

Також аудитору важливо розуміти, що різні відхилення мають різне значення для СМІБ і для підприємства. Тому доцільно розрізняти критичні і некритичні відхилення. Критичне відхилення передбачає часткове невиконання вимог елемента СМІБ, але при цьому має серйозні наслідки. Приклад: «Тільки одна людина з відділу по роботі з клієнтами не знайома з правилами СМІБ, хоча весь відділ пройшов навчання згідно з графіком». Відхилення також вважається критичним, коли повністю або в більшості випадків не дотримуються вимог одного або декількох елементів СМІБ. Приклад: «Немає процедури і робочого процесу резервного копіювання інформації. Повністю не дотримуються вимоги пункту А.10.5 стандарту ISO/IEC 27001». Відхилення некритичне, коли вимоги елемента якості виконуються не повністю, але відхилення не може спричинити значних негативних наслідків. Приклад: «Було встановлено факт, що 1 раз з 15 згідно з графіком не було проведено резервне копіювання». Кожне з виявлених відхилень доцільно зафіксувати в окремому бланку (рис. 2.9).

При реєстрації відхилення важливо відзначити наступні факти:

- місце виявлення відхилення;
- дату (час) виявлення;
- опис невідповідності;

- групу аудиторів;
- відповідальну особу – представника підрозділу, що перевіряється;
- номер бланка.

ВАТ "XYZ"
Протокол відхилення

Місце перевірки: Служба управління IT	Пункт стандарту, положення внутрішньої процедури A. 10.5 ISO/IEC 27001	Дата: 16.04.13 Номер 3

НЕВІДПОВІДНІСТЬ
Відсутня політика резервного копіювання. Резервне копіювання не виконується на вузлах М5, М3.

АУДИТОРИ		**ВІДПОВІДАЛЬНА ОСОБА**
1. Мороз І.І.	2. Петров П.П.	Александров О.О. _____ (підпис)

КОРИГУЮЧІ / ПОПЕРЕДЖУВАЛЬНІ ДІЇ,

ПРИЙНЯТІ ДЛЯ ДОСЛІДЖЕННЯ НЕВІДПОВІДНОСТІ

1. Розробити політику резервного копіювання
2. Розробити і виконати графік резервного копіювання

СРОК ВИПРАВЛЕННЯ: 20.05.13

ПЕРЕВІРКА ЕФЕКТИВНОСТІ ВИКОНАННЯ КОРЕГУЮЧИХ ЗАХОДІВ
Додатковий аудит через 3 місяці з метою підтвердження здійснення резервного копіювання.

НЕЗАДОВІЛЬНЕ ВИКОНАННЯ КОРЕГУЮЧОГО ДІЇ	**ЗАДОВІЛЬНЕ ВИКОНАННЯ КОРЕГУЮЧОГО ДІЇ**
ПІДПИС: **ДАТА:**	**ПІДПИС:** Мороз І.І. **ДАТА:** 25.05.13

Рис. 2.9. Приклад складання протоколу відхилень

Факти відхилень повинні бути узгоджені до того, як аудитори залишать зону аудиту та перейдуть до іншої. Відомості про відхилення мають бути зрозумілими за змістом як учасникам аудиту, так і тим, хто не брав участь в ньому. Після фіксації виявлених фактів доцільно ознайомити з ними підрозділ, що перевіряється, письмово.

Можливі причини відхилень:

- розглянуті документи не містять вимог до ІБ;
- вивчені процеси (документи, записи СМІБ) не відповідають вимогам процедур СМІБ або вимогам стандарту ISO/IEC 27001;
- документи не застосовуються на практиці або не дотримуються їх обов'язкові вимоги;
- прийнята практика неефективна, тобто необхідні результати не

досягаються.

На підсумковій нараді, як правило, оголошують виявлені невідповідності і дають можливість перевіреним підрозділам їх оскаржити. Це створює атмосферу довіри між тими, хто перевіряється, і аудиторами. Також вкрай важливою є присутність на підсумковій нараді першого керівника.

6) РОЗРОБКА ЗВІТУ ПРО АУДИТ. За результатами аудиту розробляється звіт. Найчастіше подібні звіти досить громіздкі. Кращою практикою вважається розробка короткого звіту. Фактично він може являти собою всього лише одну сторінку (див. рис. 2.10).

Затверджую
Уповноважений з СМІБ
ВАТ "XYZ"

_____ Петров П.П.
____.____. 2014

ЗВІТ №
про проведення внутрішнього аудиту

_____
(найменування підрозділу)

Вид аудиту: Критерії:	Результат	виявлено відхилення: з них значних: незначних:

П.І.П., підписи аудиторів: _____

Дата:

+ Протоколи відхилень

Рис. 2.10. Приклад бланка звітності про результати внутрішнього аудиту

На цій єдиній сторінці описують загальні параметри аудиту та загальну статистику відхилень. До цієї сторінки додають копії протоколів відхилень.

7) РОЗРОБКА КОРЕГУВАЛЬНИХ ТА ЗАПОБІЖНИХ ЗАХОДІВ. На підставі визначених відхилень необхідно спланувати корегувальні і/або запобіжних заходів. Ці заходи мають бути спрямовані на усунення причин реальних або потенційних невідповідностей. Даний перелік доцільно фіксувати в протоколі відхилень. Розробку корегувальних та запобіжних заходів найчастіше здійснює підрозділ, у якому виявлено невідповідність. Це найбільш адекватний підхід. Однак для вироблення корегувальних або

запобіжних дій можуть залучатися фахівців інших служб підприємства. Також практикується залучення сторонніх організацій для складних інформаційних активів. Важливо після узгодження корегувальних та запобіжних заходів визначити плановий термін їх реалізації. Саме цей термін необхідний команді аудиторів для подальшої перевірки.

8-9) ПЕРЕВІРКА ВИКОНАННЯ ЗАХОДІВ І АНАЛІЗ РЕЗУЛЬТАТИВНОСТІ. Стандарт ISO/IEC 27001 вимагає проводити перевірку виконання запланованих раніше корегувальних та запобіжних заходів. Це прямий обов'язок внутрішніх аудиторів. Окрім визначення самого факту реалізації заходів, внутрішні аудитори повинні проаналізувати результативність вжитих дій. Найчастіше заплановані та реалізовані заходи не усувають причин невідповідностей. Тільки після перевірки результативності реалізованих заходів конкретний аудит можна вважати завершеним.

10) ПІДГОТОВКА ЗВІТУ для вищого керівництва. Завершуючи річну програму аудитів, необхідно підготувати зведений звіт для вищого керівництва. Це обов'язкова вимога стандарту ISO/IEC 27001. Звіт про внутрішній аудит є найважливішим документом для аналізу СМІБ з боку вищого керівництва. На початку звіту найкраще не загострювати увагу на конкретних особистостях і всіх виявлених відхиленнях. Це може негативно позначитися на долі багатьох співробітників підприємства, при цьому рівень СМІБ необов’язково покращиться. Краще оперувати загальними зведеними даними. Такими як: загальна кількість відхилень, кількість критичних відхилень, характер критичних відхилень. Загострити увагу керівництва необхідно на тих проблемах, які не вирішуються без участі керівництва. Такі проблеми необхідно чітко висвітлити. У цьому випадку іноді доцільно говорити про особистості та інші деталі проблем. При підготовці звіту важливо розуміти його значення для служби ІБ. Найбільш серйозні відхилення слід висвітлити, завдяки чому отримати ресурси на найнеобхідніше. Керівництво підрозділу, що перевіряється, має забезпечити своєчасне виконання корегувальних заходів (без необґрунтованої затримки), щоб усунути виявлені невідповідності та їх причини. Аудитори повинні перевірити виконання та ефективність вжитих корегувальних та запобіжних заходів, і зробити відмітку за результатами перевірки.

Якщо корегувальні заходи не виконані або виконані недостатньо ефективно, аудитор відзначає це в бланку невідповідності, а керівник підрозділу визначає нові корегувальні заходи та/або терміни їх виконання,

після чого відбувається наступна перевірка. Якщо в підрозділі, що перевіряється, не будуть усунуті невідповідності у повторно призначені терміни, аудитор ставить до відома про це керівництво для прийняття відповідних заходів. Слід зауважити, що відхилення – це лише симптоми серйозних причин. Необхідно з'ясувати справжню причину, щоб розпізнати реальні масштаби проблеми і визначити потенціал для її вирішення.

Отже, алгоритм усунення невідповідностей:

1) визначити явну причину відмови в системі.
2) визначити причину потенційної невідповідності.
3) визначити корегувальні заходи.
4) визначити запобіжні заходи.
5) виконати корегувальні та запобіжні заходи (при необхідності).
6) забезпечити контроль виконання та ефективності корегувальних та запобіжних заходів.

Приклад вимог до процедур з внутрішнього аудиту. Представник керівництва за системою менеджменту ІБ відповідає за:

- планування аудитів з урахуванням важливості процесів і ділянок, а також результатів попередніх аудитів;
- організацію проведення аудитів (хто? коли?...).
- забезпечення звітності про аудити, що є основою для аналізу, оцінювання та вдосконалення процесів СМІБ. До 10 січня поточного року інженер з ІБ розробляє програму проведення внутрішніх аудитів на рік, керуючись при цьому:
- результатами минулих аудитів;
- важливістю процесів і ділянок, що перевіряються;
- станом роботи підрозділів, планом проведення капітальних ремонтів в цехах тощо. План погоджує представник керівництва з СМІБ і затверджує голова правління. Аудит конкретного підрозділу проводиться не менше 1 разу на рік. Програма аудиту включає:
- всі елементи ISO/IEC 27001;
- підрозділи підприємства, в яких перевіряється даний елемент;
- прізвища призначених аудиторів, термін перевірки (місяць).

Інженер з ІБ знайомить призначених аудиторів з програмою під підпис. Керівництво підприємства може призначити позаплановий аудит у випадку серйозних порушень в СМІБ. Підрозділ, що підлягає аудиту, ставиться до відома про це не менше, ніж за 24 години. Якщо обсяг аудиту передбачає залучення кількох людей, представник керівництва призначає старшого в цій

групі. Призначений аудитор несе відповідальність за планування, підготовку, проведення та складання звітності про виконання аудиту.

Підготовка до аудиту включає:

- вивчення процедури «Внутрішній аудит»;
- вивчення процедур по процесам, які перевіряються;
- складання переліку контрольних питань.

Старший групи аудиторів несе відповідальність за планування аудиту:

- узгодження дати; - складання плану;
- призначення індивідуальних завдань;
- підготовку звітності з аудиту;
- аудит на адекватність;
- організацію нарад аудиторів (при необхідності);
- представлення групи аудиторів і проведення вступної та підсумкової нарад.

Контрольні запитання

1. Якими стандартами вимагається планування та проведення внутрішніх аудитів?
2. Надайте загальну характеристику внутрішніх аудитів.
3. Яка тривалість внутрішнього аудиту?
4. Надайте алгоритм організації та проведення внутрішніх аудитів.
5. Надайте алгоритм усунення невідповідностей.

3. ПРИНЦИПИ ПРОВЕДЕННЯ ВНУТРІШНЬОГО АУДИТУ

Особливістю проведення внутрішніх аудитів є довіра до них, яка ґрунтується на низці принципів. Останні забезпечують результативність і надійність аудиту як інструменту підтримки політик, методів і засобів управління шляхом подання інформації, на основі якої організація може здійснювати комплекс заходів, спрямований на удосконалення своєї діяльності. Дотримання цих принципів є передумовою для отримання висновків з аудиту, які мають бути доречними (стосуватися справи) і обґрунтовані, а також для того, щоб аудитори, діючи незалежно один від одного, були спроможні отримувати в схожих ситуаціях однакові висновки. Такими принципами є:

1) цілісність як основа професіоналізму. Аудиторам і особі, яка здійснює управління програмою аудиту, слід:

- здійснювати свою роботу чесно, старанно і відповідально;
- використовувати усі можливі правові вимоги і діяти відповідно до них; - демонструвати свою компетентність при виконанні своєї роботи;
- здійснювати свою роботу неупереджено, тобто зберігати справедливість і об'єктивність щодо всього, з чим доводиться мати справу;
- бути уважними до будь-яких впливів, що, як можна очікувати, чинитимуть тиск на прийняття рішень при проведенні аудиту.

2) неупереджене надання результатів – це зобов'язання надавати правдиві і точні звіти. Результатами аудиту, висновками з аудиту і звітами про аудити слід правдиво і точно відображати діяльність з проведення аудитів. Істотні перешкоди, що з'являються під час аудиту, а також протиріччя і розбіжності між командою з аудиту та організацією, що перевіряється, слід відображати в звіті. Спілкування між зазначеними суб’єктами має бути чесним, точним, об'єктивним, своєчасним, зрозумілим і повним.

3) належна професійна ретельність, що полягає у виявленні старанності і прояві розсудливості при проведенні аудиту. Аудиторам слід приділяти увагу ретельності, яка повинна відповідати важливості виконуваного ними завдання, щоб зберегти довіру, надану їм замовником аудиту та іншими зацікавленими сторонами. Важливим фактором виконання аудиторської діяльності, що забезпечує належний рівень професійної ретельності, є здатність приймати обґрунтовані рішення в усіх ситуаціях, що виникають під час аудиту.

4) конфіденційність полягає у захисті отриманої інформації. Аудиторам слід проявляти обережність у роботі з інформацією, яку вони отримують у зв'язку

із здійснюваною ними діяльністю. Інформацію, отриману під час аудиту, не слід використовувати в цілях отримання вигоди для аудиторів або замовника аудиту або таким чином, який завдає шкоди законним інтересам аудиторської організації. Даний підхід передбачає належне поводження з «чутливою» або конфіденційною інформацією.

5) незалежність – це основа неупередженості при проведенні аудиту та об'єктивності висновків аудиту. Аудиторам, де це тільки можливо, слід бути незалежними від діяльності, яка буде піддаватися аудиту, і у всіх випадках діяти таким чином, щоб бути вільними від упередженості і конфлікту інтересів. При проведенні внутрішніх аудитів аудиторам необхідно бути незалежними від керівників функціональних структур, що підлягають аудиту. Аудиторам слід зберігати об'єктивність під час усього процесу аудиту з тією метою, щоб результати аудиту та його висновки були засновані тільки на даних (свідченнях) аудиту. Для невеликих організацій, можливо, буде достатньо, щоб внутрішні аудитори були повністю незалежними від діяльності, що піддається аудиту, але при цьому слід докласти всіх зусиль, щоб виключити упередженість і забезпечити об'єктивність.

6) підхід, заснований на даних. Цей принцип полягає у тому, щоб кожного разу отримувати надійні та відтворювані висновки за результатами аудитів, що систематично проводяться. Дані аудиту мають бути верифікованими. У загальному випадку вони будуть базуватися на вибірках доступної (отриманої в розпорядження) інформації, оскільки аудит проводиться в обмежений період часу і з обмеженими ресурсами. Слід використовувати відповідні (доречні, підходящі) вибірки прикладів, оскільки це значно впливає на довіру до висновків аудиту.

Дев’ять правил успішного проведення аудиту:

1) аудитор – НЕ диктатор, а мотиватор удосконалення.

2) підрозділи, що перевіряються, не повинні боятися аудиту.

3) аудитор повинен допомагати тим, хто підлягає перевірці, розпізнавати проблеми і домагатися усунення їх причин.

4) діалог з тими, хто піддається перевірці, повинен сприяти покращенню.

5) аудитор повинен чітко уявляти цілі підрозділу.

6) процеси системи менеджменту якості мають бути документованими. Кращий посібник для переліку питань з аудиту – це опис процесу.

7) результати аудиту також повинні документуватися.

8) процеси СМІБ мають бути перевірені на: а) досяжність цілей відповідностей із заданими значеннями процесів; б) актуальність заданих

значень; в) ефективність заходів для досягнення цілей.
9) аудит повинен передбачати постійне відслідковування виявлених проблем.

Контрольні запитання

1. У чому полягає особливість проведення внутрішніх аудитів?
2. Охарактеизуйте цілісність як основу професіоналізму.
3. Що таке неупереджене надання результатів?
4. У чому заклечається підхід, заснований на даних?
5. Розкажіть про правила успішного проведення аудиту.

4. ОСОБЛИВОСТІ РЕАЛІЗАЦІЇ АГЕНТСЬКОГО ПЕРЕХОПЛЕННЯ

Часто в компаніях більше уваги приділяють зовнішнім загрозам: спаму і фішинг-атакам типу "відмова в обслуговуванні", вірусам (троянському ПЗ, хробакам), підміні головних сторінок інтернет-ресурсів, шпигунському і рекламному програмному забезпеченню, соціальному інжинірингу. Але насправді внутрішні загрози здатні завдати компанії значно серйознішої шкоди, ніж зловмисники за її межами.

У принципі будь-який працівник компанії може бути потенційним інсайдером і поставити інформаційну безпеку під загрозу. Від злого наміру або банальної помилки не застрахований ніхто: від найнижчої ланки і до топ-менеджменту.

Принцип роботи DLP-системи простий і полягає в аналізі всієї інформації: вихідної, вхідної та тієї, що циркулює всередині компанії. Система за допомогою алгоритмів аналізує, що це за інформація, і в разі, якщо вона критична і надсилається туди, куди їй не належить, - блокує передачу та/або повідомляє про це відповідального співробітника. Основа DLP - набір правил. Вони можуть бути будь-якої складності і стосуватися різних аспектів роботи. Якщо хтось їх порушує, то відповідальні особи отримують повідомлення.

Так, наприклад, у компанії X виявили співробітника, який займався майнінгом криптовалют. Це було виявлено під час використання модуля активності користувачів. Звіт показав, що робоча станція не відключалася на ніч. Після перегляду запущених процесів з'ясувалося, що співробітник перед відходом запускав процес майнінгу. Система відстежує не тільки час роботи й активні програми на комп'ютері, а й будь-яку іншу роботу з інформацією, - введення даних з клавіатури, листування та передавання файлів поштою, у соцмережах і месенджерах, документи, які надсилають на друк, час простою, SIP-телефонію, активність на сайтах і багато іншого.

Способи перехоплення даних. Для того, щоб аналізувати дані, DLP-система спершу повинна їх отримати. Є два основні способи перехоплення - серверний і агентський. У першому випадку система контролює мережевий трафік на сервері, через який комп'ютери "спілкуються" із зовнішнім світом. У другому випадку спеціальні невеликі програми, так звані агенти, встановлюються на всі комп'ютери організації і передають з кожної машини дані для аналізу. Агентське перехоплення є більш поширеним, адже за його допомогою можна отримати набагато більше даних із різних каналів комунікації, а отже, і надійніше запобігти можливим витокам.

DLP-системи та законодавство. Сама DLP-система, а також процедура її впровадження при правильному виконанні відповідає вимогам цивільного законодавства, т.к. система моніторить виключно робочий процес, а не приватне життя людини.

Неочевидні способи використання DLP-системи. Здавалося б, система, створена для контролю витоку даних, більше нічим не може бути корисна. Однак сучасні DLP мають й інші можливості, неочевидні на перший погляд:

- аналіз завантаженості персоналу. Багато DLP-систем здатні вести облік робочого часу співробітників. Робочий процес кожного користувача можна представити у вигляді статистики, яка дає змогу проаналізувати, наскільки співробітник залучений у трудовий процес.

- забезпечення юридичної підтримки. Завдання DLP полягає не тільки в тому, щоб запобігти витоку, а ще й за наявності судового розгляду, надати докази зловмисної діяльності.

- DLP як інструмент мотивації. Коли співробітники усвідомлюють, що їхня трудова діяльність перебуває під моніторингом, з'являється більша відповідальність за робочий процес. І це своєю чергою призводить до поліпшення клімату в колективі.

- DLP як сховище. DLP-технологія гарантує збереження всієї інформації, оскільки містить у своєму архіві всі комунікації співробітників, до яких у разі потреби можна буде звернутися.

Додатки-агенти являють собою програми або сервіси, що здійснюють перехоплення трафіку з робочих станцій мережі, а не з мережевих шлюзів. Їхнє використання припадає до речі, коли немає можливості застосувати інші методи перехоплення, такий самий, як дзеркальне. В ідеалі агенти встановлюються на всі призначені для користувача пристрої, чи то смартфони, ноутбуки, чи то інші пристрої. У принципі, такий метод навіть кращий за попередній, оскільки контролює набагато більше каналів зв'язку, а також уміє працювати з шифрованим трафіком за необхідності. Контроль потоку даних йде буквально по всіх фронтах: зовнішні пристрої, файлові документи, месенджери, пошта тощо. Але все ж кілька мінусів є і в такого способу перехоплення.

По-перше, це залежність від операційної системи, тому що для кожної системи має бути свій агент.

По-друге, створюється додаткове навантаження на мережу.

По-третє, агент може бути виявлений, оскільки встановлюється на користувацьких пристроях, але це вже дрібниці. ПЗ, інтегроване в сторонні

продукти, наприклад, у корпоративні додатки або поштові сервери (поштові сервіси MS Exchange, Lync, Lotus тощо) найчастіше застосовують для збирання інформації з проксі-серверів або напряму з поштових серверів, оброблення отриманих даних і записування їх у базу даних.

Відмінність від мережевого перехоплення полягає в тому, що адреса, з якої відстежується трафік, буде не мережевого адаптера, а адреса сервера і порт. Крім такого типу інтеграції існують і DLP-системи, що впроваджуються не тільки в додатки, а й у мережеві пристрої. Якщо бути точніше, впровадження проводиться не всієї системи, а будь-якої її частини. Порівняно з попередніми способами такий підхід є більш вузькоспеціалізованим, тому має використовуватися укупі з іншими. Знову ж таки, якщо порівнювати такий метод перехоплення з мережевим, інтегрування передбачає ще меншу кількість каналів, які можливо буде контролювати.

Особливості реалізації агентського перехоплення трафіку. Такий метод перехоплення трафіку передбачає збір інформації на рівні робочих станцій користувачів. На кожен комп'ютер у компанії встановлюється спеціальне ПЗ - агент, який відстежує всі операції співробітників, зазвичай у режимі, непомітному для користувачів. В ідеалі агенти також встановлюються на особисті нотубуки, смартфони та інші гаджети, якими під час роботи користуються співробітники. Принцип роботи такого методу досить простий, якщо не вдаватися в подробиці: агент відстежує роботу з будь-якими документами, а також розмежовує доступ до них. Якщо документ захищений, а у користувача недостатньо прав на виконання операцій з документом, то доступ до нього блокується, а співробітник служби безпеки повідомляється про спробу. Інакше кажучи, агент - співробітник секретної служби, який хапає зловмисника за рукав, коли той бере з полиці чужу книжку. Сучасні системи обросли додатковим функціоналом і на сьогодні вміють не тільки "хапати за рукав". Ось основна частина умінь, якими можуть володіти агентські DLP системи:

1) перехоплення отриманих/відправлених даних, таких як:

- дані, що передаються через інтернет-браузер;
- історія операцій з файлами, що знаходяться на контрольованих пристроях або файл-серверах;
- дані, що копіюються на зовнішні пристрої;
- повідомлення, що передаються через месенджери (AIM, ICQ, Mail agent, MSN, Jabber, Google Talk та інші);

- електронна пошта, поштові протоколи (POP3, SMTP, MAPI, IMAP, NNTP, протоколи веб-пошти: EWS KOC OWA ZWC, а також інші);
- дані, отримані/відправлені через FTP-з'єднання;
- скріншоти екранів моніторів;
- запис голосів користувачів;
- текстовий і голосовий зв'язок по Skype;
- дані, відправлені на друк фізичних або віртуальних принтерів;
- інформація, що передається за допомогою мобільних пристроїв.

2) перехоплення даних, що передаються зашифрованим з'єднанням;

3) занесення всіх перехоплених даних у базу даних;

4) прикріплення до перехоплених даних атрибутів: час і дата перехоплення, MAC- і IP-адреси, доменне ім'я і домен, користувацькі дані (ім'я принтера, логіни, поштові адреси відправника й одержувача та інше);

5) додавання індексів, створюваних для аналізу перехопленої інформації та контекстного пошуку за ними;

6) зберігання історії подій і налаштувань у базі даних.

Такий великий функціонал, якщо він цілком поєднується в одній системі, може, як не дивно, накладати деякі проблеми. Агенти впливають на продуктивність комп'ютерів.

По-перше, не секрет, що чим більше дій виконує система, тим сильніше виходить завантаженість. Також виявляється завантаженою і мережа, оскільки кожен ПК або інший пристрій з агентом періодично робить запити до бази сигнатур документів для оновлення даних.

По-друге, перед будь-якою дією (відкриття, друк, копіювання) з документом виконується визначення його сигнатури, порівняння зі зразком та інші операції. Слабке "залізо" просто буде довго виконувати всі ці процеси, а операційна система - підвисати по кілька секунд.

Ще один з найбільш значущих недоліків - налаштування агентської системи запобігання витокам. Адже їй потрібно задати всі файли, які потрібно захищати, розмежувати доступ для користувачів, а також періодично поповнювати й оновлювати базу конфіденційних файлів.

Також мінусом можна відзначити ціну - адже агент встановлюється на кожен пристрій, а ліцензія за одну штуку в середньому коштує недешево. Встановлення будь-якої з розглянутих систем у компанії чисельністю 1000 осіб обійдеться мінімум у кілька десятків тисяч доларів. Принцип роботи агентського модуля і DLP-систем загалом можна розділити на кілька частин. Послідовність дій наведено в табл.4.1.

Сучасні DLP-системи містять у собі набір готових правил реагування на витік інформації, наприклад, форм фінансової звітності, даних кредитних карт і паспортів. Це набагато спрощує початкове налаштування системи адміністратором/офіцером інформаційної безпеки компанії. Якщо розглядати роботу агентського модуля окремо від інших, можна виділити певний план дій. Як уже йшлося раніше, на робочі станції встановлюють агенти, які виконують перехоплення документів та іншої інформації, а також її копіювання на керуючий сервер. Керуючий сервер заносить перехоплену інформацію (месенджерів, повідомлення електронної пошти, текстові та голосові сеанси зв'язку в Skype, скріншоти з екранів моніторів тощо) до бази даних. У деяких випадках запис даних, відправлених на зовнішні пристрої, і даних, переданих за протоколом FTP, для зручності відбувається окремо - у файлове сховище. Перехоплення налаштовується відповідно до потреб і обмежується за спеціальними атрибутами, наприклад, за MAC- або IP-адресою. Для перегляду документів і швидкого пошуку за ними база даних і файлове сховище індексуються. Якщо передбачена функція оновлення індексів, то оновлення відбувається автоматично, за заданим розкладом. Так само за розкладом відбувається перевірка. Керуючий сервер сканує індекси та документи за заданими критеріями пошуку й автоматично надсилає адміністратору (співробітникові служби безпеки) сповіщення, якщо було виявлено інцидент. Адміністратор зі своєї робочої станції через клієнт переглядає історію інцидентів, історію активності користувачів та інші дані залежно від заданого фільтра. Через ту саму робочу станцію здійснюється управління серверною частиною.

Таблиця 4.1

Принцип роботи системи

Процедура	**Опис процедури**	**Роль учасників з боку бізнес-підрозділів**
Навчання системи принципам класифікації інформації	Занесення в систему принципів виявлення та класифікації конфідеційних даних	Власники інформаційних ресурсів беруть участь у класифікації інформації

Введення правил реагування	Налаштування правил реагування системи на виявлену інформацію і груп співробітників, дії яких будуть контролюватися. Додаються винятки для довірених користувачів	Служба безпеки розробляє й уточнює правила захисту ресурсів
Виконання системою операцій контролю	Система аналізує інформацію (локальні дії користувачів, вихідні інформаційні потоки, результати сканування мережевих ресурсів і робочих станцій). Виконується порівняння з принципами виявлення і класифікації даних. У разі знаходження конфідеційних даних система порівнює їх з наявними політиками, налаштованими на виявлену категорію інформації. У разі порушення в системі створюється інцидент	Офіцери безпеки або відповідальні люди з боку власників ресурсів отримують повідомлення про інциденти, що сталися
Обробка інцидентів	Отримані інциденти в системі можуть бути налаштовані на такі правила реагування, як проінформувати/призупинити/заблокувати відправку. Ба більше, статистична інформація та подробиці щодо інцидентів доступні для аналізу офіцером безпеки/аудитором/власником ресурсу в системі. Унаслідок опрацювання офіцером безпеки інцидент може бути закритий/ескальований/спрямований на допрацювання політик	

Також через свій клієнт адміністратор може змінювати параметри і виконувати такі дії, як: перегляд поточної активності системи, управління агентами загалом, створення і налаштування індексів, управління ліцензією на продукт, налаштування винятків системи (для виключення з обробки додатків або процесів) та інше. Для перехоплення інформації на підконтрольні користувацькі станції мають бути інстальовані агенти з підключеними модулями перехоплення. Залежно від марки DLP-системи, модулі можуть відрізнятися. У сумі з усіх систем модулі можуть бути

приблизно такими: File, Device, Print, Mail, IM, HTTP, FTP, Monitor, Skype. Кожен із них відповідає тому типу інформації, який планується відстежувати. Для кожної з робочих станцій співробітників можна задавати індивідуальні параметри.

Налаштування агентів стало доволі тонким у кожній із розглянутих DLP-систем і може містити параметри, які будуть перелічені та розглянуті нижче. Загалом налаштування можуть бути загальними для всіх під'єднаних користувачів, індивідуальними для кожного з користувачів, або груповими (призначаються для групи користувачів).

Налаштування для груп зазвичай впливають на глобальні, які є для них вихідними, а призначені для користувача налаштування впливають і на групові, і на глобальні, оскільки використовують їхню основу і перекривають своїми власними параметрами. Такий взаємозв'язок називається ієрархічною структурою. Перший із параметрів, що впливає на працездатність, - це розмір дискового простору, який буде виділятися під тимчасове зберігання даних, що перехоплюються, у разі, якщо сервер завантажений або недоступний. Якщо розмір тимчасового сховища малий, дані будуть перезаписуватися поверх, а старі - видалятися. Також, якщо сервер недоступний, блокуватиметься вихідна пошта. У такому разі, залежно від системи, листи поміщаються в карантин, у тимчасове сховище або в чернетки листів.

За замовчуванням установлення агентів має здійснюватися на системний обліковий запис. Це налаштування також можна змінити і вибрати робочі станції, де обліковий запис буде змінено. Крім того, в деяких системах передбачено зміну налаштування запуску, заборонивши/дозволивши автозапуск під час старту операційної системи. Функція "Офлайновий режим" дає змогу змінити розклад передавання інформації на сервер агентами. Таке налаштування корисне в разі, коли потрібно знизити навантаження на мережу в умовах низької пропускної здатності каналу передавання даних.

Робота з індексами. Для виконання операцій з індексами в мережі або локально в системах запобігання витокам передбачена відповідна функція. Залежно від системи індекси можуть задаватися для системи в цілому, або для кожного з її модулів окремо. Це можуть бути й індекси протоколів: FTP, POP3, SMTP, NTP, HTTP та інші. мережевий трафік сервіс сніффер. Типові операції, які можуть бути зроблені з індексами:

- створення індексу;
- підключення індексу;

- видалення або очищення індексу;

- створення розкладу оновлення індексу;

- ручне оновлення індексу.

Параметри фільтрації. У цьому разі під фільтрацією розуміється обмеження перехоплення даних за певними атрибутами документів: MAC- і IP-адреси, користувач домену. Основне призначення цієї функції - прибрати з моніторингу будь-яких користувачів або груп користувачів (наприклад, керівництво компанії, відповідальні співробітники тощо). Можливі й інші причини, які вимагають обмеження перехоплення. Як альтернативу фільтрації перехопленої інформації може розглядатися інша дія - видалення агентських модулів з робочих станцій, з яких не потрібно контролювати курсування трафіку. Так чи інакше, фільтрація все ж важлива, якщо є робочі станції або термінальні сервери, які одночасно можуть знадобитися і "привілейованим" співробітникам, і тим, кого потрібно піддавати моніторингу. Якщо дивитися за узагальненою схемою, фільтрація відбувається на керуючому сервері (або на сервері управління). Процес фільтрації виконується за таким принципом:

- незалежно від параметрів, заданих для фільтрації, агенти, інстальовані на робочих станціях, роблять тіньове копіювання перехоплених даних і переспрямовують їх на керуючий сервер;

- керуючий сервер порівнює атрибути кожного отриманого пакета даних за заданими фільтрами. Якщо налаштування задано "за замовчуванням" (фільтри не було задано), фільтрації не відбувається, і абсолютно всі пакети даних надсилаються в базу даних.

Якщо фільтри були задані, то частина пакетів буде відсіюватися, не записуючись у базу даних. Керуючий сервер може фільтрувати трафік як за окремими каналами передавання даних (фільтри за протоколами), так і за всіма відразу (глобальні фільтри). Глобальні фільтри використовуються для всіх продуктів і протоколів. Фільтри за протоколами використовуються для задіяних протоколів. У будь-якому з двох випадків має бути обрано режим фільтрації, що забороняє або дозволяє. Переважно фільтрацію проводять за трьома основними атрибутами пакетів: за ім'ям локального користувача, за MAC-адресою локального користувача і за IP-адресою віддаленого або локального користувача.

Загальні правила роботи фільтрів:

- якщо функцію фільтрації ввімкнено, але в списку немає жодного фільтра, перехоплення буде виконуватися без обмежень за адресами; - щоб

пакет даних потрапив під одну з дій ("дозволити" або "заборонити" перехоплення), достатньо, щоб виник збіг за якимось із атрибутів; - залежно від системи буває так, що одночасно можна використовувати або тільки дозвільні, або тільки заборонні фільтри;

- у разі заборонних фільтрів у базу даних надсилатимуться всі перехоплені пакети за винятком збігів за фільтрами;
- у разі задіяння фільтрів, що дозволяють, у базу даних буде надіслано всі перехоплені пакети, які збіглися з виставленими фільтрами.

Під час налаштування фільтрів за IP-адресами можуть використовуватися як окремі IP-адреси, так і діапазони IP-адрес, а також мережеві маски.

Також у DLP-системах передбачено налаштування винятків. Воно використовується для того, щоб робота агентів не заважала виконанню системних процесів, а також не впливала на програми, які позначені адміністратором безпеки як довірені. У такому разі стандартні системні процеси мають бути виведені з обробки агентами. Винятки такого типу процесів не можуть змінюватися, вони додаються за допомогою імпортування. Крім цього, можливі випадки, коли за наявності запущених агентів користувацькі програмні додатки (наприклад, модулі інших DLP-систем, антивіруси, банківські клієнти) перестають функціонувати. Так само поводитися можуть і різноманітні системи електронного документообігу при впливі на них агента. У разі виявлення неправильної роботи застосунків у системі, в якій встановлено агентський модуль, призначені для користувача застосунки заносяться до списку винятків. Для цього використовується попередньо встановлена функція виключення процесів. Крім того, процеси агентського модуля можуть бути додані до списку винятків конфліктуючих додатків. Особливо це стосується під час використання DLP-систем спільно з антивірусним програмним забезпеченням. Крім застосунків, до списку винятків слід заносити хости, що мають вбудований захист від моніторингу переданої інформації. Крім них слід враховувати і можливі шифровані з'єднання. Наприклад, деякі системи запобігання витокам (такі фірми, як Symantec і Searchinform) уміють працювати з трафіком, переданим за протоколом SSL. SSL - криптографічний протокол, що використовує асиметричну криптографію для автентифікації ключів обміну, симетричне шифрування для забезпечення конфіденційності, а також коди автентифікації повідомлень для цілісності повідомлень. Система здійснює перехоплення такого трафіку шляхом непомітної заміни оригінального сертифіката на свій.

Якщо через відгук на цю дію зв'язок перервався або система отримала повідомлення про помилку, то сервер має повернути з'єднанню оригінальний сертифікат, а програму - додати до списку виключень агента.

Розглянемо тепер модулі або, називаючи їх простіше, складові частини агентських DLP-систем, а також принцип їхньої роботи. Відверто кажучи, ті ж самі модулі можуть стосуватися і мережевих систем. Більшість передових сучасних систем запобігання витокам інформації є комплексними, тому досить складно розділити їх на окремі невзаємопов'язані частини. Проте основний комплект, набір модулів (способів) перехоплення інформації приблизно скрізь однаковий, за винятком деяких - десь більше, десь менше. Але все ж далі постараємося перерахувати всі з них. У різних системах такі агентські модулі називаються по-різному - у Infowatch це Monitor'и, у Searchinform це Sniffer'и, у Symantec узагалі немає загальної назви. Не в цьому суть. Їм усім можна дати одну загальну назву, близьку за значенням - сніффери (від англійського to sniff - нюхати). Сніффер - пристрій або програма для перехоплення та аналізу мережевого трафіку. Принцип роботи таких модулів, як і в сніфферів, полягає в "прослуховуванні" мережевого інтерфейсу за будь-яким одним або кількома протоколами передавання даних. Є ще варіант, коли модуль підключається в розрив каналу, і варіант, коли трафік відгалужується (повністю копіюється). Схема роботи агентської системи загалом була розглянута раніше.

Агент, встановлений на робочій станції, непомітно для користувача перехоплює дані. Весь перехоплений трафік проходить через декодер пакетів, який розпізнає і розділяє пакети за відповідними рівнями ієрархії. Далі йде подальше опрацювання й ухвалення рішень адміністратором безпеки.

Тепер розглянемо основні модулі, які присутні в тих чи інших системах:

Модуль контролю носіїв і процесів. Це програмний засіб, що здійснює аудит всіляких пристроїв і процесів, які виконуються на робочих станціях співробітників. Можливі варіанти того, що може відстежуватися і контролюватися:

- доступ до різних портів і приймачів (USB, COM, LPT, FireWire та ін.);
- бездротове передавання даних за технологіями Wi-Fi, Bluetooth, IrDA;
- підключення зовнішніх носіїв до робочої станції (смартфони, камери, SSD, флеш-накопичувачі, CD/DVD/BlueRay/флоппі диски, смарт-картки тощо);
- під'єднання аудіо/відео пристроїв, ігрових контролерів та інших пристроїв

введення; - копіювання тексту в буфер обміну;
- запуск будь-яких процесів і файлів.

Крім цього виконується перехоплення файлів, що копіюються на носії, якщо передбачена функція "тіньового копіювання". Додатково можлива наявність функції шифрування всіх даних, що передаються на зовнішні носії. Природно, що така програма насамперед убереже компанію від витоку великих обсягів інформації, яку інсайдер намагається скопіювати на зовнішній носій, тому що передати через інтернет не вдалося.

Файловий модуль контролю. Виконує контроль роботи з файлами, що зберігаються на серверах і загальних мережевих ресурсах, які містять чималі обсяги конфіденційної інформації, забороненої для поширення поза межами компанії. Переміщаючи документи з таких ресурсів, співробітники можуть використовувати корпоративні секрети ненавмисно або, наприклад, для особистої вигоди. Стеження за операціями з конфіденційними файлами на загальнодоступних мережевих ресурсах запобігає такому варіанту. У цьому і попередньому модулі, зазвичай передбачено варіант управління доступом до окремих файлів і до типів файлів (за розширенням).

Модуль контролю електронної пошти. Електронна пошта - ще один із найнебезпечніших каналів витоку, оскільки нею можна надсилати дані досить великих обсягів. Чим більше модуль підтримує поштових протоколів, тим вища ймовірність уникнути витоку. Модуль дає змогу відстежувати трафік як на рівні мережевих протоколів, так і робочих станцій.

Модуль контролю IM. IM (Instant Messenger) - клас програм для миттєвого обміну повідомленнями. Сюди належать ICQ, MSN, Mail.ru Агент, JABBER, Yahoo! Messenger, AOL IM, mIRC та інші. Месенджери досить поширені не тільки в суспільному житті, а й у корпоративному середовищі, тому часто використовуються офісними працівниками. У компанії Searchinform є невелика перевага перед іншими компаніями - модулі агентської частини ПЗ, MailSniffer і IMSniffer, мають додаткову стійкість до всіляких збоїв (перехоплення однаково виконуватиметься, навіть якщо сервера раптом стануть недоступними), а також можуть перехоплювати дані, що надсилаються за захищеними протоколами.

Модуль контролю хмарних сервісів. Хмарні сховища (Dropbox, Yandex Disk, Google Drive та інші) виконують функцію зберігання інформації прямо в інтернеті, на виділених сервісом під цю справу серверах. Тож ще одна небезпека - копіювання інформації в них та автоматична синхронізація сховищ із пристроями, якими користується працівник.

Модуль контролю AD. Active Directory - служба каталогів корпорації Microsoft для ОС сімейства Windows Server. Ця служба дає змогу адміністраторам використовувати групові політики для збереження однаковості налаштувань користувацького робочого середовища, встановлення ПЗ, оновлень та іншого. Відповідно контроль і аналіз подій журналів Active Directory дає можливість помітити підозрілі операції, які може виконати системний адміністратор компанії. Такий модуль, до того ж, дозволяє відстежувати і зберігати в базу даних події, які загрожують безпеці системи.

Модуль контролю виведення на друк, як можна здогадатися, стежить за вмістом документів, що відправляються на принтери. Усі дані перехоплюються, а вміст документів індексується і поміщається в базу для подальшого аналізу. Відстежуючи дані, що надсилаються на друк, можна не тільки запобігати випадковим/вмисним витокам інформації, а й частково оцінювати доцільність використання принтера співробітниками, щоб надалі уникнути зайвих витрат на папір і тонер.

Модуль контролю HTTP/HTTPS. Насамперед це відстеження дій співробітників на сторонніх сайтах. Як додаткова функція цього модуля - контроль розподілу робочого часу. Таким чином, можна стежити не тільки за тим, яку інформацію отримує/передає співробітник, а й за тим, чим зайнятий співробітник у робочий час.

Модуль контролю FTP. Протокол FTP (File Transfer Protocol) - стандартний протокол, який використовується для передавання файлів через TCP-мережі (наприклад, Інтернет). Цей протокол - один із засобів передавання величезних обсягів інформації, і його можуть використовувати погані співробітники компанії для надсилання цілих баз даних, архівів сканів конфіденційних документів, креслень та іншого.

Модуль контролю моніторів (зображення). Ця програма дає змогу перехоплювати інформацію, що відображається на екранах співробітників, якщо точніше - в режимі реального часу або через заданий інтервал часу робити скріншоти і записувати відео з екранів робочих станцій співробітників, а також копіювати отриману інформацію в базу даних. Деякі DLP-системи пропонують крім цього відстежувати стан екранів користувачів термінальних серверів, що працюють по RDP-з'єднанню (Remote Desktop Protocol - протокол віддаленого робочого столу).

Модулі контролю Skype та інших сервісів VoIP. Дають змогу перехоплювати інформацію, передану у вигляді голосових і текстових

повідомлень, а також у вигляді переданих файлів.

Звуковий модуль контролю або, простіше кажучи, своєрідний диктофон, що відстежує і записує будь-які звуки, які надходять на мікрофон. Дає змогу записувати будь-які розмови навколо або навіть прослуховувати їх у реальному часі як усередині організації, так і за межами (наприклад, під час відряджень). Запис голосу відбувається за допомогою будь-якого мікрофона, який буде виявлено системою (вбудована в ноутбук, на веб-камері, в гарнітурі тощо).

Модуль звітності - модуль, який допомагає співробітнику служби безпеки сформувати звіти за кожним співробітником за такими критеріями, як-от: час роботи за комп'ютером; статистика використання застосунків; час приходу й відходу людини на роботу та з роботи. Як можна помітити, у списку присутні і протоколи. Це не повний список протоколів, які можуть бути підконтрольні агентським модулям. Також варто зауважити, що мережеві протоколи можуть оброблятися не тільки агентами, встановленими на робочих станціях. Мережевий метод перехоплення інформації, описаний у попередньому розділі, також працює з протоколами. У комплексних системах запобігання витокам обов'язки розподіляються між усіма частинами (агентською, мережевою, інтегрованими рішеннями), але водночас усі компоненти діють взаємопов'язано.

Таким чином, адміністратор інформаційної безпеки компанії може контролювати будь-які дії співробітників, забороняючи, дозволяючи або вибірково обмежуючи їм доступ до засобів і процесів, що виконуються на робочих станціях

Контрольні запитання

1. Назвіть принцип роботи DLP-системи.
2. Які існують способи перехоплення даних?
3. Назвіть неочевидні способи використання DLP-системи.
4. Назвіть особливості реалізації агентського перехоплення трафіку.
5. Назвіть складові частини агентських DLP-систем.

5. ПРОГРАМНИЙ КОМПЛЕКС SEARCHINFORM ДЛЯ КОНТРОЛЮ МЕРЕЖІ

Витік важливої інформації або її ненавмисний «злив» можуть завдати бізнесу істотну шкоду. Як правило, джерелами таких загроз є недобросовісні або ущемлені в тому чи іншому аспекті співробітники компаній. Мотиви у співробітників можуть бути абсолютно різні: підкуп з боку конкурентів або зацікавлених осіб, шантаж, особиста вигода і багато іншого.

В умовах кризи проблема витоку інформації тільки зростає. Згідно проведених досліджень з'ясувано, що кількість спроб «зливу» інформації співробітниками компаній зростає щорічно, де 31,4% - це умисна крадіжка інформації (в тому числі збереження інформації на особистому носії «про всяк випадок» або через зміни роботи), 17,9% - випадкові «зливи» даних або результат діяльності соціальних інженерів. 50,7% - це інциденти, мотиви яких однозначно встановити не вдалося. У зв'язку з цим все більше компаній замислюється про надійний захист. Традиційно для захисту від витоків і контролю інформаційних потоків в організаціях застосовуються системи класу DLP.

В даної лекції ми докладно розглянемо як гарний приклад DLP-систему «Контур інформаційної безпеки SearchInform», розроблену вітчизняною компанією ТОВ «СёрчІнформ». У матеріалі будуть розглянуті архітектура рішення, системні вимоги і основні функціональні можливості продукту.

Архітектура рішення. «Контур інформаційної безпеки SearchInform» призначений для контролю інформаційних потоків в рамках локальної обчислювальної мережі. Контроль можливий двома способами, в залежності від використовуваного серверного компонента: SearchInform EndpointSniffer або SearchInform NetworkSniffer. Серверні компоненти являють собою платформи, на яких працюють модулі перехоплення даних. Кожен модуль перехоплення виступає в ролі аналізатора трафіку і контролює свій канал передачі даних.

«Контур інформаційної безпеки SearchInform» має модульну структуру, і умовно її можна згрупувати наступним чином (рис.5.1).

Модулі контролю інформації. SearchInform EndpointSniffer - платформа для перехоплення і блокування інформаційних потоків за допомогою агентів, встановлених на робочі станції. Платформа Endpoint дозволяє перехоплювати інформацію за допомогою агентів, які встановлюються на ПК співробітників. При цьому контролюються: інтернет, корпоративна і особиста електронна пошта, всі популярні месенджери (Viber, ICQ, і ін.),

Skype, хмарні сховища, FTP, Sharepoint, надання документів на принтери, використання зовнішніх пристроїв зберігання. Контролюється файлова система ПК, активність процесів і сайтів, контакти, натиснуті клавіші, віддалене онлайн-спостереження за ПК. Також агент дозволяє примусово шифрувати будь-які призначені для користувача дані, що записуються на носій. Доступний контроль як відкритих, так і шифрованих з'єднань. Можлива установка заборони на використання портів введення-виведення або певних пристроїв.

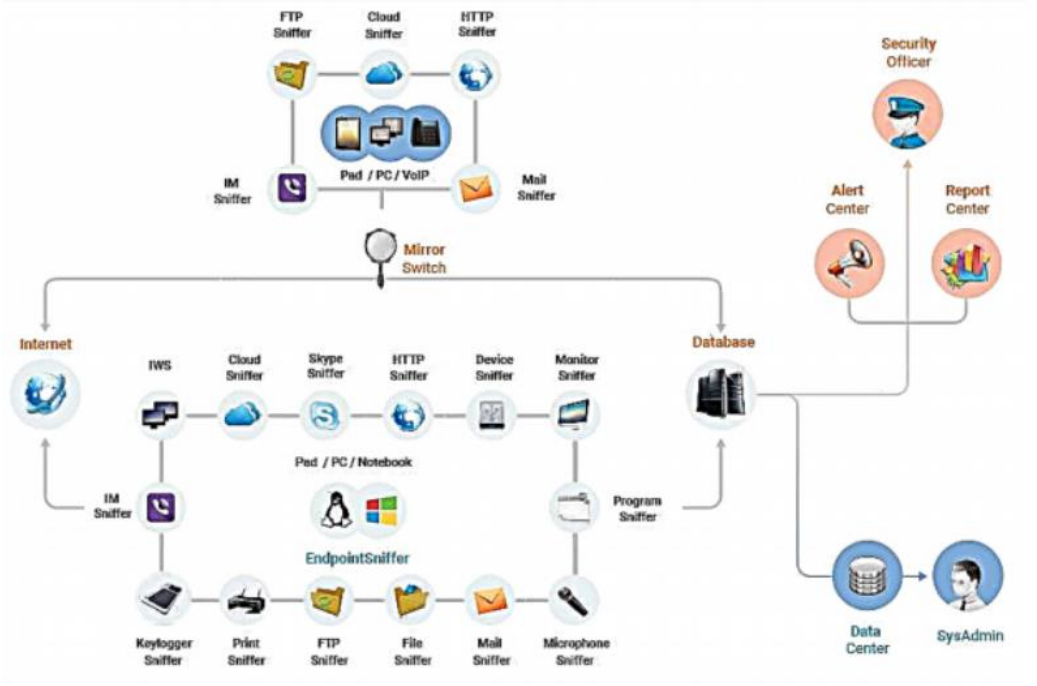

Рисунок 5.1. Архітектура DLP-системи «Контур інформаційної безпеки SearchInform»

Також в системі реалізована захист локальних ресурсів. Функціонал дозволяє регулювати доступ до критичних даних: приховує / закриває папки топ-менеджменту, забороняє доступ до інформації навіть привілейованим користувачам (системним адміністраторам, технічним фахівцям і т.д.). Розмежування доступу до ресурсів (папок і дисків) проводиться тільки на рівні DLP і не може бути скасовано ні на рівні системи, ні на рівні домену.

Агенти SearchInform EndpointSniffer виробляють тіньове копіювання перехопленої інформації і направляють отримані дані на сервера SearchInform EndpointSniffer. Сервер поміщає перехоплені дані в базу під управлінням СУБД Microsoft SQL Server (рис.5.2).

SearchInform NetworkSniffer - платформа перехоплення і блокування інформаційних потоків на рівні мережі. SearchInform NetworkSniffer дозволяє

працювати з зеркаліруемим трафіком, проксі-серверами (ICAP або ISA TMG), поштовими серверами (інтеграція через поштову скриньку (POP3, IMAP, EWS), через SMTP, шляхом транспортних правил або журналирования), іншим корпоративним ПО, наприклад, Lync (рис.5.3).

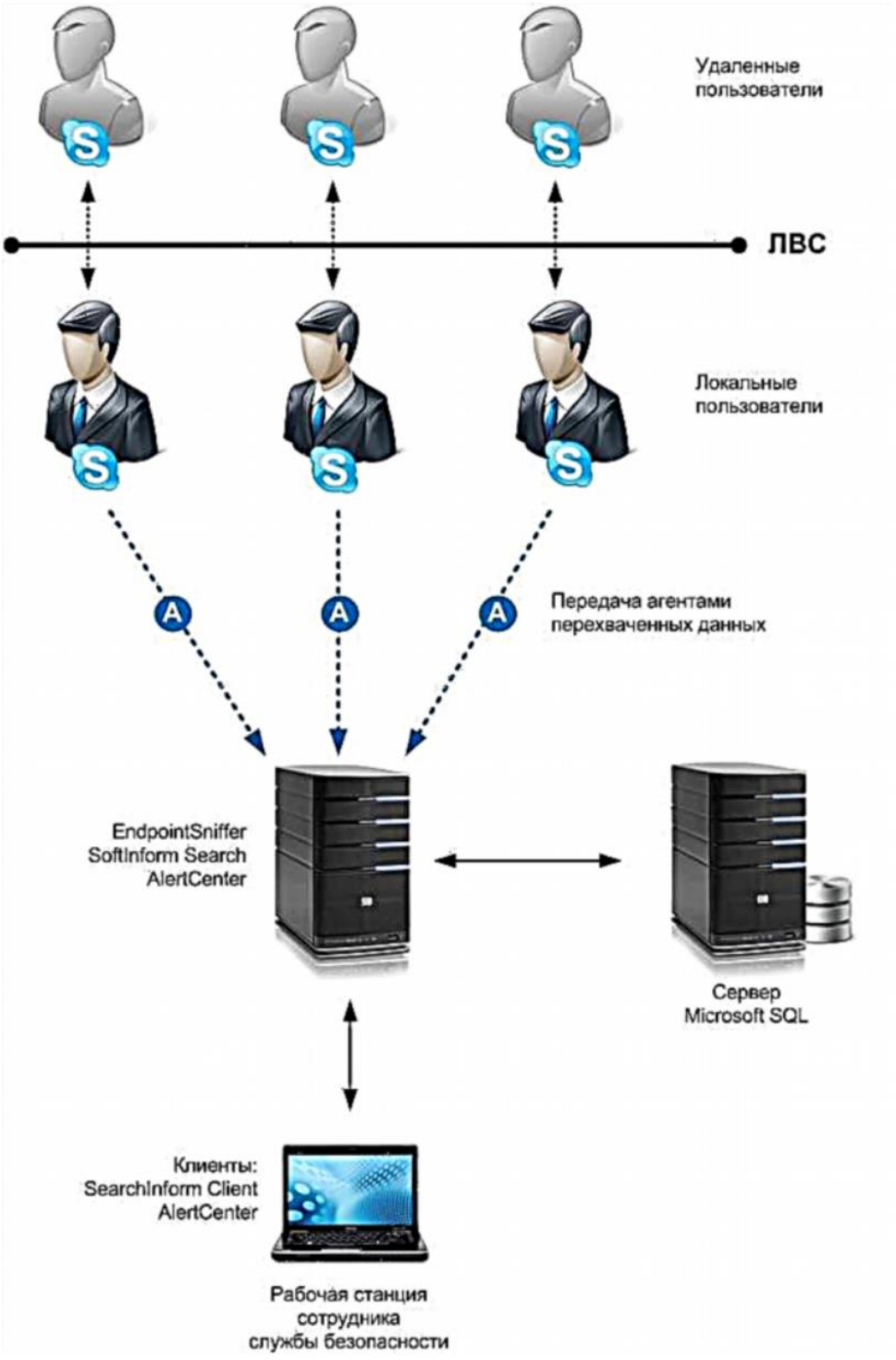

Рисунок 5.2. Типова схема роботи SearchInform EndpointSniffer

Перехоплення мережевого трафіку проводиться на рівні мережевих протоколів (Mail, HTTP, IM, FTP, Cloud). Можлива фільтрація по доменному

імені користувача, імені комп'ютера, IP- і MAC-адресами. Перехоплені повідомлення переносяться в базу даних SQL.

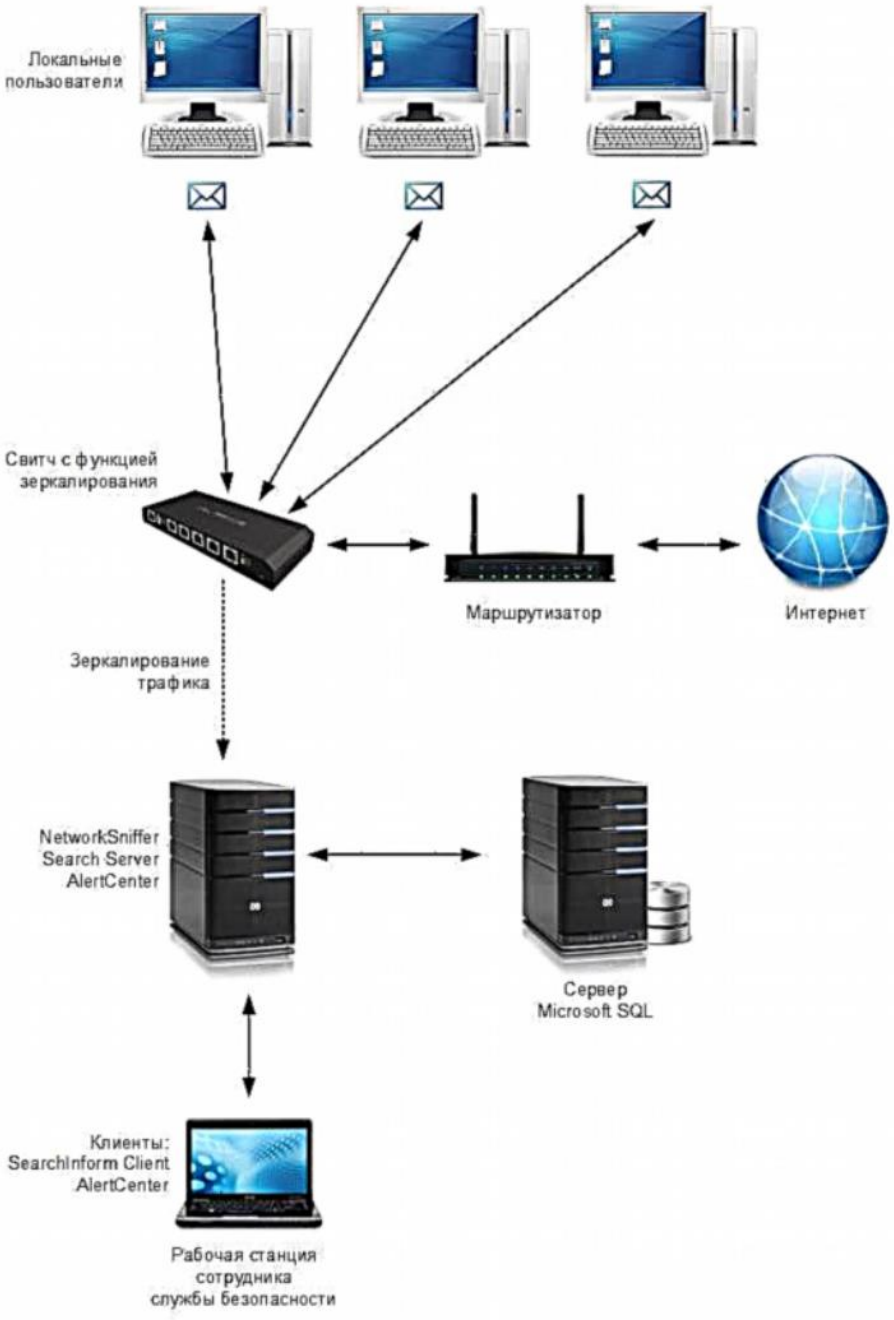

Рисунок 5.3. Типова схема роботи SearchInform NetworkSniffer

Для комплексного контролю переданих даних доцільно використовувати одночасно і SearchInform NetworkSniffer, і SearchInform EndpointSniffer. Наприклад, якщо агент зумів перехопити повідомлення, що не перехоплені на «дзеркалі», то має місце шифрування трафіку, яке може використовуватися для передачі конфіденційних даних за межі організації. Використання двох платформ збору також дозволяє збалансувати навантаження на систему і агента.

Модулі аналізу інформації. Search Server - сервер індексації та пошуку. Продукт власної розробки, не використовує чужі технології індексації, наприклад, elasticsearch або sphinx. Являє собою високопродуктивне рішення для індексації будь-яких типів даних, бесшовно інтегроване в структуру «Контура інформаційної безпеки SearchInform». Також дозволяє індексувати документи «в спокої» - на робочих станціях користувачів або мережевих пристроях. Може індексувати будь-яку текстову інформацію з будь-яких джерел, які мають API або можливість підключення через ODBC.

SearchInform AlertCenter є «мозковим центром» системи «Контур інформаційної безпеки SearchInform». У AlertCenter задаються політики безпеки, модуль стежить за їх виконанням, а при їх порушенні оповіщає ІБ-фахівця про інцидент.

SearchInform ReportCenter модуль збирає статистику і генерує звіти по інцидентах з порушенням політик інформаційної безпеки, стежить за зв'язками співробітників із зовнішнім світом і всередині колективу.

Модуль адміністрування:

SearchInform DataCenter призначений для автоматизованого і ручного управління різними аспектами роботи системи. Інструмент управляє базами даних і індексами, створеними компонентами «Контура інформаційної безпеки», а також здійснює автоматичний моніторинг їх стану.

Модулі перехоплення. SearchInform KeyLogger дозволяє перехоплювати дані, що вводяться користувачем з клавіатури.

SearchInform FileSniffer - призначений для контролю операцій з файлами, що зберігаються на серверах і в загальних мережевих папках.

SearchInform Cloud & SharePoint призначений для контролю трафіку з хмарних сховищ.

SearchInform FTPSniffer призначений для контролю вхідного і вихідного FTP-трафіку на рівні робочих станцій.

SearchInform ProgramSniffer призначений для ведення обліку активності користувачів в запускаємих ними додатках і на відвідуваних веб-ресурсах протягом робочого дня.

SearchInform PrintSniffer призначений для контролю вмісту документів, відправлених користувачем на друк за допомогою як мережевих, так і локальних принтерів.

SearchInform HTTPSniffer призначений для перехоплення повідомлень, переданих по HTTP-протоколу, індексування перехоплених повідомлень і повнотекстовий пошук по ним. Модуль також дозволяє контролювати роботу

співробітників і відстежувати їх спілкування в робочий час.

SearchInform MonitorSniffer призначений для перехоплення інформації, яка відображається на моніторах користувачів. Рішення поставляється разом з програмним модулем KeyLogger.

SearchInform MicrophoneSniffer призначений для запису розмов, що ведуться співробітниками всередині офісу і у відрядженнях.

SearchInform MailSniffer призначений для перехоплення поштового трафіку на рівні робочих станцій і мережних протоколів, індексування отриманих повідомлень і здійснення пошуку по ним.

SearchInform IMSniffer призначений для перехоплення повідомлень популярних IM-клієнтів.

SearchInform SkypeSniffer – додаток, що перехоплює сеанси голосової і текстового зв'язку, SMS-повідомлення та файли, що передаються за допомогою Skype.

SearchInform DeviceSniffer - програмний модуль, що перехоплює інформацію, передану користувачем на зовнішні пристрої, а також відслідковує сам факт підключення такого роду пристроїв.

SearchInform ADSniffer - контроль і аналіз подій журналів Active Directory дозволяє виявляти підозрілі дії, які можуть відбуватися системним адміністратором компанії.

Телефонія-модуль забезпечує перехоплення аудіодзвінків і текстових повідомлень телефонії SIP через стандарти GSM, A-Law, u-Law і G.722.

Модуль шифрування даних забезпечує шифрування всіх типів даних, що записуються на зовнішні пристрої зберігання USB.

Таблиця 5.1

Мінімальні системні вимоги для сервера «Контура інформаційної безпеки SearchInform»

Характеристики	Мінімальна конфігурація сервера «Контур інформаційної безпеки SearchInform»			
	для контролю 50 робочих станцій	для контролю від 50 до 100 робочих станцій	для контролю від 100 до 300 робочих станцій	для контролю від 300 до 1000 робочих станцій
Процесор CPU	2,4 GHz 4 Core	2,4 GHz 6 Core	від 2 x 2,4 GHz 4 Core (2	від 2 x 2,4 GHz 4 Core (2

			чотирьох-ядерних CPU)	чотирьох-ядерних CPU)
Об'єм оперативної пам'яті RAM	8 Gb	8 Gb	16 Gb	24 Gb
Обсяг пристрої зберігання даних HDD	500 Gb (бажано RAID 10)	Tb (RAID 10)	2 Tb (RAID 10)	4 Tb (RAID 10)
LAN	1 Gbps	1 Gbps	1 Gbps	1 Gbps
Операційна система	MS Windows Server 2008 R2	MS Windows Server 2008 R2	MS Windows Server 2008 R2	MS Windows Server 2008 R2
СУБД	MS SQL Server 2008 R2 Express	MS SQL Server 2008 R2 Express	MS SQL Server 2008 R2 Express	MS SQL Server 2008 R2 Express

Системні вимоги. Системні вимоги «Контура інформаційної безпеки SearchInform» безпосередньо залежать від розміру інфраструктури компанії. Нижче наведені (табл.5.1) мінімальні системні вимоги для сервера DLP-системи в залежності від кількості контрольованих робочих станцій в інфраструктурі.

Агенти «Контура інформаційної безпеки SearchInform», які встановлюються на кінцеві точки мережі, підтримують операційні системи сімейства Windows, а також вітчизняну операційну систему Astra Linux. Особливих вимог до апаратної частини робочих станцій агенти «Контура інформаційної безпеки SearchInform» не пред'являють.

«КІБ SearchInform» має гнучку політику ліцензування. Модульна архітектура продукту дозволяє клієнтам впроваджувати тільки ті модулі, в яких є потреба. Ліцензії отримуються за кількістю користувачів і кількістю каналів контролю.

Також варто відзначити, що «Контур інформаційної безпеки SearchInform» має можливість інтеграції з наступними системами:

- інтеграція з доменною структурою Active Directory;
- інтеграція з SearchInform Event Manager (SIEM);
- інтеграція с поштовими серверами Microsoft Exchange, Lotus Domino і ін.;
- інтеграція с Microsoft ISA / Forefront TMG та іншими проксі-серверами,

що працюють по протоколу ICAP.

Основні функціональні можливості продукту. Однією з ключових можливостей «Контура інформаційної безпеки SearchInform» як системи класу DLP є контроль інформаційних потоків і перехоплення даних. «Контур інформаційної безпеки SearchInform» підтримує перехоплення наступних даних:

- повідомлення електронної пошти, надісланих або отриманих за протоколами SMTP, POP3, IMAP, MAPI, NNTP, HTTP (S);
- миттєві повідомлення, передані по протоколах OSCAR (служби ICQ, AIM), MMP (Mail.ru Agent), MSNP (Windows Live / MSN), XMPP (Google Hangouts, Jabber), а також текстові / голосові повідомлення і файли, що передаються за допомогою Microsoft Lync і Viber Desktop;
- повідомлення і файли, які приходять від браузера в чати, форуми, блоги, соціальні мережі (Facebook, LinkedIn, В Контакте, Мой Мир@Mail.Ru, Одноклассники.ru, Google+, Mamba.ru і ін.);
- вхідні та вихідні дані хмарних сервісів при роботі через веб-інтерфейс (Google Docs, OneDrive (Microsoft), Office 365 (Office Online), DropBox, Evernote, Яндекс.Діск Cloud.mail.ru, SharePoint);
- зупинка трафіку на рівні мережі на рівні ICAP - HTTP, FTP;
- дані, що передаються на зовнішні пристрої;
- історія операцій з файлами, розташованими на ноутбуках;
- файли, відправлені або отримані з FTP-з'єднання;
- вміст моніторів ноутбуків користувачів, а також натискання клавіш;
- розмови співробітника, який перебуває поза офісом;
- документи, відправлені на друк;
- текстові та голосові сеанси зв'язку по Skype, файли і SMS-повідомлення, передані або отримані за допомогою Skype;
- активність користувачів і запускаються ними додатків;
- контроль пристроїв на робочих станціях.

Крім того, в «КІБ SearchInform» існує можливість детального розслідування порушень за допомогою зняття скріншотів екранів, записи відео роботи користувача на робочому місці і аудіозаписи розмов, перехоплення даних, що вводяться користувачем з клавіатури, розпізнавання аудіозаписи в текст, а також текстовий пошук по аудіо та відео.

У «Контур інформаційної безпеки SearchInform» можливий також контроль привілейованих користувачів шляхом аналізу подій журналів Active Directory для виявлення підозрілих дій, які можуть відбуватися

системним адміністратором компанії.

В системі також передбачена можливість детектування агентів інших DLP, тайм-трекерів, клавіатурних шпигунів. Така можливість особливо корисна, коли необхідно очистити інфраструктуру від залишків інших систем контролю, які можуть створювати труднощі при інтеграції і експлуатації «Контура інформаційної безпеки SearchInform». Агент «КІБ SearchInform» після установки видає інформацію про недеінсталлірованних продуктах, що дозволяє в підсумку очистити систему і спокійно працювати.

Аналітичні можливості. Контроль інформаційних потоків і перехоплення даних - тільки частина функціоналу DLP-системи «Контур інформаційної безпеки SearchInform». Щоб проаналізувати весь масив інформації і виявити інцидент, необхідні потужні пошукові та аналітичні інструменти.

Спільне використання всіх типів пошуку дозволяє максимально ефективно захищати конфіденційні дані в корпоративній мережі і, що особливо важливо в сучасних умовах, різко скоротити трудовитрати на їх аналіз. Пошукові механізми, вбудовані в DLP-систему «Контур інформаційної безпеки SearchInform», дозволяють ефективно працювати з усіма видами конфіденційної інформації, що міститься в перехоплених даних.

У рішенні закладено різноманітні технології пошуку:

- пошук за словами з урахуванням морфології і синонімів. Найпростіший вид пошуку, що дозволяє знаходити документи, що містять задані слова, їх різні форми і синоніми, незалежно від того, в якому місці документа вони знаходяться;
- пошук по фразах з урахуванням порядку слів і відстані між ними. За допомогою даного виду пошуку можна аналізувати документ не за окремими словами, а по словосполученням (наприклад, прізвища і імені) або усталеним визначенням;
- пошук по атрибутам. Використання цього виду пошуку дозволяє шукати документи по їх ознаками (формату, імені відправника або одержувача і ін.). Також можна відстежувати активність окремих доменних користувачів, IP-адреси, визначені адреси електронної пошти, документи і т. д.;
- пошук за регулярними виразами. Такий пошук дозволяє відстежити послідовності символів, які характерні для різних форм персональних даних, що містяться в фінансових документах, структурованих записах баз даних і

т.д. З його допомогою система оперативно реагує на спробу відправки записи з такими персональними даними, як прізвище людини, день його народження, номери кредитних карт, телефонів і т. д. (рис.5.4);

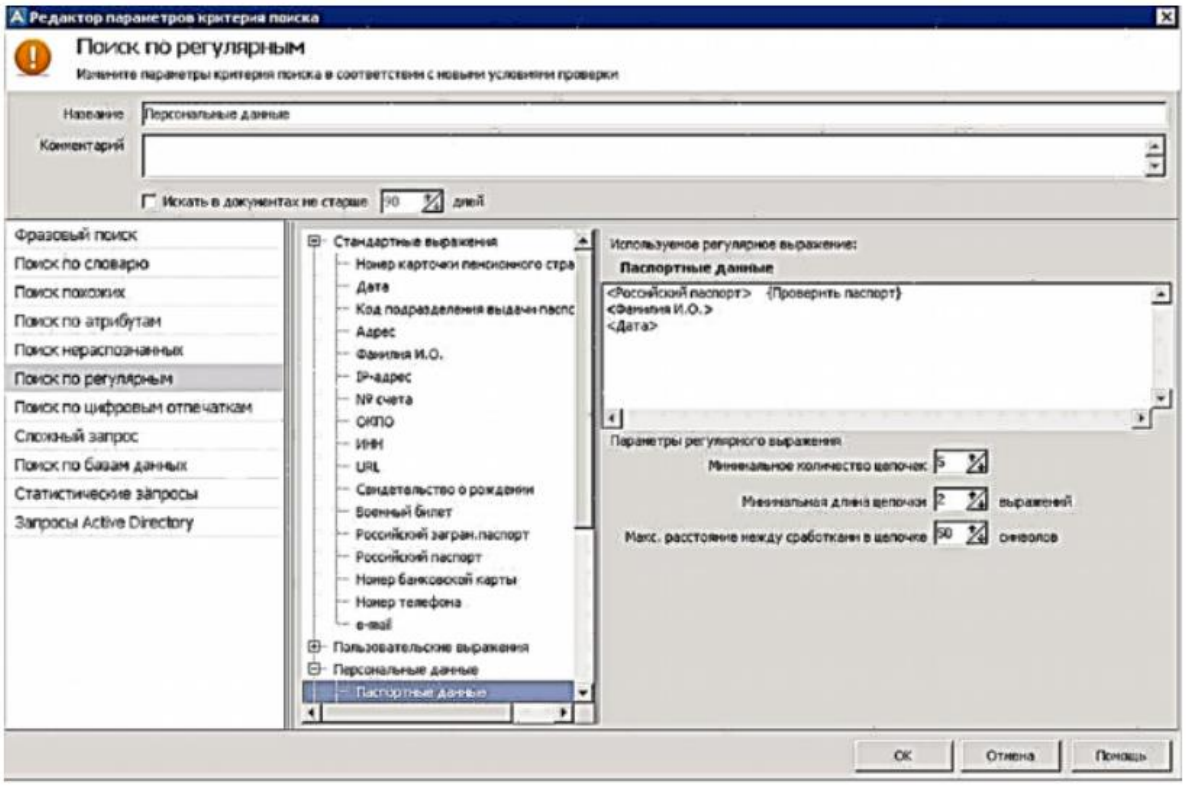

Рисунок 5.4. Приклад відбору за регулярними виразами в модулі AlertCenter

- пошук по цифровим відбитками. Цей вид пошуку передбачає виявлення групи конфіденційних документів і зняття з них цифрових відбитків, за якими в подальшому і буде здійснюватися пошук. За допомогою даного методу можна швидко відстежити в інформаційних потоках файли, що містять великі фрагменти тексту з документів, що відносяться до конфіденційних;
- «Пошук схожих» (Запатентований алгоритм компанії «SearchInform»). Інтелектуальні можливості даного типу пошуку дозволяють відслідковувати відсилання конфіденційних документів навіть у тому випадку, якщо вони були попередньо відредаговані. В якості пошукового запиту використовуються як фрагменти документів, так і документи цілком. В результаті пошуку виявляються документи, що містять не тільки весь пошуковий запит, але і файли, схожі на нього за змістом. Даний алгоритм дозволяє істотно скоротити часові витрати на аналіз інформації, значно спрощуючи роботу фахівця з безпеки (рис.5.5).

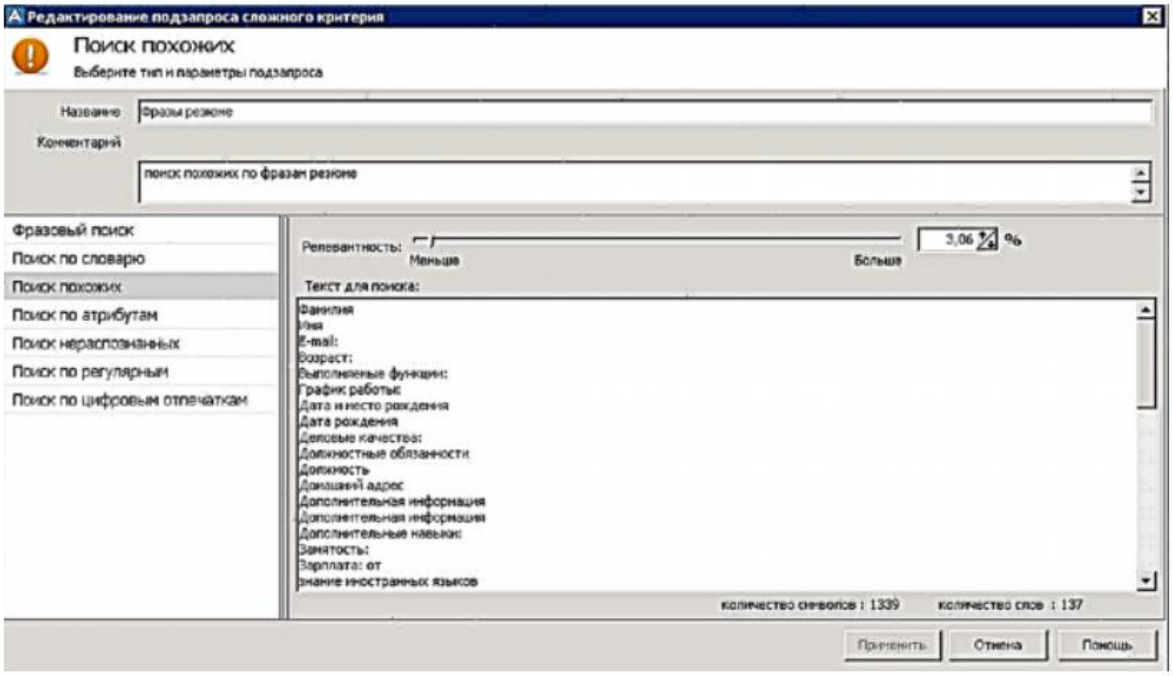

Рисунок 5.5. Приклад «пошуку схожих» засобами модуля AlertCenter

- комплексні пошукові запити. Складні запити можуть включати в себе два і більше простих запитів, об'єднаних за допомогою логічних операторів AND, OR, NOT. С їх допомогою можна вирішувати нестандартні пошукові завдання, вибираючи саме ті дані, які потрібні в даний момент фахівця з інформаційної безпеки (рис.5.7).

Пошукові можливості «Контура інформаційної безпеки SearchInform» дозволяють проводити аналітику будь-якої складності і адаптувати DLP-систему під конкретні завдання і корпоративні стандарти. В консолі модуля AlertCenter, що відповідає за автоматичне виявлення порушень політик безпеки (рис.5.6), задаються критерії політики ІБ і розклад їх автоматичної перевірки. При виявленні інциденту система оповіщає співробітника служби ІБ про порушення політики або блокує потенційно небезпечне діяння до його завершення (рис.5.8).

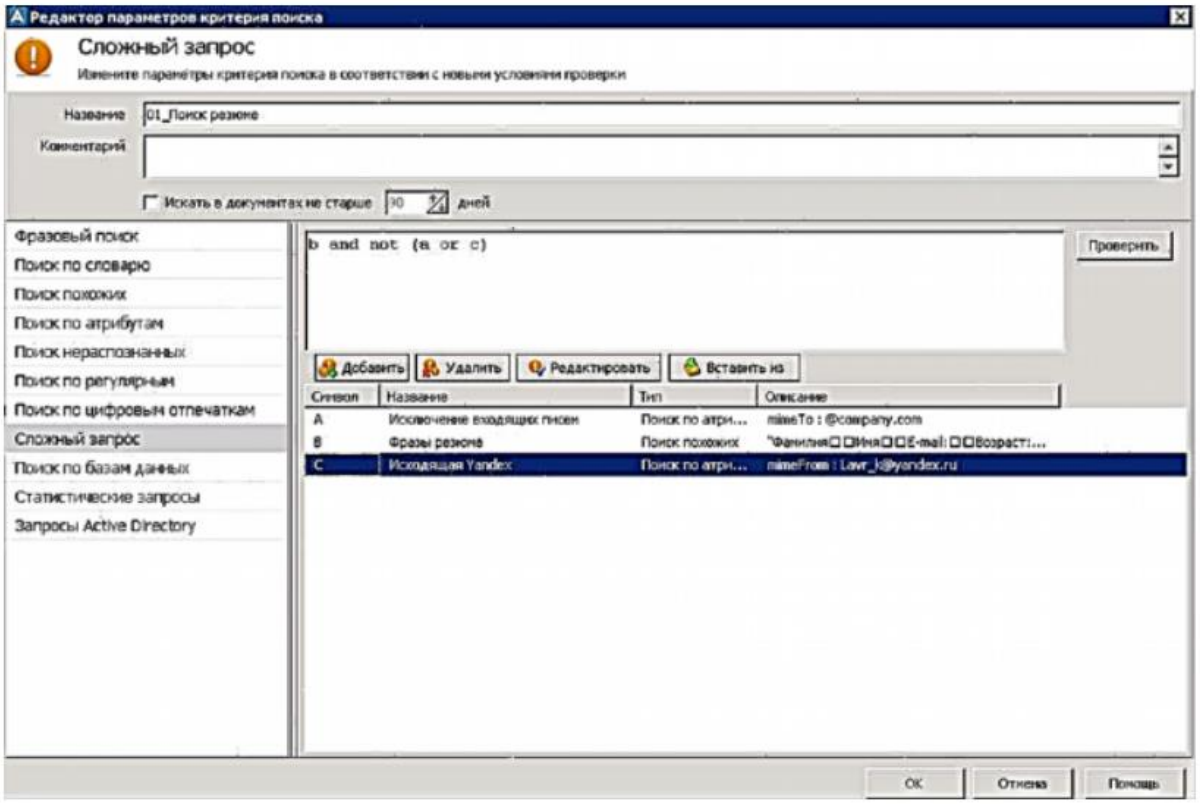

Рисунок 5.6. Приклад складного запиту засобами модуля AlertCenter

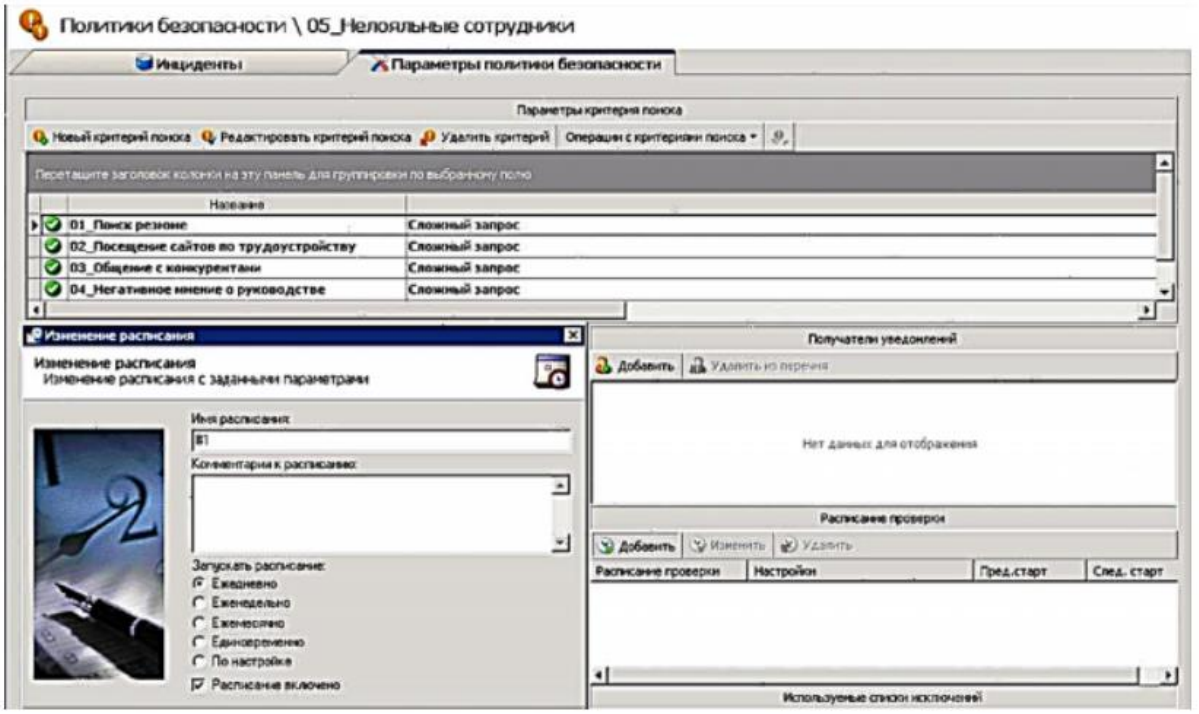

Рисунок 5.7. Встановлення в модулі AlertCenter критеріїв і розкладу перевірок на прикладі політики безпеки «Пошук резюме»

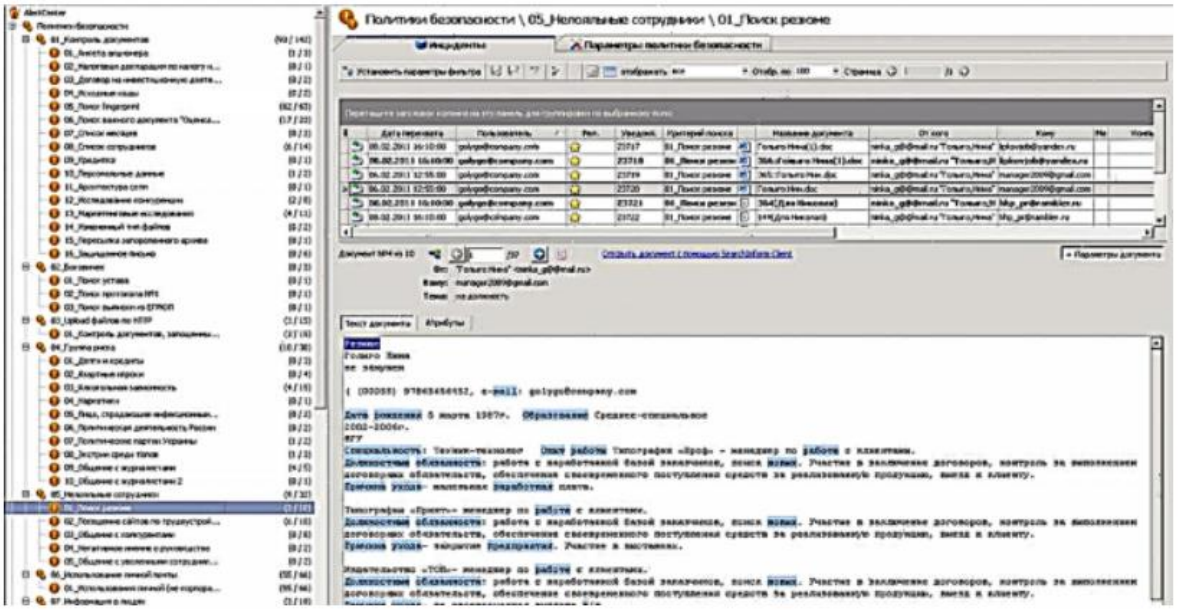

Рисунок 5.8. Список інцидентів, зафіксованих у відповідності з критеріями політики безпеки «Пошук резюме»

Система звітів. Модуль SearchInform ReportCenter збирає статистику по активності користувачів і інцидентів, пов'язаних з порушеннями політик інформаційної безпеки, і представляє її у вигляді звітів (графіків, діаграм, таблиць і графів):

- звіти по зв'язках користувачів наочно відображають всю зібрану інформацію про зовнішніх і внутрішніх контактах користувачів і каналах їх зв'язку (рис.5.9, 5.10).

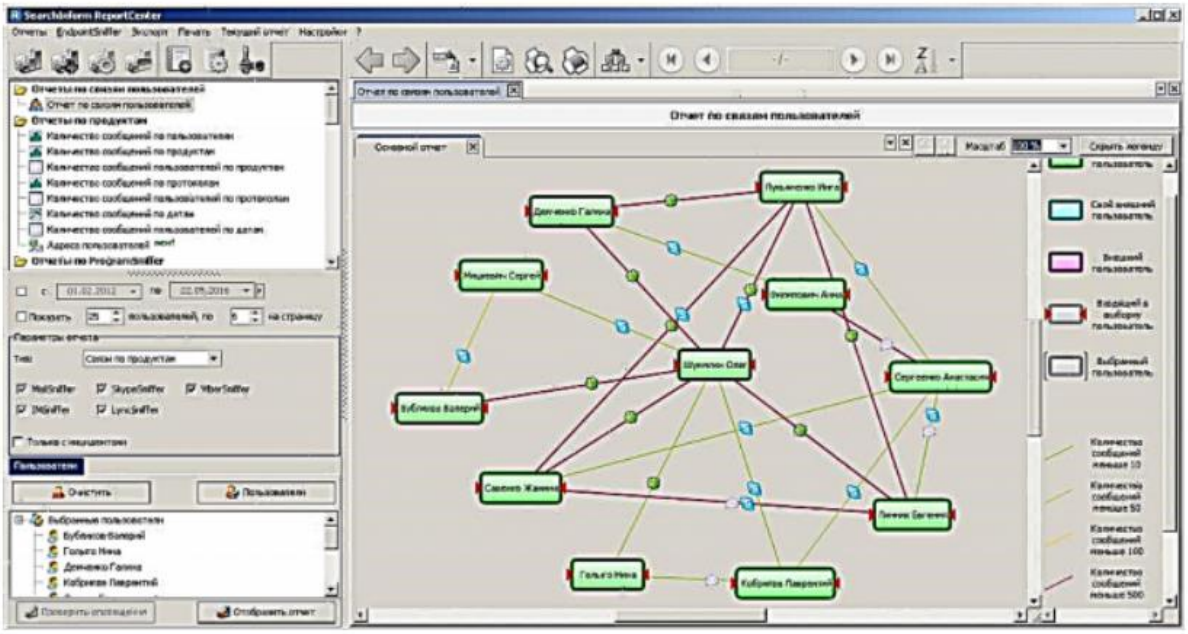

Рисунок 5.9. Звіт по зв'язках користувачів, що формується в модулі ReportCenter

- звіти по продуктам системи дозволяють вивести в структурованому вигляді статистичні дані перехоплення за якийсь проміжок часу, наприклад, кількість повідомлень по користувачам і продуктам, кількість повідомлень за протоколами, дат і т.д.

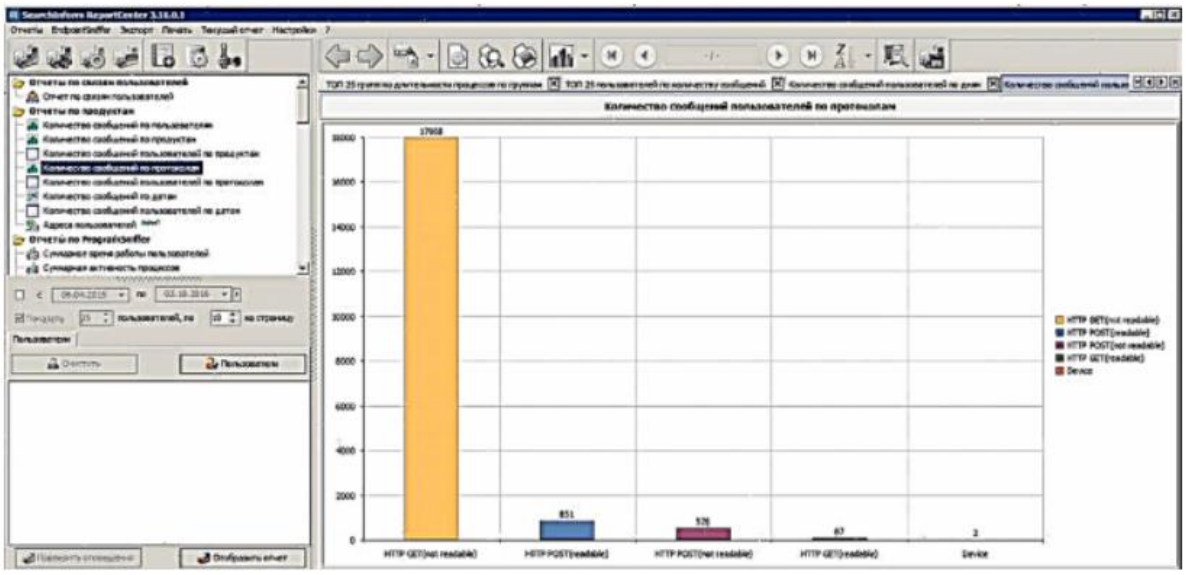

Рисунок 5.10. Звіт про кількість повідомлень за протоколами, що формується в модулі ReportCenter

Група звітів ProgramSniffer дозволяє фіксувати запізнення, ранні відходи і відсутність на робочому місці співробітника, оцінювати ефективність співробітників, проміжки неактивності, а також активність процесів і / або сайтів на комп'ютерах користувачів системи і багато іншого (рис.5.11).

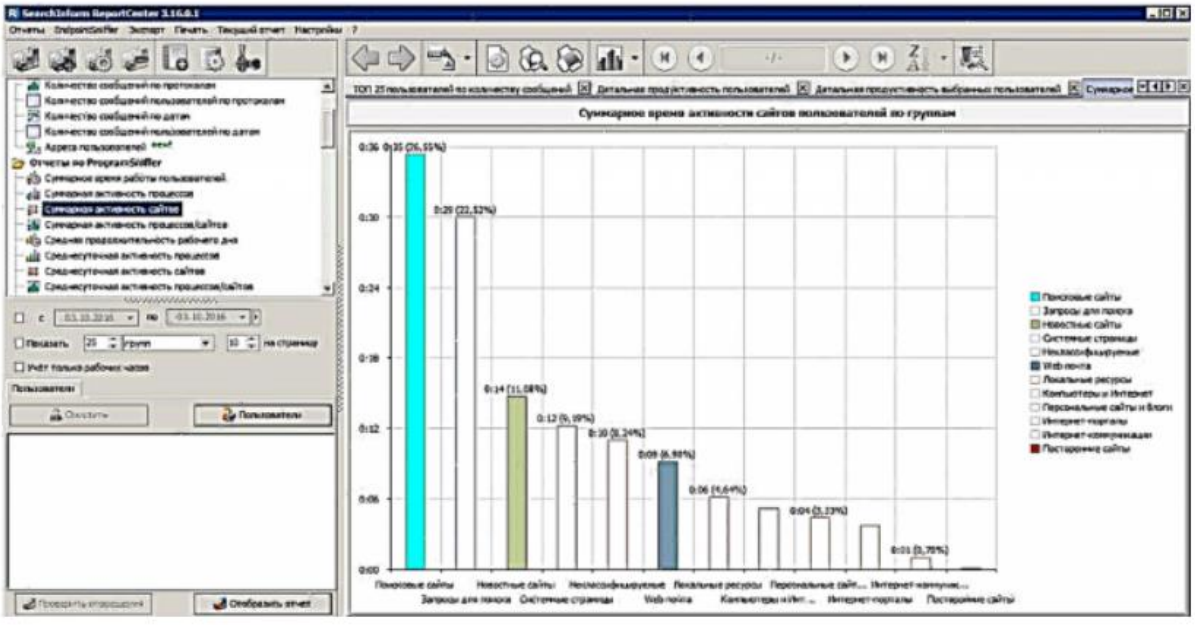

Рисунок 5.11. Звіт про сумарному часу активності сайтів користувачів по групах, що формується в модулі ReportCenter

Група звітів AlertCenter дозволяє формувати статистичні звіти по зафіксованим інцидентів.

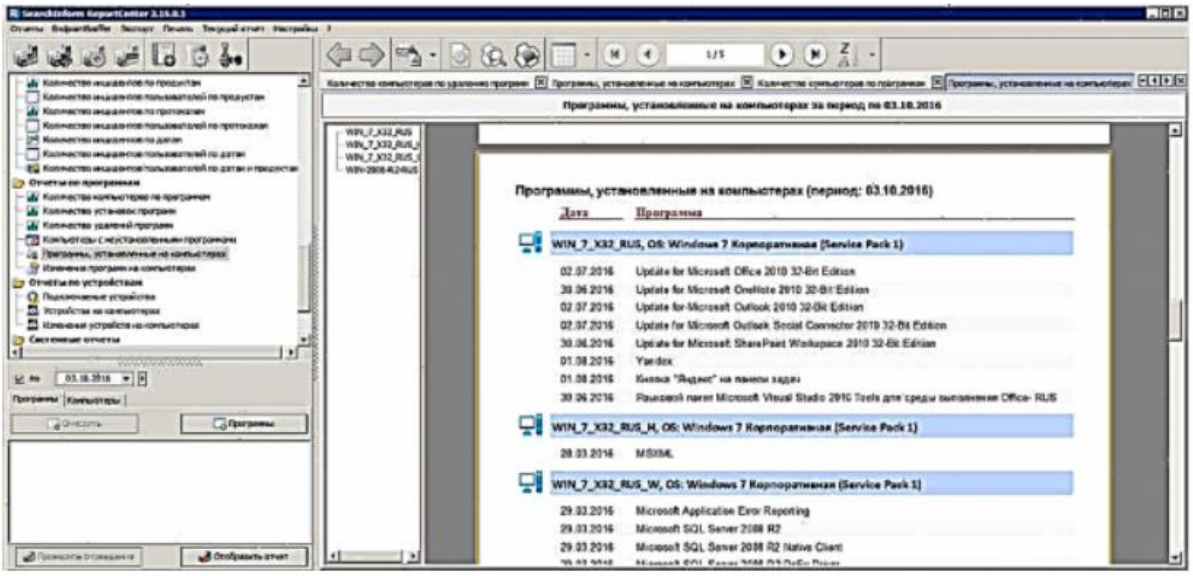

Рисунок 5.12. Звіт про встановлені програми на комп'ютері, що формується в модулі ReportCenter

Група звітів за програмами дозволяє формувати статистичні звіти про виконані дії з програмним забезпеченням і наявності його на комп'ютерах (рис.5.12).

Група звітів по підключається пристроїв дозволяє формувати статистичні звіти про підключені пристрої, встановленому обладнанні і про їх зміну.

Група системних звітів дозволяє аналізувати операції з агентами, протоколами, наприклад, виводять список комп'ютерів без агентів, список комп'ютерів, які виконали вхід в домен, але не мають встановленого агента та ін. «Контур інформаційної безпеки SearchInform» також надає можливість створювати власні шаблони звітів.

Розпізнавання хитрощів інсайдерів. Найчастіше недобросовісні співробітники, намагаючись обдурити службу безпеки, змінюють розширення переданого документа (рис.5.13) або запаковують дані в запаролений архів.

Для розпізнавання хитрувань «КІБ SearchInform» дозволяє:

- розпізнавати текст в графічних файлах і здійснювати пошук по ним;
- виявити передачу захищених паролем архівів по всіх каналах можливого витоку інформації;
- виявляти пересилання файлів з навмисне зміненим типом документа.

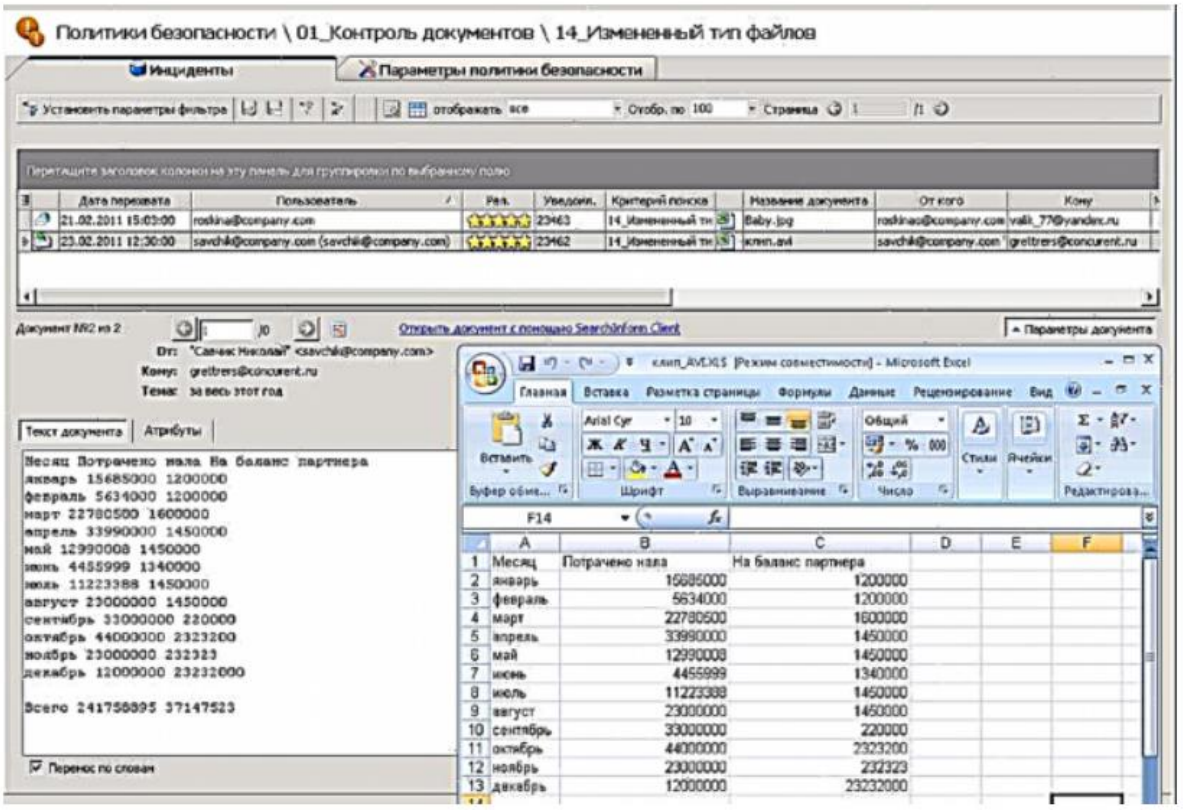

Рисунок 5.13. Приклад виявлення пересилання файлу з навмисне зміненим типом документа

Контроль ефективності роботи співробітників. Дослідження показують, що типовий офісний працівник використовує від 30 до 70% робочого часу в особистих цілях. Ігри, чати і соціальні мережі забирають левову частку сплаченого роботодавцем часу, знижують ефективність роботи персоналу і конкурентоспроможність компанії. Контроль за дотриманням співробітниками трудового розпорядку, їх активності протягом робочого дня, а також аналіз їх роботи в запускаємих додатках дозволяють не тільки вирішити питання безпеки і дисципліни, а й стимулюють співробітників ефективно використовувати робочий час з метою організації.

У ReportCenter передбачена можливість формування різноманітних звітів, що дозволяють скласти уявлення про раціональність використання робочого часу тих чи інших користувачем, а також про дотримання ним політик безпеки організації, наприклад (рис.5.14):

- ТОП за кількістю перехоплених файлів і повідомлень;
- ТОП користувачів по числу інцидентів;
- візуалізація зв'язків співробітників з їх адресатами;
- середня тривалість робочого дня і сумарний час роботи співробітників;
- середньодобова і сумарна активність запускаємих користувачами процесів;

- середньодобова і сумарна активність на відвідуваних користувачами веб-сайтах;
- детальна інформація по роботі користувачів;
- журнал робочого часу користувачів;

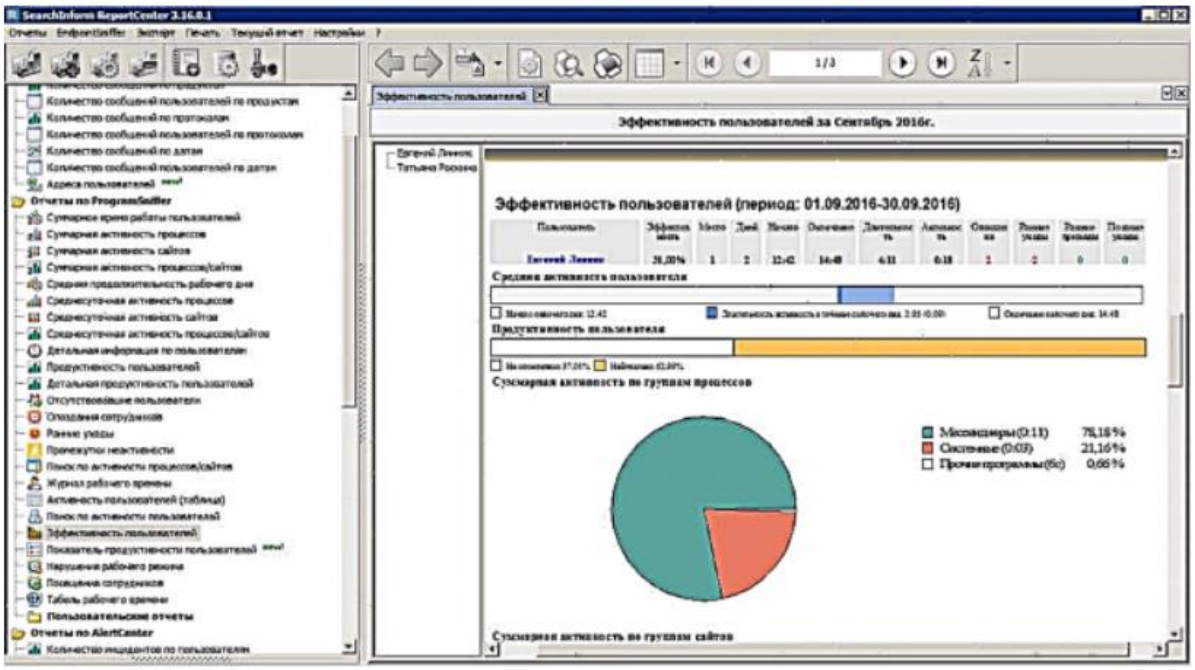

Рисунок 5.14. Звіт про ефективність користувачів, що формується в модулі ReportCenter

- звіт щодо порушень робочого режиму;
- звіт за встановленим і зміненим на комп'ютерах користувачів обладнання та ін.

Крім того, в «Контур інформаційної безпеки SearchInform» існує можливість моніторингу активності користувачів в режимі реального часу.

Політики безпеки. «Контур інформаційної безпеки SearchInform» включає більше 150 готових політик безпеки:

- універсальні політики безпеки (актуальні для будь-якої організації):
- контроль відкатів і хабарництва;
- виявлення негативних настроїв і змов в колективі;
- визначення груп ризику (проблеми з алкоголем, наркотиками, великі борги і т. д.);
- контроль персональних даних (паспорта, номери банківських карт і ін.);
- виявлення спілкування з конкурентами, зі звільненими співробітниками;
- відвідування заборонених сайтів;

- антитерористичні політики та ін.

Галузеві політики безпеки (враховують сферу діяльності компанії):

- банки та фінанси;
- видобувна та хімічна промисловість;
- транспорт і логістика;
- газо-, електро- і водопостачання;
- будівництво, зв'язок.

Індивідуальні політики безпеки - політики, які фахівці компанії безкоштовно розробляють під запити клієнта.

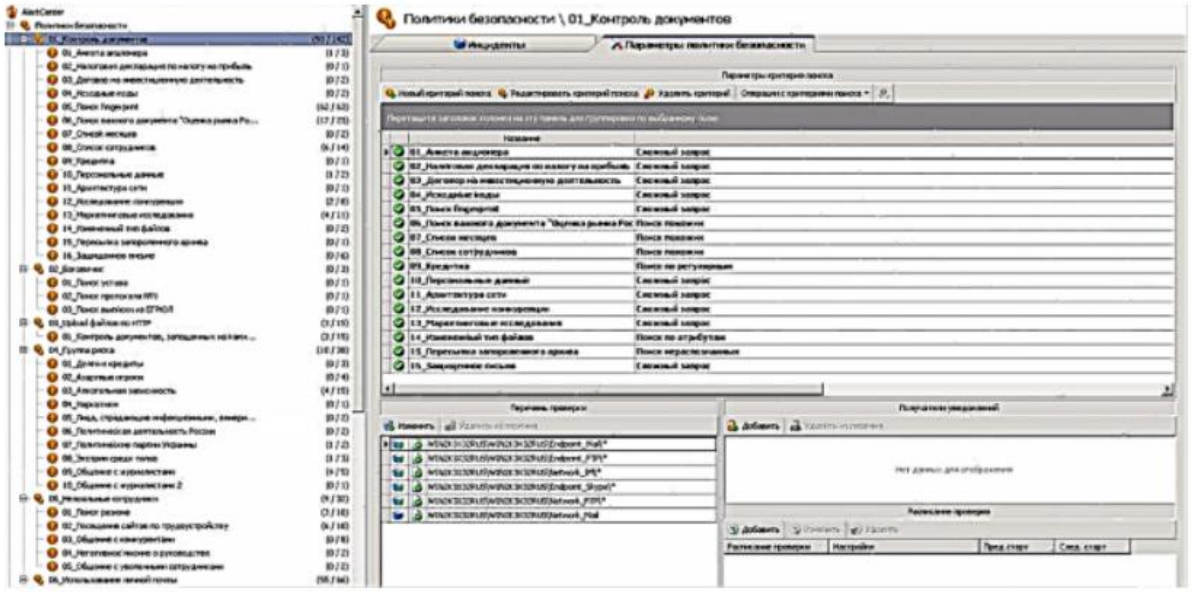

Рисунок 5.15. Перелік політик безпеки «Контура інформаційної безпеки SearchInform»

Відповідність вимогам регуляторів. Сертифікація за вимогами безпеки дає можливість використовувати «Контур інформаційної безпеки SearchInform» в складі системи захисту інформаційних систем, де застосування сертифікованих продуктів обов'язково, наприклад, в інформаційних системах персональних даних, державних інформаційних системах (ГІС), автоматизованих системах управління технологічним процесом (АСУ ТП) та ін.

Контрольні запитання

1. Опишіть архітектура рішення системи.
2. Опишіть можливості модулю контролю інформації.
3. Як здійснюється захист локальних ресурсів в системі?
4. Опишіть можливості модулю аналізу інформації.
5. Опишіть аналітичні можливості системи.

6. РЕАЛІЗАЦІЯ ОПЕРАТИВНОГО КОНТРОЛЮ ЗА ДІЯМИ КОРИСТУВАЧІВ

Активний розвиток новітніх форм господарювання обумовив розширення та урізноманітнення кола інтересів, запитів і потреб суб'єктів ринку. Якісне та результативне управління господарською діяльністю, а особливо її трудомісткими секторами і напрямами, вимагає сьогодні формування належного інформаційно-аналітичного забезпечення. Водночас реалії сучасного бізнес-середовища поглиблюють критичне ставлення до інформації, що створюється в системі «традиційного» бухгалтерського обліку. Сьогодні необхідно володіти своєчасними і доречними даними про стан господарських операцій та подій на всіх стадіях їх здійснення. Задоволення сукупності нових та оновлених потреб користувачів різних рангів можливе при ефективному і раціональному функціонуванні системи оперативного контролю. Результативне та якісне його проведення полягає у спостереженні за ходом здійснення визначених процесів, перевірки їх відповідності нормам і нормативам й виявленні відхилень, що перешкоджають отриманню запланованих результатів. Дотримання системності та цілеспрямованості при проведенні оперативного контролю забезпечує досягнення поставлених цілей з врахуванням можливого впливу на них зовнішніх і внутрішніх факторів. Тобто роль оперативного контролю в сучасних умовах визнані як в науковому світі, так і в практичній діяльності. Проте, динамічний розвиток ринку потребує всебічного та повсякчасного удосконалення його методик, прийомів; уточнення термінології та категорійного апарату.

Питання економічної сутності, ознак і особливостей оперативного контролю досліджувались та висвітлені у багатьох працях вітчизняних і зарубіжних вчених, зокрема таких, як Ф.Ф. Бутинець, Б.І. Валуєв, Н.Г. Виговська, В.М. Жук, М.Я. Дем'яненко, В.А. Дерій, І.К. Дрозд, Є.В. Калюга, Г.Г. Кірейцев, В.Г. Лінник, Ю.Я. Литвин, Л.В. Нападовська, О.А. Петрик, Л.В. Сотнікова, Р.Б. Чейз, В.О. Шевчук та інші. Науковці звертали увагу на визначення місця і функціонального призначення оперативного контролю в системі управління, досліджували його інформаційне забезпечення, категорії та критерії визнання об'єктів. Особливого значення надавали показникам відповідно потреб окремого кола користувачів.

Метою цієї лекції є систематизація знання про оперативний контроль, уточнення деяких категорій та понять: предмета, методу і суб'єктів, а також

формулювання концепції його розвитку.

Раціональна організація та методика проведення оперативного контролю Раціональна організація та методика проведення оперативного контролю здійснюється з врахуванням особливостей виробничо-господарської діяльності, напрямів і видів господарювання, форм та рівня інформаційного забезпечення. Сукупність таких аспектів першочергово створює основу для формування концепції розвитку та функціонування оперативного контролю в сучасних умовах. Разом з тим необхідно з'ясувати суть значення «концепції» в управлінні як всією діяльністю, так і окремими її складовими. З філософського погляду концепцію розглядають як спосіб розуміння чи трактування будь чого на основі власних чи вже існуючих висновків. У діловому світі концепцію розуміють як письмовий виклад будь-якої стратегії. Професор А.Г. Загородній висловлює думку про те, що концепція – це наукова теорія щодо появи, становлення та розвитку окремих явищ чи предметів, що становлять в сукупності систему, але остання має специфічну і власну концепцією. В економічній енциклопедії С.В. Мочерного концепція розглядається як сукупність ідей, положень, способів пізнання, методологічних принципів. Науковець В.П. Пантєлєєв у докторській дисертації зазначає широке трактування концепції контролю: від побудови цілісної системи, концептуальної інтерпретації множинного змісту поняття «контроль» і розкриття багатоаспектності його системної сутності до перспектив розвитку контролю, його методології та організації. Враховуючи таке, доповнимо, що концепція оперативного контролю має враховувати його специфічні особливості і ознаки, але разом з тим сама регламентує такі характеристики. Треба також брати до уваги, що у вузькому розумінні оперативний контроль – це контроль при веденні оперативного обліку, внутрішнього контролю, а також тих дій і подій, що не мають відображення у паперовій чи іншій формі. У ширшому розумінні - це різного роду вплив суб'єкта оперативного контролю (керівної системи) на об'єкт (керовану систему) за допомогою способів і прийомів, що забезпечують виконання планів, бюджетів і програм (система методичних інструментів). Слід з'ясувати концепцію розвитку оперативного контролю як систематизований та узагальнений погляд на розвиток оперативного контролю як науки; та як розроблення проекту внутрішнього нормативно-правового положення – Концепції оперативного контролю суб'єктів господарювання. Основною метою концепції є визначення завдань і сфер (напрямів) здійснення оперативного контролю з врахуванням пріоритетності інтересів користувачів

(власника, бухгалтера, управлінця, спеціаліста, робітника) та дотримання вимог обов'язкового законодавства. Реалізація цілі концепції передбачає виконання таких завдань: формування нормативно правового регулювання; розроблення організаційно-методичного забезпечення; удосконалення кадрової політики і розроблення мотиваційних заходів. Забезпечення ефективного здійснення таких завдань можливе при обґрунтуванні та уточненні науково-теоретичних засад концепції. До них можна віднести сукупність специфічних норм, положень, ознак, понять, що становлять концептуальну основу результативного та якісного здійснення оперативного контролю. За вищевикладеним, концепція розвитку оперативного контролю складається із деяких послідовних елементів, функціонально пов'язаних між собою (рис.6.1).

Суть концептуальної основи визначена деякими законодавчими і міжнародними документами, де зазначено, що концептуальна основа включає мету здійснюваного процесу, якісні характеристики інформації, принципи та характеристику елементів системи. Отже, концептуальна основа дає змогу дослідити та виявити межі функціонування конкретного явища чи процесу, способи реалізації їх базових функцій і властивостей, а також пояснює роль та місце серед інших напрямів діяльності чи в системі управління загалом (з погляду теорії). Крім того, передбачає використання специфічних методів та прийомів у випадку існування конкретних умов господарювання з метою забезпечення досягнення поставленої мети за найменших втрат (з погляду практики).

Рисунок 6.1. Структура концепції розвитку оперативного контролю

Мета оперативного контролю полягає у попередженні і своєчасному виявленні відхилень фактичного стану об'єкта управління від нормативних,

планових та інших його характеристик, відповідно до яких можливе його функціонування. Оперативний контроль попереджує можливі зловживання при одержанні інформації підприємства, сприяє дотриманню інформаційної безпеки. Ціль концепції - визначення завдань і сфер (напрямів) здійснення оперативного контролю з врахуванням пріоритетності інтересів користувачів (власника, управлінця, спеціаліста, робітника) та дотримання вимог існуючого законодавства.

Концепція оперативного контролю включає:

– мету та завдання оперативного контролю;

– характеристику елементів оперативного контролю як системи (суб'єкти, предмет, метод).

Реалізація цілі концепції передбачає виконання таких завдань:

– формування нормативно-правового регулювання;

– розроблення організаційно-методичного забезпечення;

– удосконалення кадрової політики і розробка мотиваційних заходів дисципліни, а також має відповідати інтересам власника.

Мету та завдання оперативного контролю можна достовірно визначити, розкриваючи економічну суть такого процесу. Діяльність або впорядкованість дій окремих зацікавлених осіб спрямована на формування достатнього для прийняття поточних управлінських рішень інформаційного забезпечення, що в сукупності становить певну систему постійного спостереження, огляду і перевірки форми, стану та рівня господарських об'єктів, процедур й показників запланованим чи потрібним. Крім того, оперативнй контроль характеризується здійсненням в незначні інтервали часу, протяжність яких залежить від тривалості окремих підконтрольних процесів. Разом з тим, такі процеси можуть містити інші явища, події та операції, що також потребують перевірки під час їхнього здійснення. Саме така функціональна особливість забезпечує результативне та доречне проведення оперативного контролю відповідно до його мети. Отже, оперативний контроль є «швидким» інструментом управління, який присутній на всіх етапах реалізацій господарських цілей. Також зауважимо, що його прийоми і способи здійснення залежать від конкретних потреб управління, яке і визначає сферу його застосування.

Спираючись на мету оперативного контролю, можна визначити його основні завдання:

1) поточне спостереження за господарськими операціями, а також факторами, що впливають на них в процесі їх здійснення;

2) своєчасне попередження різного роду відхилень, формування яких знизить ймовірність отримання поставлених результатів;
3) оперативне виявлення фактичних відхилень.

Забезпечення ефективного оперативного контролю можливе за умови раціонально організованої роботи осіб, зацікавлених у його результативному здійсненні. Побудова організаційної структури оперативного контролю має враховувати деякі особливості як самих господарюючих одиниць, так і середовища, в якому вони діють. Серед них можна виділити такі:
1) галузь господарювання визначає рівень потреби у поточних інформаційних даних у процесі прийняття управлінських рішень;
2) вид (напрям) діяльності суб'єкта господарювання обумовлює правильність вибору методики, прийомів та форм оперативного контролю;
3) форма власності визначає рівень забезпеченості оперативного контролю нормативно – правовим регулюванням, яке в свою чергу класифікується за ступенем участі у його формуванні законотворчих органів та поділяється на такі види:
– загальнодержавне (здійснюється на рівні держави, під його дію як правило попадають державні та комунальні підприємства);
– галузеве (діє тільки у межах однієї галузі народного господарства);
– внутрішньогосподарське (здійснюється та формується на рівні підприємства)
4) розмір підприємства (кількість виробничих підрозділів, багатоступеневий цик виробництва і реалізації) впливає на кількість штатних одиниць, безпосередньо задіяних у спостереженні та перевірці за ходом здійснення господарсько-виробничих процедур та операцій.

З врахуванням вищенаведених особливостей та з метою дієвості оперативного контролю можна висловити думку про те, що його ефективне здійснення забезпечується об'єднанням зусиль усіх зацікавлених у якісному його проведенні осіб. Таких осіб пов'язує тільки досягнення конкретних результатів господарювання, що дає змогу здійснювати оперативну зустрічну перевірку виконання ними своїх функціональних завдань та обов'язків. Разом з тим, вони працюють відокремлено і незалежно, що підвищує неупередженість та якість інформації про дійсний (фактичний) стан господарських операцій та подій. Тому, на нашу думку, доречно вважати таких осіб суб'єктами оперативного контролю та об'єднати їх у такі групи:
1) власники (акціонери) – специфічні користувачі, що мають доступ до всіх сфер та напрямів господарювання, наділені правом контролю за

формуванням різного роду результатів діяльності з метою забезпечення своїх майнових та інших інтересів, але часто обмежені у практичній присутності в ході здійснення господарських подій;

2) управлінський персонал та спеціалісти здійснюють щоденний контроль за переміщенням цінностей, розподілом і використанням ресурсів та засобів виробництва як в середині структурних підрозділів, так і між ними з метою правомірності, економічної ефективності й доцільності реалізації господарських операцій та процедур відповідно до внутрішніх нормативних документів, передбачених календарним планом;

3) спеціальні служби, створені на підприємстві з метою посилення контролю за правильністю дій персоналу підприємства.

Організація діяльності таких служб є гнучкою та структурованою. До них входять як облікові працівники, так і спеціалісти з технології захисту інформації. Для ефективного виконання завдань оперативного контролю спеціальні служби використовують тільки фактичні прийоми його здійснення. Прикладами таких суб'єктів оперативного контролю можуть бути: інвентаризаційні комісії, комісії з розслідування надзвичайних подій та, в окремих випадках, ревізійні комісії; 4) працівники, безпосередньо зайняті захистом інформації. Також вони мають можливість в найкоротші проміжки часу виявляти будь-які відхилення, збої та порушення нормального ходу обробки інформації на підприємстві. Концептуальна основа оперативного контролю розкриватиме, конкретизуватиме та ідентифікуватиме його предмет і метод.

Разом з тим зауважимо, що метод та його прийоми є більш наступними поняттями відносно предмету, оскільки саме останній визначає область дії окремого явища, а відповідні існуючі умови формують його методичне забезпечення. На основі цього вважаємо за доцільне насамперед уточнити суть предмета оперативного контролю, що забезпечить коректне визначення його методу, прийомів та способів здійснення. Для дослідження предмета оперативного контролю необхідно оцінити його з боку внутрішніх користувачів інформації, зокрема управлінців різних рівнів. Важливим є точне та неупереджене розуміння функціональної приналежності оперативного контролю до внутрішнього, як такого, що становить систему заходів, організованих керівництвом підприємства, що реалізуються з метою найефективнішого виконання всіма працівниками своїх обов'язків при здійсненні обробки інформації. Внутрішній контроль визначає законність таких операцій та їх доцільність для підприємства. Роль оперативного

контролю в цьому процесі полягає у постійній присутності в ході виникнення окремих подій і явищ, а також своєчасній оцінці при появі відхилень чи інших недоліків обробки інформації. Крім того, в окремих випадках оперативний контроль здійснюється інтуїтивно, що забезпечує його постійність і можливість вчасно виявити відхилення чи інші негативні явища. У деяких ситуаціях важливу роль відіграє людський фактор, який дає змогу незалежно від існування певних методик, нормативів чи доручень усунути формування небажаного результату в найкоротші терміни. Така особливість є, безумовно, позитивною характеристикою оперативного контролю і істотно впливає на визначення його предмета.

Вивчення психологічних аспектів поведінки людини в умовах жорсткого контролю та використання його результатів для покарань показали, що саме такі умови змушують їх більше часу приділяти пошуку виправдань власних дій. Актуальність та цінність такого погляду в сучасних умовах господарювання відносно оперативного контролю полягає насамперед у тому, що збільшення (зменшення) чи зростання (спад) окремих показників порушень не завжди розцінюється як небажане явище. Така особливість дає змогу встановити прямий зв'язок між елементами системи оперативного контролю.

Відсутність єдиної думки про предмет оперативного контролю нівелює його можливість виділитись в окрему самостійну функцію управління. Тому, враховуючи існуючі реалії теорії і практики щодо обґрунтованої потреби в оперативному контролі в сучасних умовах та недостатньому його вивченні, основні ознаки його предмета згруповані й уточнені. Так, предмет як економічна категорія має визначати межі застосування окремих процесів чи систем та з іншого боку бути своєрідним зв'язком між окремими самостійними ланками управління. Отже, предмет оперативного контролю має містити:

1) характеристику визначеної частини дій, що створюють певний вплив на стан, форму і рівень використання інформаційних ресурсів;

2) думку про те, що коло осіб, зайнятих у процесі перевірки дій персоналу підприємства, подій та явищ, не є обмеженим і формується залежно від організаційної структури та інших особливостей діяльності;

3) об'єкти, які вважаємо вужчими поняттями, але тільки ті, що відповідають критеріям оцінки з погляду можливості й доцільності їх оперативної перевірки;

4) рекомендації з вибору можливих методів, прийомів та способів здійснення

оперативного контролю, але чітко не визначати їх обов'язковість;
5) якісну характеристику інтервалів часу такої діяльності, враховуючи, що остання має відповідати тривалості підконтрольних господарських процесів й операцій.

Визначення предмета оперативного контролю дає змогу з'ясувати його місце серед інших систем управління. Разом з тим, можна виявити взаємозалежності інших елементів й складових господарської діяльності. Згруповані та уточнені ознаки предмета дають змогу наголосити на тому, що оперативний контроль є невід'ємною частиною господарського та внутрішнього контролю, оскільки забезпечує ефективне досягнення накреслених цілей шляхом реалізації прийнятих управлінських рішень у процесі виконання поставлених завдань. Крім того, оперативний контроль є не тільки окремим видом, він є безумовною складовою інших підсистем (форм, видів) контролю. Це пояснюється насамперед таким:

- ефективність інформаційного контролю, виконання самих планів та операцій інформаційного контролю забезпечується своєчасною оцінкою правильності, законності та доцільності здійснених дій, отриманих даних контролю, проведених розслідувань в ході їх здійснення;
- результативність адміністративного контролю можлива за умови поточного нагляду за виконанням функціональних обов'язків, повноважень службовцями та керівниками;
- також особливої уваги потребує несанкціоноване делегування повноважень в ході нормального операційного режиму;
- крім того, оперативний контроль виконує особливу стимулюючу функції при запровадженні мотиваційних та іншого роду програм;
- доцільність інформаційного контролю (контроль обробки інформації) забезпечується можливістю попередити виникнення невиправданих втрат.

Крім того, значення оперативного контролю обумовлюється ще й тим, що він є засобом попередження формування недостовірної та викривленої інформації. Оперативний контроль як процес, що забезпечує виконання запланованих дій і процесів відповідно до потреб, правил і нормативів, здійснюється шляхом використання специфічних прийомів і способів, сукупність яких називається його методом. Метод та предмет формують систему оперативного контролю. З боку практики важливо спиратись на основну мету та завдання оперативного контролю, реалізація яких прямо залежить від правильності вибору методики його проведення. Разом з тим в сучасних умовах контрольні процедури потребують удосконалення й

доповнення з метою отримання доречної та неупередженої інформації про фактичний стан справ захисту інформації на підприємства.

При здійсненні оперативного контролю документальні способи і прийоми не можуть бути реалізовані повною мірою. Документи в системі діловодства складаються після завершення господарського операції – тоді, коли результат від її здійснення вже відомий (підписання договорів, актів, протоколів). Оперативний контроль, своєю чергою, проводиться в процесі виконання певних дій і перевіряє їх відповідність запланованим. Тобто документ на той час ще не може бути складеним, оскільки на це немає юридичної підстави. Однак, необхідно зауважити, документальні прийоми і способи в оперативному контролі можуть бути використані на основі документів оперативного обліку та внутрішньої специфічної звітності. Фактичні прийоми в оперативному контролі можуть використовуватись варіативно, відповідно до потреб і можливостей суб'єктів його здійснення, а також з врахуванням галузевої специфіки, форм господарювання, напрямів і видів діяльності підприємства. Також способи проведення перевірок можуть бути комбінованими з метою оперативного забезпечення користувачів доречною та своєчасною інформацією.

Узагальнюючи вищевикладене, в сучасних умовах актуальність оперативного контроль зростає. Він має бути основою для забезпеченні інтересів користувачів різних рівнів оперативною інформацією про фактичний стан захисту інформації, операцій і подій з метою попередження небажаних ситуацій в ході їх здійснення. Реалізація мети концепції розвитку оперативного контролю можлива за умови належних організації та методики його проведення на окремих підприємствах. Разом з тим, організація і методика проведення перевірок, оглядів і спостережень потребують детальних досліджень, уточнень та вдосконалення.

Контрольні запитання

1. У чому заключена раціональна організація та методика проведення оперативного контролю?
2. Опишіть структуру концепції розвитку оперативного контролю.
3. Назвіть мету операт*и*вного контролю.
4. Що є завданням оперативного контролю?
5. З чого починається побудова організаційної структури оперативного контролю?

7. ОСОБЛИВОСТІ АУДИТУ ІНФОРМАЦІЙНИХ СИСТЕМ І ТЕХНОЛОГІЙ

Важко переоцінити вплив комп'ютерних систем і технологій на загальну роботу підприємства та її ефективність. Практично вся облікова інформація підприємства концентрується в різноманітних електронних облікових системах. Ризики, пов'язані з комп'ютерно-інформаційними системами, величезні. У першу чергу це питання ефективності використання програмно-апаратних ресурсів і можливості максимальної автоматизації всієї системи обліку. Важливу роль відіграє також підтримка на сучасному рівні інформаційної архітектури (сукупність інформаційних систем і потоків між ними), що забезпечує обробку й зберігання облікової інформації в умовах всі зростаючих вимог до швидкодії й надійності. І, нарешті, необхідно забезпечувати всебічний захист даних від несанкціонованого доступу, що є одним із пріоритетних завдань.

На сьогодні достатня кількість підприємств придбаває і впроваджує комп'ютерну техніку або програмне забезпечення. У числі завдань аудиторських підприємств, в цьому випадку, можуть бути аналіз результатів впровадження, оцінка ефективності різних етапів експлуатації, ступінь відповідності очікуванням керівництва.

Міжнародний стандарт аудиту МСА 401 «Аудит у середовищі комп'ютерних інформаційних мереж» (Auditing in Computer Information Systems Environment) описує навички й компетентність, якими повинна володіти аудиторська група при проведенні аудита в середовищі комп'ютерних інформаційних систем. Зазначений МСА також надає рекомендації, що стосуються делегування роботи асистентам, що володіють навичками в даній області, і використання роботи інших аудиторів або експертів з подібними навичками. Зокрема, аудиторська група повинна мати достатні знання, щоб планувати, виконувати й використовувати результати обраних аудиторських методів.

Практично кожний підручник з аудиту містить окремий розділ, який присвячений аудиту у комп'ютерному середовищі. Про цікавість до даної проблеми свідчить також і той факт, що значна кількість дисертаційних робіт містить рекомендації щодо удосконалення аудиту в середовищі електронної обробки даних [1-7]. Питання проведення аудиторських перевірок з використанням комп'ютерної техніки і програмного забезпечення обговорюються на сторінках фахової преси [8, 9, 10].

Проте, незважаючи на постійну увагу до даної проблематики, як з боку

науковців так і практиків, все ще залишаються доволі суттєві прогалини, які стосуються, в першу чергу розробок конкретних методик для окремих об'єктів аудиторських перевірок.

Метою даної лекції є узагальнення практики проведення аудиту у комп'ютерному середовищі та подання власного бачення аудиту інформаційних систем і технологій. Крім того, в цієї лекції запропонується порядок оцінки аудиторами результатів процесу впровадження нової комп'ютерної техніки й програмного забезпечення підприємства-замовника аудиту.

Використання комп'ютерного середовища в аудиті, окрім МСА 401 передбачено ще такими документами, як:

- Положенням про міжнародну аудиторську практику 1001 «Середовище комп'ютерних інформаційних систем – автономні мікрокомп'ютери»;
- Положенням про міжнародну аудиторську практику 1002 «Середовище комп'ютерних інформаційних систем – інтерактивні комп'ютерні системи»;
- Положенням про міжнародну аудиторську практику 1003 «Середовище комп'ютерних інформаційних систем – системи баз даних»;
- Положенням про міжнародну аудиторську практику 1009 «Методи аудиту з використанням комп'ютерів» [11];
- прикладна програма може поставити аудитора перед необхідністю використання комп'ютера як засобу контролю. Ці різнобічні варіанти використання комп'ютера відомі як «Методи Аудиту при Сприянні Комп'ютера (МАСК)». До них належать:

а) програмне забезпечення;

б) тестові дані.

Необхідність використання МАСК виникає за тих обставин, коли відсутні вхідні документи і неможливо простежити повний хід операцій (контрольний слід), а також тоді, коли ефективність аудиту можна значно поліпшити використанням спеціальної комп'ютерної аудиторської програми. Аудиторське програмне забезпечення складається із комп'ютерних програм, що використовуються аудитором як елемент аудиторських процедур для обробки даних, що мають суттєве значення для аудиту і взяті з облікової системи клієнта. Програмне забезпечення може складатись із:

- пакета програм;
- програм спеціального призначення (використання);
- програм-утилітів.

Пакет програм – це узагальнені комп'ютерні програми, що призначені

для виконання функцій з обробки даних, включаючи зчитування комп’ютерних файлів, відбір інформації, проведення розрахунків, створення файлів з даними і друкування звітів за формою, що визначена аудитором.

Програми спеціального призначення – це програми, розроблені для виконання конкретних аудиторських завдань. Ці програми можуть бути створені як самим аудитором, так і іншим спеціалістом.

Програми-утиліти – програми, що використовуються суб’єктом для виконання загальних функцій обробки даних. Такі програми, як правило, не призначені конкретно для аудиторської практики.

Тестові дані – це дані (як правило, вибіркові дані), що призначені для внесення аудитором в комп’ютерну систему суб’єкта та порівняння отриманих результатів із раніше визначеними результатами [11].

Перш за все, необхідно сказати про компетентність аудиторів, які будуть проводити контрольні процедури перевірки. Компетентність аудитора не може бути рівнозначною сумі знань професійного фахівця з комп'ютерних систем. Рівень необхідних знань залежить від складності й характеру аудиторських процедур і облікової системи підприємства. Аудитору бажано мати належне уявлення про технічний, програмний, математичний і інший види забезпечення комп'ютерної техніки, а також про системи обробки інформації. У випадку відсутності в аудитора зазначених знань варто використовувати роботу експертів в області інформаційних технологій. Однак у випадку використання роботи експерта варто пам'ятати, що аудитор повинен мати достатнє уявлення про комп'ютерну систему в цілому, для того щоб планувати, регулювати й контролювати роботу експертів.

Аудитору необхідно провести аналіз і скласти висновок по всіх істотних питаннях організації комп’ютерно-інформаційної системи, а саме:

- детальний розгляд функціонування комп’ютерно-інформаційної системи (способи організації, уведення, настроювання, відновлення даних);
- забезпечення архівування й зберігання даних;
- наявність спеціальних контрольних процедур для моніторингу функціонування середовища комп'ютерної обробки даних;
- аналіз програмного забезпечення й наявність ліцензій;
- відповідність застосовуваних алгоритмів вимогам нормативної документації по веденню обліку й стану звітності по основних автоматизованих розрахунках (бізнес-процесам);
- можливості гнучкого реагування на зміни законодавства з погляду

настроювання (відновлення) програмного забезпечення;
- можливості розширення функцій наявних комп’ютерно-інформаційних систем;
- питання інформаційної безпеки (обмеження несанкціонованого доступу);
- аналіз загальної інформаційної політики й планів розвитку системи інформаційних технологій суб'єкта, що перевіряється.

На тлі розвитку бізнесу стрімко збільшується кількість оброблюваних облікових даних, збільшується число інформаційних систем, що автоматизують різні види діяльності. В умовах великого підприємства із широкою інформаційною архітектурою для керівництва не завжди прозора діяльність співробітників, які розробляють, впроваджують і підтримують всю сукупність інформаційних систем, а також модель взаємодії інформаційних систем різних рівнів. Рішенням цього завдання і може зайнятись аудит інформаційних систем і технологій. У цій області на сьогоднішній день найбільш актуальними стають наступні завдання:
- аналіз ризиків існуючої комбінації інформаційних систем за різними показниками. Дане завдання містить у собі повну перевірку всіх інформаційних систем підприємства, їх взаємодії, виявлення недоліків і невідповідностей, формулювання пропозицій (рекомендацій) по вдосконаленню використання існуючих інформаційних систем і роботи відділу інформаційних технологій в цілому;
- аналіз результатів процесу впровадження нового обладнання й програмного забезпечення при необхідності оцінки ефективності придбаного підприємством дорогого встаткування й витрат на впровадження нових автоматизованих систем;
- аналіз планованих до впровадження автоматизованих інформаційних систем і визначення їх можливої ефективності й економічної обґрунтованості впровадження.

У результаті виконання аудиторських процедур по перевірці інформаційних систем і роботи фахівців відділу інформаційних технологій керівництво підприємства одержить аудиторський висновок по всіх істотних питаннях, як-от:
- оцінка ступеня автоматизації й настроювання облікових процесів;
- адекватність контрольних процедур;
- аналіз однорідності й сумісності системних рішень;
- аналіз ризиків, пов'язаних із впровадженням нових інформаційних систем;
- помилки й невідповідності в автоматизованих інформаційних системах;

- моніторинг працездатності й продуктивності інформаційних систем, реакція й дії в критичних ситуаціях;
- питання схоронності інформації й відновлення даних;
- оцінка якості інформаційної безпеки (організація й керування ролями й повноваженнями в інформаційних системах, парольна політика, аудит подій і дій користувачів, контроль несанкціонованого доступу);
- структура ролей у відділі інформаційних технологій і ступінь залежності безпеки підприємства від цих кадрів, оцінка кваліфікації таких співробітників і процес підтримки повноти й актуальності бази знань у даній області, мотивація персоналу з метою зниження ризиків втрати кадрів, що володіють реальним практичним досвідом.

При вирішенні аудитором завдання аналізу результатів процесу впровадження нового обладнання й програмного забезпечення проводиться огляд проекту впровадження з метою його поточного виконання, оцінки адекватності контрольних процедур у процесі керування проектом, а також ступеня виконання рекомендацій зовнішніх консультантів у рамках проекту по забезпеченню якості впровадження інформаційних систем. Основні етапи аудиту впровадження інформаційних систем і технологій, схематично представлено на рис.7.1.

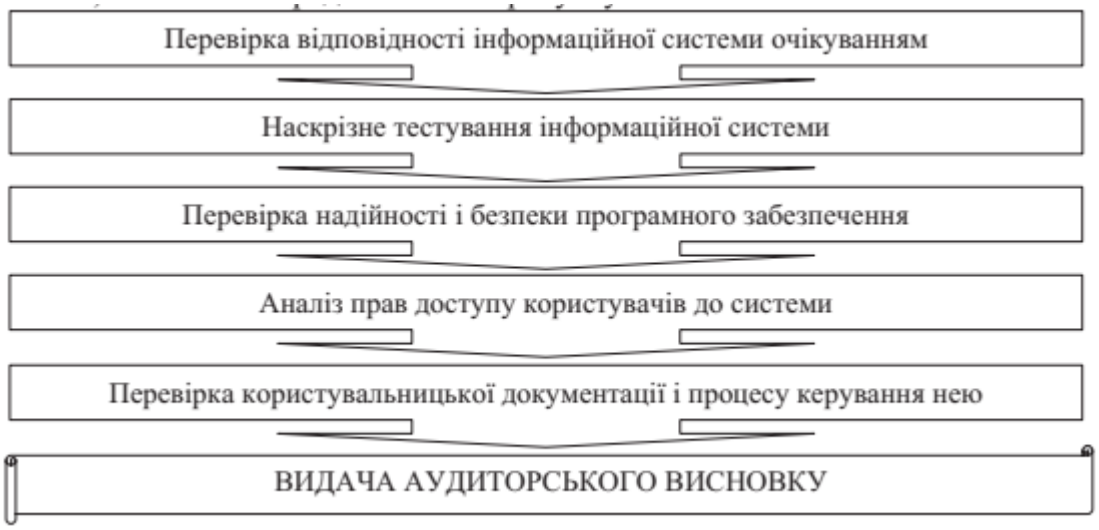

Рисунок 7.1. Основні етапи аудиту впровадження інформаційних систем і технологій

На першому етапі зазвичай перевіряється відповідність інформаційної системи очікуванням керівництва, аналізується процес прийняття рішень у процесі автоматизації, відмінність реалізованої системи від запланованої на початковому етапі впровадження.

Самим складним, тривалим і трудомістким етапом перевірки є наскрізне тестування впровадженої облікової системи. Групі аудиторів необхідно не тільки перевірити відповідність роботи системи заданим алгоритмам, повноту й коректність облікових даних, але й провести перевірку роботи програмного контролю підтвердження (узгодження) документів у системі, що визначає ієрархію відповідальності й адекватне розмежування повноважень. Крім того, необхідно оцінити ступінь автоматизації облікових процесів, щоб мінімізувати додаткові трудовитрати, пов'язані з ручним контролем. У процесі тестування аудитором оцінюється також досконаліть системи автоматичного контролю некоректних дій в обліковій системі (непідтверджених, фальсифікованих даних, помилок ручного уведення), що дозволяє знизити інформаційні ризики. У системі повинні бути організовані періодичні звірення, аналізи даних і звітів з метою виявлення можливих відхилень. Однієї з найважливіших характеристик впровадженої системи є можливість інтеграції з іншими інформаційними системами, можливості автоматичного імпорту/експорту, програмна верифікація підсумків даних різних систем.

Питанням надійності й безпеки системи в ході перевірки також приділяється значна увага. Недоліки організації контролю доступу до системи виявляються за допомогою спеціалізованих аудиторських процедур: практики періодичного аналізу прав користувачів на предмет їх надмірності, наявності системного підходу до поділу повноважень за допомогою обмеження доступу до бізнес-функцій. Невиконання даних вимог може привести до серйозних наслідків: несанкціонованому доступу до даних і виконання неавторизованих операцій у системі, неможливості однозначного визначення відповідальності за зміни. Аудитором може бути рекомендовано сформувати матрицю розмежування повноважень для забезпечення дотримання принципів мінімальних прав доступу, документувати всі зміни в системі контролю доступу й привести їх у відповідність із посадовими обов'язками.

На наступному етапі проводиться аналіз права доступу розроблювачів і співробітників відділу інформаційних технологій до системи. Розроблювачі, як правило, мають необмежений доступ до облікової системи, співробітники відділу інформаційних технологій мають необмежені права в системі на рівні модулів, задіяних в автоматизованих ними процесах. Це збільшує ризики несанкціонованої зміни даних облікової системи в результаті ненавмисних або навмисних дій користувачів, що мають необмежені права й при цьому не

несуть пряму відповідальність за дії в системі.

Рекомендації аудиторів у цьому випадку можуть бути наступними: проведення аналізу виробничої потреби наявності у співробітників необмежених прав у системі, аналіз процесу керування змінами й доступом, забезпечення протоколювання всіх дій користувачів, що володіють розширеними повноваженнями, організація аудита подій, що дозволяє однозначно встановити відповідальність за дії в системі і встановити хронологію внесення змін.

На заключному етапі перевіряється користувальницька документація й процес керування документацією, неактуальність якої, особливо у випадку впровадження нової системи, може привести до зниження ефективності й оперативності роботи користувачів у системі, а також ускладнює проведення адекватного аналізу ризиків і знижує рівень якості контролю в процесі керування проектом.

Аудиторський висновок по проекту впровадження дає цілісну картину процесу, що дозволяє оцінити стан справ на поточному етапі, перелік недоліків, невідповідностей, можливих ризиків, пов'язаних з ними, і рекомендації з їх усунення. Це дозволить керівникам оцінити якість впровадження, можливості системи, пріоритетність планованих завдань і вибір подальшої стратегії розвитку.

Результати таких аудиторських перевірок дозволять керівництву одержати достовірну, повну й точну інформацію про стан справ у цій області, що дозволить збільшити загальну ефективність і економічну обґрунтованість прийняття управлінських рішень як в частині впровадження інформаційних систем і технологій так і в цілому.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Облік і аудит капітальних інвестицій (на прикладі житлобудівних підприємств): автореф. дис... канд. екон. наук: 08.00.09 [Електронний ресурс] / О.С. Гавриловський; Держ. вищ. навч. закл. «Київ. нац. екон. ун-т ім. В.Гетьмана». – К., 2008. – 20с. – укр.

2. Аудиторська діяльність в аграрному секторі АПК: автореф. дис... канд. екон. наук: 08.00.09 [Електронний ресурс] / О.Г. Пономаренко; Нац. наук. центр «Ін-т аграр. Економіки» УААН. – К., 2007. – 20с. – укр.

3. Облік і аудит нематеріальних активів (на прикладі підприємств харчової промисловості): автореф. дис... канд. екон. наук: 08.00.09 [Електронний ресурс] / Н.М. Бразілій; Київ. нац. екон. ун-т ім. В.Гетьмана. – К., 2007. – 20с.

– укр.
4. Облік і аудит нематеріальних активів: теорія, організація, методика: Автореф. дис... канд. екон. наук: 08.06.04 [Електронний ресурс] / С.В. Шульга; Держ. акад. статистики, обліку та аудиту Держкомстату України. – К., 2006. – 21с. – укр.
5. Облік, аналіз та аудит праці і її оплати: Автореф. дис... канд. екон. наук: 08.04.06 [Електронний ресурс] / Т.Г. Мельник; Київ. нац. ун-т ім. Т.Шевченка. – К., 2006. – 20с. – укр.
6. Фінансовий облік та внутрішній аудит товарних запасів в оптовій торгівлі України: Автореф. дис... канд. екон. наук: 08.06.04 [Електронний ресурс] / О.А. Зоріна; Укоопспілка, Львів. комерц. акад. – Л., 2005. – 21с. – укр.
7. Облік та аудит фінансових результатів діяльності промислових підприємств: Автореф. дис... канд. екон. наук: 08.06.04 [Електронний ресурс] / Г.М. Курило; Київ. нац. екон. ун-т. – К., 2004. – 19с. табл. – укр.
8. Ширяева О.В. МСА 401 «Аудит в среде компьютерных информационных сетей» («Внедрение Международных стандартов финансовой отчетности (МСФО) в кредитной организации») / О.В. Ширяева // Бухгалтерия и финансы. – 2007. – № 2. – С.19-24.
9. Славкова О.П. Особливості проведення аудиту в комп'ютерному середовищі / О.П. Славкова // Економіка АПК. – 2006. – №3. – С.45-49.
10. Тарасенко Ю.О. Особливості аудиту в комп'ютерному середовищі / Ю.О. Тарасенко // Збірник тез наукових доповідей XI Міжвузівської студентсько-аспірантської конференції 21 листопада 2008 року «Перспективні напрями реформування фінансової системи України».
11. Особливості проведення аудиту в комп'ютерному середовищі [Електронний ресурс]. - http://library.if.ua/book/78/5611.html (lfnf pdthytyyz 13/05/2023).

Контрольні запитання

1. Назвіть міжнародні стандарти аудиту.
2. У чому є завдання аудиту інформаційних систем і технологій?
3. Назвіть основні етапи аудиту впровадження інформаційних систем і технологій.
4. Що може бути у рекомендаціях аудиторів?
5. Аудиторський висновок є обов'язковим для виконання?

8. КОМПЛЕКСНИЙ АУДИТ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Комплексний аудит інформаційної безпеки передбачає перевірку технічних засобів (інструментальний аудит) та організаційних заходів (організаційний аудит), впроваджених з метою забезпечення інформаційної безпеки (рис. 8.1). Зокрема, аудит безпеки інформаційних систем (ІС) дозволяє отримати найбільш повну і об'єктивну оцінку захищеності ІС, локалізувати наявні проблеми і розробити ефективну програму побудови системи забезпечення ІБ організації.

Рисунок 8.1. Комплексний аудит інформаційної безпеки

8.1. Основні етапи аудиту безпеки інформаційних систем

Проведення аудиту безпеки ІС організації складається з чотирьох етапів:

1. Постановка задачі та уточнення обсягу робіт.
2. Збір і аналіз інформації.
3. Проведення аналізу ризиків.
4. Розробка рекомендацій.

Постановка задачі та уточнення обсягу робіт. На даному етапі проводиться збір первинних даних від замовника, їх попередній аналіз, а також організаційні заходи з підготовки до проведення аудиту:

- уточнюються цілі і задачі аудиту;
- формується робоча група;
- готується і узгоджується технічне завдання на проведення аудиту.

На цьому етапі мета проведення аудиту уточнюється і плануються всі

наступні кроки. До складу робочої групи мають входити як аудитори (компанії, що проводять аудит), так і співробітники організації, що підлягає аудиту. Останні забезпечують подання всієї необхідної інформації, контролюють процеси проведення обстеження, а також беруть участь в узгодженні його результатів (проміжних і кінцевих). Аудитори відповідають за кваліфіковане проведення робіт по обстеженню предметних областей відповідно до визначених цілей та завдань проекту, узгоджують процеси і результати проведення обстеження. Етап постановки задачі завершується розробкою, узгодженням та затвердженням технічного завдання (ТЗ). У ТЗ на аудит фіксується склад і зміст робіт з аудиту та вимоги до звітних документів. Крім того, в ТЗ вносять терміни проведення робіт, а при необхідності відображають їх план-графік. Паралельно з ТЗ розробляється угода про конфіденційність і організується взаємодія зі службою безпеки замовника.

Збір і аналіз інформації. На цьому етапі збирається інформація і надається оцінка:

- організаційним заходам у сфері ІБ;
- програмно-технічних засобам ЗІ;
- заходам щодо забезпечення фізичної безпеки.

Аналізуються наступні характеристики побудови і функціонування корпоративної ІС:

- організаційні характеристики;
- організаційно-технічні характеристики;
- технічні характеристики, пов'язані з архітектурою ІС;
- технічні характеристики, пов'язані з конфігурацією мережевих пристроїв і серверів ІС;
- технічні характеристики, пов'язані з використанням вбудованих механізмів ІБ.

Після отримання первинних даних готується звіт про обстеження. Звіт про обстеження є основою для наступних етапів аудиту: аналізу ризиків та розробки рекомендацій. Під час цього етапу проводиться:

1) аналіз роботи всіх програмних та апаратних рішень, які забезпечують безпечну і безперервну роботу ІТ-інфраструктури підприємства, зокрема аналіз:

- засобів забезпечення мережної безпеки – міжмережевих екранів, проксі серверів, засобів організації VLAN, засобів організації захищеної міжмережевої взаємодії (Site-to-Site VPN), засобів організації безпечного

віддаленого доступу до корпоративних ресурсів (Remote Access VPN) тощо;
- засобів антивірусного захисту робочих станцій, серверів, електронної пошти, доступу в Інтернет;
- засобів шифрування даних;
- засобів забезпечення резервного копіювання даних і ПЗ;
- засобів безперебійного живлення устаткування;
- засобів контролю за розповсюдженням і використанням конфіденційної інформації;
2) аналіз заходів щодо захисту апаратного забезпечення (мережевого обладнання, серверів, робочих станцій, систем зберігання), зокрема:
- аналіз наявності та відповідності конфігурацій штатних механізмів ІБ рекомендаціям виробника і кращій практиці;
- аналіз заходів щодо забезпечення доступу;
- виявлення сервісів, які не використовуються, і сервісів, що містять відомі уразливості;
3) збір даних про взаємозв'язки об'єктів аудиту з іншими елементами ІТ інфраструктури, документування етапів бізнес-процесів і відхилень від них;
4) документування топології та логічної організації мережевої інфраструктури, адекватності заходів контролю логічних шляхів доступу, сегментування мережі;
5) документування топології та логічної організації системи захисту периметра, адекватності заходів контролю доступу з зовнішніх і внутрішніх мереж;
6) документування топології, логічної організації та адекватності контролю доступу між сегментами документованої мережі;
7) пошук і аналіз роботи елементів мережі, збої в роботі яких призведуть до неможливості функціонування критичних для бізнесу сервісів;
8) аналіз роботи точок віддаленого доступу до інформаційних ресурсів мережі та перевірка адекватності захисту доступу;
9) оцінка відповідності конфігурації вбудованих засобів захисту документованим вимогам і оцінка адекватності існуючої конфігурації;
10) оцінка адекватності використання криптографічного захисту інформації та процедури розподілу ключів шифрування;
11) оцінка достатності заходів антивірусного контролю робочих станцій і серверів;
12) перевірка наявності резервних копій файлів конфігурації та образів

дисків для критичних мережевих пристроїв і серверів;
13) перевірка наявності джерел безперебійного живлення для критичних мережевих пристроїв і серверів і їх відповідність вимогам щодо часу безперебійної роботи;
14) аналіз заходів захисту обладнання, необхідного для підтримки функціонування ІТ-інфраструктури, ступеня захисту наявних приміщень, систем зв'язку та структурованих кабельних систем, зокрема, перевірку актуальності операційних систем, систем управління базами даних, інтеграції застосунків тощо, у тому числі наявність необхідних патчів (виправлення до файлів);
15) документування етапів бізнес-процесів, систем документообігу, зберігання даних і надання послуг. Оцінка достатності ПЗ, використовуваного на різних етапах;
16) збір інформації про навички, знання та досвід роботи персоналу, безпосередньо пов'язаного з обслуговуванням ІТ-інфраструктури, наданням ІТ послуг;
17) документування комплексу заходів щодо забезпечення ІБ, зокрема:
- можливості використання знайдених уразливих місць в мережевих пристроях і серверах для реалізації атак;
- процедури оцінки повноти аналізованих подій, адекватності захисту журналів аудиту;
- наявності процедур щодо виявлення і фіксації інцидентів ІБ та механізмів розслідування таких інцидентів, включаючи процедури аналізу журналів подій та спроб несанкціонованого доступу;
- наявності процедури документування будь-яких дій, пов'язаних з модифікацією прав доступу, змінами параметрів аудиту;
- періодичності контролю захищеності мережевих пристроїв і серверів; - наявності процедури відстеження нових уразливостей в системному ПЗ і його оновлення;
- заходів з обмеження доступу в серверні приміщення; - адекватності часу відновлення у випадку збоїв критичних пристроїв і серверів;
18) перевірка наявності зони дослідної експлуатації нових рішень, процедур тестування та введення в промислову експлуатацію нових програмних і апаратних рішень;
19) перевірка наявності організаційних заходів у сфері ІБ, зокрема:
- наявність, повноту та актуальність організаційно-регламентних та нормативно-технічних документів;

- існування ролей доступу персоналу до критично-важливої інформації, мережних пристроїв і серверів. Відповідність цих ролей мінімальному набору прав, необхідних для виконання виробничих завдань;
- відповідність механізму й стійкості процедури аутентифікації, оцінка адекватності парольної політики та протоколювання діяльності користувачів;
- наявність нормативних документів, що описують повноваження працівників щодо доступу до мережевих пристроїв і серверів, і списків персоналу, які мають доступ до цих пристроїв;
- наявність відповідального за забезпечення ІБ;
- наявність заходів щодо підтримки рівня знань працівників у сфері ІБ, планів навчання працівників, відповідальних за підтримання системи ІБ;
- обізнаність користувачів локальної мережі про вимоги щодо забезпечення ІБ;
- коректність процедур управління змінами і установки оновлень;
- порядок надання доступу до внутрішніх ресурсів інформаційних систем. Збір даних може здійснюватися шляхом:
- інтерв'ювання персоналу замовника з використанням заздалегідь підготовлених опитувальних листів; - аналізу наданих документів;
- огляду та інвентаризації інфраструктури з використанням спеціалізованого програмного інструментарію і шаблонів звітів;
- збору та аналізу конфігурацій засобів ЗІ;
- аналізу сценаріїв здійснення атак і використання списків перевірки;
- аналізу організаційно-розпорядчої документації щодо забезпечення режиму ІБ;
- інструментального обстеження шляхом застосування спеціальних засобів аналізу захищеності.

Інтерв'ювання персоналу призначено як для документування бізнес процедур, так і для виявлення існуючих проблем, пов'язаних з використанням програмного і апаратного забезпечення. До інтерв’ювання обов'язково залучаються:
- працівники, що безпосередньо використовують ПЗ для вирішення своїх завдань;
- фахівці, пов'язані з наданням ІТ-послуг.

В ході інтерв'ювання необхідно враховувати, що розуміння однієї й тієї ж проблеми може істотно відрізнятися, наприклад, користувачем та системним адміністратором. Результатом цього етапу є комплект документів, що містять повну інформацію щодо всіх аспектів функціонування системи

інформаційної безпеки.

Проведення аналізу ризиків. Проведення даного етапу є важливим етапом аудиту ІБ. Аналіз ризиків проводиться для оцінки реальних загроз порушення ІБ і розробки рекомендацій, виконання яких дозволить мінімізувати ці загрози. Вихідною інформацією для аналізу ризиків є погоджений з аудиторською організацією звіт про проведене обстеження. Аналіз ризиків дає можливість:

- адекватно оцінити існуючі загрози;
- ідентифікувати критичні ресурси ІС;
- виробити адекватні вимоги щодо захисту інформації;
- сформувати перелік найбільш небезпечних уразливих місць, загроз та потенційних зловмисників;
- отримати певний рівень гарантій, заснований на об'єктивному експертному висновку. При аналізі ризиків здійснюється:
- класифікація інформаційних ресурсів;
- аналіз уразливостей;
- складання моделі потенційного зловмисника;
- оцінка ризиків порушення ІБ. 102

В процесі аналізу ризиків проводиться оцінка критичності ідентифікованих уразливих місць та можливості їх використання потенційним зловмисником для здійснення несанкціонованих дій. На даному етапі проводиться:

- зіставлення і аналіз зібраних даних; - аналіз ризиків;
- формування висновків і рекомендацій;
- підготовка та оформлення звіту про аудит.

Проведений під час даного етапу аналіз ризиків дозволяє:

- сформувати перелік найбільш небезпечних уразливих місць і загроз;
- скласти модель потенційного зловмисника;
- оцінити ступінь критичності загроз порушення ІБ і можливості їх використання потенційним зловмисником для здійснення несанкціонованих дій;
- розробити рекомендації, виконання яких дозволить мінімізувати існуючі загрози.

Під час даного етапу може бути прийнято рішення про збір додаткових даних.

Розробка рекомендацій. На підставі інформації, отриманої під час перевірки інформаційної інфраструктури замовника та результатів аналізу

ризиків, розробляються рекомендації щодо вдосконалення системи ЗІ, застосування яких дозволить мінімізувати ризики, а також формується список конкретних уразливостей активного мережевого обладнання, серверів, міжмережевих екранів і ін.

Після завершення аудиту готується підсумковий звіт, що містить оцінку поточного рівня безпеки IT-інфраструктури, інформацію про виявлені проблеми, аналіз відповідних ризиків і рекомендації щодо їх усунення. Результатом аудиту безпеки зовнішнього периметра корпоративної мережі є аудиторський звіт. Загальна структура звіту:

1) оцінка поточного рівня захищеності ІС:

- опис і оцінка поточного рівня ІБ системи;
- аналіз інформації про конфігурацію ІС, знайдені уразливості;
- аналіз ризиків, пов'язаних з можливістю реалізації внутрішніх і зовнішніх загроз ресурсам ІС.

2) рекомендації з технічної складової ІБ:

- щодо змін конфігурації існуючих мережевих пристроїв і серверів;
- щодо змін конфігурації існуючих засобів захисту;
- щодо активації додаткових штатних механізмів безпеки на рівні системного програмного забезпечення;
- щодо використання додаткових засобів захисту.

3) рекомендації щодо організаційної складової ІБ:

- щодо розробки політики ІБ;
- щодо організації роботи служби ІБ;
- щодо розробки організаційно-розпорядчих і нормативно-технічних документів;
- з перегляду функцій персоналу та зон їх відповідальності;
- щодо розробки програми обізнаності співробітників з питаннями ІБ;
- щодо підтримки і підвищення кваліфікації персоналу.

8.2. Оцінка діяльності з управління інформаційною безпекою організації

Вимірювання, показники і метрика безпеки. Відповідно до одного із загальновідомих принципів управління вважається, що діяльність не може бути керованою, якщо вона не може бути виміряною. Цей принцип поширюється і на сферу ІБ. Задача оцінювання рівня ІБ організації і функціонування СМІБ на сьогодні невирішена однозначно. Переважно для отримання таких оцінок використовують три поняття: вимірювання (англ. measurement), показники (англ. measures) і метрики безпеки (англ. security

metrics). Зауважимо, що часто вони застосовуються як взаємозамінні (особливо друге і третє), оскільки отримуються при безпосередньому зборі необробленої інформації (англ. raw data), разом з тим мають певні відмінності. Метрики безпеки зазвичай є результатом застосування методу вимірювання для одного або декількох елементів системи, що перевіряється, з метою одержання кількісного значення показника. Метрика – це система показників, призначена для підтримки прийняття рішень, спрямованих на удосконалення певної діяльності шляхом забезпечення її обліку (збору, аналізу і складання звітів за даними, які характеризують цю діяльність). Показник – це число або символ, що ставиться у відповідність елементу системи в процесі вимірювання з метою опису його властивостей (атрибутів), або надання кількісної оцінки ступеня, в якому продукт або процес володіє певним атрибутом.

Основні положення стандарту ISO/IEC 27004:2009. Для допомоги організаціям в оцінці результативності діяльності з управління ІБ призначений стандарт ISO/IEC 27004:2009, який пропонує методологію застосування механізмів оцінювання на основі вимірювань та введення системи показників. Дані, отримані за результатами вимірювання таких показників, є підґрунтям для аналізу та прийняття рішень щодо усунення виявлених проблем, завдяки чому організації підвищують ефективність функціонування їх СМІБ. У стандарті містяться загальні рекомендації щодо розробки і використання показників та їх збору з метою оцінки ефективності впровадженої в організації СМІБ, а також рекомендації щодо окремих об’єктів контролю – елементів управління ІБ (англ. controls), визначених в ISO/IEC 27001, зокрема політики проведення контрольних заходів, управління ризиками ІБ, контрольних завдань, безпосередньо заходів, процесів та процедур, а також підтримки процесу їх перегляду, допомоги у визначенні необхідності зміни чи удосконалення процесів СМІБ і сфер контролю для СМІБ.

Стандарт описує процес збору базових показників, використання операції агрегування отриманих вимірювань, математичного обчислення похідних (від двох і більше базових) показників і застосування аналітичних методів і методів прийняття рішень для виявлення «індикаторів» удосконалення СМІБ. Відправною точкою для розробки показників та процедур їх збору є правильне розуміння організацією ризиків ІБ, з якими вона стикається. Вибрані і використовувані показники повинні характеризувати безпосередньо функціонування СМІБ та бути пов'язаними з

показниками основних бізнес процесів організації. Сам процес вимірювання показників визначається як процес отримання інформації про СМІБ і елементи управління ІБ шляхом вибору показників, проведення вимірювань і обчислень, аналітичної моделі і критеріїв прийняття рішень.

Організація визначає цілі проведення вимірювань показників СМІБ з урахуванням таких факторів:

- роль забезпечення ІБ в основній діяльності організації і ризики ІБ, які при цьому можуть виникнути;
- відповідні вимоги нормативно-правових актів і договірних зобов'язань; - структура організації;
- вартість і очікувана вигода від використання результатів вимірювання ефективності СМІБ;
- критерії прийняття організацією ризиків ІБ;
- необхідність порівняння декількох СМІБ в організації.

Для постійного проведення вимірювань в організації повинна бути розроблена і прийнята відповідна програма, спрямована на досягнення цілей оцінювання рівня ІБ, що забезпечується функціонуванням СМІБ. За отриманими в результаті вимірювання даними приймаються рішення щодо вдосконалення процесів управління ІБ і самої СМІБ, а їх впровадження у діяльність організації здійснюється відповідно до моделі PDCA.

Контрольні запитання

1. Назвіть основні етапи аудиту безпеки інформаційних систем.
2. У чому полягає інтерв'ювання персоналу?
3. Які цілі має проведення аналізу ризиків?
4. Для чого здійснюється оцінка критичності ідентифікованих уразливих місць?
5. Коли приймається рішення про збір додаткових даних?

9. СТАНДАРТИЗАЦІЯ В ГАЛУЗІ МОНІТОРИНГУ СИСТЕМ БЕЗПЕКИ

Існує велика кількість стандартів з питань ІТ і безпеки. Деякі з них – галузеві, інші – загальні. Більшість стандартів засновані на оцінці ризиків як невід'ємної складової процесу їх впровадження і дотримання. З урахуванням того, що закони та нормативні акти також вимагають проведення оцінки ризиків при побудові системи внутрішнього контролю і забезпечення безпеки, стандарти є першим правильним кроком на шляху виконання вимог законодавства. У зв'язку з тим, що існує безліч стандартів у сфері ІБ, організації нерідко стикаються з проблемою вибору найбільш для них придатного. Розглянемо деякі з відомих стандартів.

CobiT. CobiT є стандартом корпоративного управління ІТ, розроблений ISACA. Він адресований фахівцям в області ІТ, керівництву та аудиторам, тому є корисним інструментом для організацій: допомагає керівництву і співробітникам зрозуміти необхідність контролю і дозволяє пояснити вимоги бізнесу співробітникам технічних відділів. CobiT розглядає корпоративне управління ІТ в межах чотирьох основних груп процесів (доменів):

1) організація та планування (PO);
2) придбання і впровадження (AI);
3) функціонування і підтримка (DS);
4) моніторинг та оцінка (ME).

У кожному з доменів виділяються окремі процеси (всього 34), для кожного з них наводяться вимоги до заходів контролю. Серед процесів CobiT існує окремий процес, присвячений забезпеченню ІБ (DS5), хоча і в інших процесах наводяться окремі заходи контролю, пов'язані з безпекою. Відмінною особливістю CobiT є наявність посібника з аудиту, що містить докладну методику перевірки заходів контролю за всіма 34 основними процесами ІТ, в тому числі за процесами, пов'язаними з безпекою. У цьому посібнику докладно розкривається, з ким із співробітників необхідно провести інтерв'ю, які документи проаналізувати, що протестувати. CobiT є корисним інструментом для аудиторів (внутрішніх і зовнішніх). Він надає методологію, за допомогою якої перевіряється рівень зрілості заходів контролю в галузі ІТ. Завдяки цьому керівництво організації може визначити, як діяти, і з’являється можливість сконцентрувати ресурси для вдосконалення заходів контролю на тих ділянках, де потрібні поліпшення.

ITIL. Іншим корисним інструментом, який може застосовуватися для удосконалення системи ІБ, є бібліотека інфраструктури інформаційних технологій (англ. Information Technology Infrastructure Library, ITIL). ITIL –

набір оптимальних методів і принципів, які визначають інтегрований, заснований на процесах підхід з управління IT. На сьогодні інтерес до застосування ITIL продовжує зростати в усьому світі. ITIL рекомендує впровадження ефективних заходів у галузі ІБ на стратегічному, тактичному та операційному рівні. Забезпечення ІБ розглядається як циклічний процес з фазами планування, впровадження, оцінки та підтримки. ITIL оперує такими поняттями в галузі ІБ як політики, процеси, процедури та інструкції. Хоча в ITIL відсутні безпосередні спеціалізовані стандарти оцінки відповідності, проте цей стандарт близький британському стандарту BS 15000 (ISO 20000), присвяченому управлінню IT-сервісами та методам оцінки. Оцінка якості аудиторів BS 15000 (ISO 20000) здійснюється UKAS (Британським агентством акредитації). UKAS встановлює основні вимоги до аудиторів в частині навчання, кваліфікації, наявності досвіду у сертифікаційних компаніях (тобто у компаніях аудиторів, які проводять сертифікаційний аудит). UKAS регулярно проводить аудит сертифікаційних компаній з метою переконатися, що вони можуть документально підтвердити свою компетентність з проведення сертифікаційних аудитів. BS 15000 (ISO 20000) містить докладні посібники для організацій, які бажають отримати сертифікацію, і вимоги до аудиторів. У 2005 році стандарт BS 15000 був представлений в ISO і після завершення процедури його розгляду був прийнятий як ISO/IEC 20000.

ISO/IEC 15408. Ще одним широко обговорюваним стандартом у галузі безпеки є стандарт ISO/IEC 15408 (Загальні критерії). Цей стандарт технічний і іноді важкий для сприйняття бізнесом. Він корисний для постачальників і покупців продукції ІБ, щоб визначити, наскільки надійний механізм захисту має продукт, що купується. Проте він не надає рекомендацій керівництву, як діяти. Навіть, якщо визначено конкретні технологічні вимоги до безпеки окремих систем, неправильне впровадження або робота будь-якого пристрою чи системи жодною мірою не поліпшить загальний рівень безпеки організації в цілому. Сфера застосування цього стандарту в інтересах встановлення відповідності нормативним вимогам досить обмежена. Однак існують виключення, зокрема у сфері процесингу платіжних карт, де певні технічні вимоги ISO/IEC 15408 зустрічаються, наприклад, в програмах перевірки на відповідність вимогам у сфері безпеки з боку платіжної системи MasterCard.

Серія ISO/IEC 270XX. Найбільш відомими і широко використовуваними стандартами управління ІБ, які свідчать про дотримання

організацією, що їх впровадила, нормативних актів і законодавства, є міжнародні стандарти серії ISO/IEC 270XX з управління ІБ. Ґрунтуючись на Британських стандартах 7799 (далі ISO/IEC 17799 і ISO/IEC 27001), стандарти серії ISO/IEC 270XX конкретно і чітко визначають, як ефективно впровадити систему менеджменту ІБ. Є кілька причин популярності цих стандартів, і насамперед, – це наявність чітких методів проведення аудиторських перевірок і, навіть, можливість сертифікації за ISO/IEC 27001. Ці стандарти допомагають відповісти на питання, як довести, що в організації забезпечений необхідний рівень безпеки і як переконати регулятивні органи, що все виконується правильно і належним чином. Стандарти охоплюють всі основні сфери вимог, які висуваються законодавством і нормативними актами, згаданими вище. Наріжним каменем відповідності стандартам є:

1) розуміння того, якими інформаційними активами володіє організація, і

2) впровадження необхідного рівня заходів контролю, заснованого на оцінці ризиків.

Стандарти ISO/IEC 17799, ISO/IEC 27001 – просто і доступно написані стандарти, надають корисні посібники щодо заходів контролю, які організація зможе впровадити. При цьому стандарти зрозумілі як фахівцям в галузі ІБ, так і керівництву, і допомагають подолати комунікаційний бар'єр між обома сторонами, забезпечивши тим самим розуміння керівництвом, що робиться і чому. Керівництво розглядається стандартом як ключова ланка при постановці цілей в сфері ІБ. Для того щоб, бути сертифікованою за цим стандартом, організація повинна також довести, що вона має процедури з ідентифікації законів і нормативних актів, які стосуються її з точки зору захисту інформації, а також має програму з дотримання цих нормативних вимог. За цих умов сертифікація по ISO/IEC 27001, якщо вона проведена належним чином, буде гарантувати, що організація реально дотримується усіх законодавчих та нормативних актів, які регулюють її діяльність. Додаток А стандарту ISO/IEC 27001 містить перелік заходів контролю, які повинні бути впроваджені в організації, яка має намір пройти сертифікацію (однак не всі заходи контролю із зазначеного переліку обов'язково мають бути впроваджені, якщо існує документально підтверджене рішення керівництва щодо цього питання, яке ґрунтується на оцінці ризиків). Багато компаній використовують цей стандарт як засіб самооцінки, оскільки методик з проведення оцінки безпеки недостатньо. Деякі компанії прагнуть пройти офіційний сертифікаційний аудит у акредитованих незалежних

аудиторських компаніях. Аналогічно BS 15000, описаному вище, компанії, що проводять сертифікаційний аудит, мають бути акредитовані по стандарту BS 7799 (частина 2) органом UKAS у Великій Британії. З огляду на перехід британських стандартів у статус міжнародних (ISO), акредитація також стала можливою через органи ISO. В опублікованому документі EA-7/3 Європейської комісії з акредитації (акредитація організацій, що займаються сертифікацією систем управління ІБ) перераховані основні вимоги до незалежності, кваліфікації та внутрішньої системи контролю якості таких організацій. Ці вимоги до якості процесу сертифікації та кваліфікації аудиторів обумовлені необхідністю довіри до результатів сертифікації. Сертифікація за стандартами також вимагає проведення регулярних аудиторських перевірок з метою забезпечення відповідності виконання вимог та належного функціонування процесу управління безпекою. Це скорочує розрив, який зараз існує між різними нормативними актами та законодавством, допомагає переконати регулюючі органи, що організація постійно дотримується вимог законодавства. Це також надає можливість співробітникам служби безпеки обґрунтувати необхідність фінансування програми управління безпекою, і не тільки сертифікаційного аудиту, а й усього комплексу заходів безпеки. У деяких країнах дотримання ISO/IEC 17799 та BS 7799:2 в окремих галузях економіки є обов'язковим (наприклад, в Японії та Україні). Контролюючі органи спираються на процес сертифікації за стандартом, як на достатню умову задоволення потреб галузі в Ззахисті інформації. Можливо, інші країни будуть наслідувати цей приклад завдяки тому, що стандарт широко використовується як інструмент впровадження безпеки, є зрозумілим, а механізми його виконання (сертифікація) – чітко встановленими.

Контрольні запитання

1. Яке призначення стандарту CobiT?
2. Якій склад бібліотеки інфраструктури інформаційних технологій ITIL?
3. Яке призначення стандарту ISO/IEC 15408?
4. Розкажить про особливості серії стандартів ISO/IEC 270XX.
5. Яке призначення стандарту ISO/IEC 17799?

10. ОСНОВИ УПРАВЛІННЯ КОМПЛЕКСНИМИ СИСТЕМАМИ ЗАХИСТУ ІНФОРМАЦІЇ

Теорія і практика забезпечення ефективності функціонування складних організованих систем, до яких, поза всякими сумнівами, відноситься і комплексні системи захисту інформації **(**КСЗІ), немислимі без застосування сучасних технологій управління.

Існує ряд визначень управління як процесу. По-перше, управління - елемент, функція організованих систем різної природи (біологічних, соціальних, технічних), що забезпечує збереження їх певної структури, підтримання режиму діяльності, реалізацію програми, цілей діяльності, по-друге, управління - процес здійснення інформаційних впливів на об'єкти управління для формування їх цілеспрямованого поведінки. Існують і інші визначення, що залежать від того, в якій сфері здійснюється управління. Разом з тим, де б не протікали процеси управління - при управлінні КСЗІ, в керуючих пристроях автоматичних систем, в нервовій системі людини, в економічних та інших структурах суспільства, вони підкоряються єдиним законам. Ці найбільш загальні закони управління системами різної природи вивчає наука про управління - кібернетика.

З позицій кібернетики управління визначається як функція системи управління, що забезпечує організацію цілеспрямованої діяльності керованої системи. Таким чином, сенс і мету управління в КСЗІ полягає в таких змінах організаційної структури сил і засобів захисту інформації (ЗІ), їх стану, методів і способів застосування, які забезпечують максимальну ефективність їх застосування для досягнення цілей захисту інформації.

Необхідно помститися, що управління можливо не у всіх системах (підсистемах), а тільки в тих, яким притаманний ряд властивостей:

- у збереженні системи як цілого вирішальна роль належить інформаційним зв'язкам. Без обміну інформацією між складовими елементами такі системи не можуть функціонувати. Ослаблення або втрата інформаційних зв'язків між елементами системи неминуче призводить до руйнування всіх інших зв'язків і, як наслідок, до розпаду (руйнування) самої системи;
- система здатна переходити в різні стани відповідно до керуючого (інформаційного) впливу;
- існує кілька допустимих ліній поведінки системи, з яких орган управління вибирає найбільш бажаних з тих чи інших критеріїв. Якщо можливості вибору кращої лінії поведінки немає, то управління втрачає сенс, тобто фактично відсутнє;

- процес функціонування системи відрізняється цілеспрямованістю. Якщо мета не визначена (або невідома), то, природно, управління стає безглуздим;
- система відкрита для зовнішнього впливу, тобто вплив зовнішніх факторів може мати найрізноманітніші природу і наслідки.

Системи, що володіють перерахованими особливостями, називаються системами з керуванням. До таких систем відноситься і система управління КСЗІ (СУ КСЗІ).

СУ КСЗІ мають ряд особливостей. Вони призначені для функціонування в конфліктних ситуаціях, так як ЗІ являє собою складний двосторонній процес між СУ КСЗІ та зловмисником. СУ КСЗІ може піддаватися різним видам впливу з боку зловмисника (злом, несанкціонований доступ, знищення інформації і т.і.), що, як правило, призводить до порушення функціонування як складових елементів, так і системи в цілому. Інформація, на основі якої виробляються керуючі впливи (проводиться вибір засобів, методів і способів ЗІ), відрізняється значною неповнотою, недостовірність і суперечливістю. Зловмисник постійно змінює засоби і методи впливу на систему.

Сутність управління КСЗІ полягає в цілеспрямованій діяльності керівництва підприємства, посадових осіб і служби ЗІ, спрямованої на досягнення цілей захисту інформації.

КСЗІ призначене для забезпечення ефективного вирішення наступних завдань:

1) запобігання несанкціонованому доступу до інформації та (або) передачі її особам, які не мають права на доступ до інформації;
2) своєчасного виявлення фактів несанкціонованого доступу до інформації;
3) попередження можливості несприятливих наслідків порушення порядку доступу до інформації;
4) недопущення впливу на технічні засоби обробки інформації, в результаті якого порушується їх функціонування;
5) негайного відновлення інформації, модифікованої або знищеної внаслідок несанкціонованого доступу до неї;
6) постійного контролю за забезпеченням рівня захищеності інформації.

Досягнення основних цілей ЗІ пов'язано з вирішенням цілого кола завдань, що становлять зміст управління КСЗІ. Основними з них є:

1) безперервне добування, збір, вивчення і аналіз даних обстановки;
2) підтримання системи в постійній готовності до виконання завдань ЗІ;
3) прийняття рішень по ЗІ;

4) доведення завдань до підлеглих;
5) планування заходів ЗІ;
6) організація і підтримання взаємодії структурних підрозділів підприємства;
7) всебічне забезпечення заходів ЗІ;
8) організація управління, під якою розуміється створення системи управління, забезпечення її ефективного функціонування (в тому числі і зашита системи управління від усіх видів впливу зловмисника), а також вдосконалення цієї системи з застосуванням, перш за все, нових інформаційних технологій;
9) управління підготовкою підрозділів ЗІ;
10) організація і здійснення контролю та допомоги підлеглим.

Необхідно відзначити, що серед зазначених завдань особливе місце займає прийняття рішення, яке є центральним моментом, ядром управління. Відповідно до теорії управління прийняття рішення в системах управління є прерогативою людини (керівника).

Суть прийняття рішення полягає в тому, що керівник (начальник) повинен творчо і відповідально визначити:
1) задум ЗІ;
2) завдання підрозділам і підлеглим;
3) основні питання взаємодії та забезпечення;
4) організацію управління.

Слід підкреслити особливу роль керівника при прийнятті рішення. В сучасних умовах прийняття рішення завжди здійснюється в умовах жорсткого дефіциту часу, браку вихідної інформації, а також в умовах ведення інформаційної війни. Щоб комплексно вирішувати всі завдання управління, необхідно створити стрункy систему управління, на науковій основі організувати роботу підлеглих, а також важливо застосовувати сучасні методи і засоби управлінської роботи, засновані на широкому використанні нових інформаційних і мережевих технологій.

Приймаючи рішення, керівник повинен враховувати об'єктивні закони управління, які виражають найбільш істотні зв'язки і відносини різних сторін управління між собою і з зовнішнім середовищем:
- залежність організаційних форм і методів управління КСЗІ від структури підприємства, матеріально-технічної бази і умов управління;
- єдність організаційно-методологічних основ на всіх рівнях управління КСЗІ;
- збереження пропорційності і оптимального співвідношення всіх елементів

системи управління;
- сумісність систем і засобів управління підлеглих підприємству організацій, а також взаємодіючих організацій;
- єдність і підпорядкованість критеріїв ефективності, які використовуються при управлінні КСЗІ;
- відповідність потрібного і наявного часу при вирішенні завдань управління;
- залежність ефективності вирішення завдань управління від обсягу інформації, що використовується і т.і.

На основі перерахованих законів управління формуються принципи управління, які в системі управління ЗІ виступають в якості основних вихідних положень управлінської діяльності, вироблених наукою і практикою, є засобом організації і регулювання цілеспрямованого впливу на КСЗІ, а також одночасно і власне функціонування керуючого суб'єкта.

Процес виявлення та обґрунтування принципів управління КСЗІ повинен відповідати наступним вимогам:
а) відображати найбільш істотні, головні, об'єктивно-необхідні закономірності, відносини і взаємозв'язки системи управління;
б) характеризувати лише стійкі закономірності, відносини і взаємозв'язки в системі управління;
в) охоплювати переважно такі закономірності, відносини і взаємозв'язки, які притаманні системі управління як цілісного організму, т. е. мають загальний, а не приватний характер;
г) відображати специфіку управління КСЗІ, його відмінність від інших видів управління.

Взаємозв'язки і взаємодії між принципами існують в рамках їх цілісної системи. Розкриття змісту і потенціалу будь-якого принципу управління можливо лише в рамках і з урахуванням його системних залежностей.

Система принципів:
а) загальні:
- принципи системності, об'єктивності, саморегулювання, зворотного зв'язку;
- принцип оптимальності, інформаційної достатності, еволюціонізму, ймовірності;
- принцип змагальності, провідної ланки, стимулювання;
б) приватні принципи, що застосовуються в різних підсистемах управління (наприклад, економічної):
- організаційно-технологічні: принципи єдиноначальності, поєднання, конкретності, розподілу праці;

- принципи ієрархії, єдності розпорядництва, одного начальника, делегування повноважень, діапазону управління.

Для прикладу наведемо кілька принципів, наприклад, системного підходу до управління КСЗІ.

Принцип мети. Цей основоположний принцип системного підходу орієнтує керівника на першочерговість аналізу (синтезу) цілей об'єкта, які повинні досягатися при його функціонуванні. Мета первинна, і для її досягнення повинна формуватися належним чином організована система. Системі може бути задано і кілька цілей. У цьому випадку повинен бути заданий принцип компромісу, наприклад, зазначенням послідовності досягнення цілей (спочатку більш важливих, а потім менш важливих). Мета обумовлює структуру і поведінку системи. У процесі функціонування мета системи може змінюватися. Відповідно до цього повинні змінюватися структура або (і) спосіб функціонування системи.

Принцип подвійності (відносності). Керований об'єкт повинен розглядатися і як система, і як підсистема системи більш високого рівня ієрархії (суперсистеми). Наприклад, об'єкт інформатизації, що складається з безлічі різних елементів (в тому числі і співробітників підприємства, що працюють на наявних на об'єкті засобах), є системою. У той же час даний об'єкт - елемент будь-якої автоматизованої системи, яка по відношенню до нього є суперсистемой. У свою чергу, об'єкт інформатизації є суперсистемой по відношенню до вхідних в його склад комп’ютерів.

Принцип цілісності. Система управління повинна розглядатися не як простий набір елементів, а як щось ціле, єдине.

Принцип складності. Управління як об'єкт є складною сукупністю різних елементів, що знаходяться в різноманітних зв'язках між собою і елементами навколишнього середовища. Кожному об'єкту притаманна нескінченна складність, невичерпність. Виходячи з цього, при вирішенні завдань управління необхідно розглядати об'єкт в спрощеному вигляді, але до такого рівня, на якому він ще зберігає свої істотні властивості. Важливо знайти компроміс між складністю і простотою, не загубивши при цьому істотних властивостей керованого об'єкта.

Принцип всебічності. Цей принцип вимагає враховувати при управлінні всі зв'язки в об'єкті і фактори, що впливають на його функціонування.

Принцип множинності. Даний принцип орієнтує керівника на те, що для повного опису результатів управлінського впливу на об'єкт необхідно

безліч моделей, кожна з яких описує його в будь-якому аспекті. Доведено, що задану точність опису можна забезпечити кінцевим безліччю моделей. Наприклад, автоматична система управління доступом описується функціональною схемою, принциповою схемою, монтажної схемою, тимчасовими діаграмами сигналів і рядом інших моделей.

Принцип динамізму. Принцип вказує на те, що управління необхідно розглядати з урахуванням динаміки функціонування об'єкта управління, т.к всі характеристики є функціями часу.

Принцип історизму. Цей принцип зобов'язує проводити дослідження минулого об'єкта, так як його функціонування в минулому і сьогоденні дозволяє розкрити закономірності і виявити тенденції його розвитку. Таким чином, даний принцип викликає необхідність розгляду об'єкта на всіх стадіях його життєвого циклу, починаючи з моменту створення і закінчуючи повною деградацією.

Принцип подібності. Даний принцип рекомендує здійснювати пошук аналогів управлінських ситуацій на предмет використання застосовувалися по ним управлінських впливів, що мали позитивні результати.

Комплексність:

- забезпечення захисту інформації від можливих загроз усіма доступними законними засобами, методами та заходами;
- забезпечення безпеки інформаційних ресурсів протягом всього їх життєвого циклу, на всіх технологічних етапах їх обробки (перетворення) і використання, у всіх режимах функціонування;
- здатність системи до розвитку та вдосконалення відповідно до змін умов функціонування.

Своєчасність. Заходи ЗІ мають попереджувальний характер. Вони передбачає постановку завдань по КЗІ на ранніх стадіях розробки системи на основі аналізу і прогнозування обстановки, погроз, а також розробку ефективних заходів попередження.

Безперервність. Вважається, що зловмисники тільки і шукають можливість, як би обійти захисні заходи, вдаючись для цього до легальних і нелегальних методів.

Активність. Заходи ЗІ проводяться з достатнім ступенем наполегливості, з широким використанням маневру силами і засобами захисту.

Законність. Цей принцип передбачає розробку КСЗІ на основі законодавства в галузі інформатизації та захисту інформації та інших

нормативних актів у цій галузі, із застосуванням всіх дозволених методів виявлення і припинення правопорушень.

Обґрунтованість. Використовувані можливості і засоби захисту повинні бути реалізованими на сучасному рівні розвитку науки і техніки, обґрунтованими з точки зору заданого рівня захисту та відповідають встановленим вимогам і нормам.

Економічна доцільність і порівнянність можливого збитку і витрат. У всіх випадках вартість системи повинна бути меншою за розмір можливого збитку.

Спеціалізація. Передбачається залучення до розробки та впровадження заходів і засобів захисту спеціалізованих організацій, що мають досвід практичної роботи та державну ліцензію на право надання послуг у цій галузі. Експлуатація технічних засобів і реалізація заходів ЗІ повинні здійснюватися професійно підготовленими фахівцями.

Взаємодія і координація. Цей принцип означає здійснення заходів забезпечення безпеки на основі чіткого взаємозв'язку відповідних підрозділів і служб, сторонніх спеціалізованих організацій у цій галузі, координації їх зусиль для досягнення поставлених цілей, а також співпраці з зацікавленими об'єднаннями та взаємодії з органами державного управління і правоохоронними органами.

Удосконалення. Удосконалення заходів і засобів захисту здійснюється на основі власного досвіду, появи нових технічних засобів з урахуванням змін в методах і засобах розвідки і промислового шпигунства, нормативно-технічних вимог, досягнутого вітчизняного і зарубіжного досвіду.

Централізація управління. Цей принцип передбачає функціонування системи ЗІ за єдиними правовим, організаційним, функціональним і методологічним принципам.

Контрольні запитання

1. У чому заключні особливості комплексних систем захисту інформації?
2. У чому заключна сутність управління комплексними системами захисту інформації?
3. Яке завдання комплексних систем захисту інформації?
4. Якій зміст управління комплексних систем захисту інформації?
5. Перерахуйте принципи системного підходу до управління комплексними системами захисту інформації?

11. СТРУКТУРА СИСТЕМИ УПРАВЛІННЯ КОМПЛЕКСНОЇ СИСТЕМИ ЗАХИСТУ ІНФОРМАЦІЇ

Система з управлінням незалежно від її фізичної природи має структуру, яка включає керуючий об'єкт, об'єкт (об'єкти) управління і канали зв'язку між ними:

- керуючий об'єкт (S) призначений для вироблення інформаційних впливів на основі обробки і відображення зібраної інформації. У ролі керуючих об'єктів можуть виступати об'єкти, здатні сприймати, зберігати, переробляти і видавати інформацію;
- об'єкт управління (О) забезпечує видачу інформації про свій стан і стан зовнішнього середовища, сприйняття інформаційних впливів від керуючих об'єктів і їх реалізацію;
- канали зв'язку служать для обміну інформацією між S і О. При цьому по каналу прямого зв'язку інформація передається від S до О, а по каналу зворотного зв'язку - в протилежному напрямку.

Сукупність, що включає S і канали зв'язку, будемо називати системою управління. Об'єкти управління в систему управління не входять, а процес реалізації ними управляють, в процес управління не включається.

Процес управління в такій системі здійснюється наступним чином. S по каналу зворотного зв'язку отримує інформацію про стан О і зовнішнього середовища (інформація стану). На основі цілей управління та інформації стану в S виробляється керуючий вплив (командна інформація); він визначає новий стан О, в яке він повинен перейти при наближенні системи до мети. Сукупність правил, за яким інформація стану перетворюється в командну інформацію, називається алгоритмом управління. Командна інформація передається по каналу прямого зв'язку. Сприйнявши інформацію, О виконує покладені на неї завдання. Так як система функціонує в деякому середовищі, що є джерелом активних і пасивних перешкод, а в роботі елементів системи можливі помилки, то новий стан О не завжди буде збігатися з бажаним. Тому поряд з виконанням певних дій О постійно передає S інформацію про свій стан.

Сукупність заходів з управління, які виконуються при зміні середовища, прийнято називати циклом управління. Цикли розрізняються за тривалістю і змістом. Цикл може бути перерваний. Виконуючи цикл за циклом, система поступово наближається до мети функціонування.

Шлях, по якому циркулює інформація між S і О, називається контуром управління. Розрізняють одноконтурні (з одним О) і багатоконтурні системи

управління, а також системи управління з замкнутим (при наявності каналів зворотного зв'язку) і розімкненим контуром управління.

До основних процесів управління КСЗІ відносяться:

1) збір інформації про стан елементів системи ЗІ і зовнішнього середовища;

2) обробка та оцінка існуючого стану системи ЗІ (її елементів) і зовнішнього середовища, порівняння і оцінка відповідності системи ЗІ цілям ЗІ, вироблення командної інформації (інформаційних впливів), що наближають КСЗІ до необхідного стану;

3) доведення інформаційних впливів до об'єктів управління.

Наведені процеси при реалізації управління КСЗІ можуть бути розділені на більш дрібні підпроцеси, завдання, процедури, операції, дії.

Основним елементом процесу управління є задача управління - технологічний модуль (одиниця) перетворення інформації, службовець для досягнення за заданий час конкретного результату. Групи завдань управління КСЗІ об'єднуються в функції управління.

Функція управління являє собою стійку сукупність завдань реалізації процесу управління (його частини) для досягнення приватних цілей управління, засновану на поділі управлінської праці в органах управління. Виділяються наступні основні управлінські функції: планування; оперативне керування; контроль; облік.

Планування - процес уточнення цілей системи і детальної програми їх досягнення. Змістом планування є розподіл ресурсів системи та визначення порядку їх використання при досягненні поставленої мети.

Оперативне керування - процес корекції поведінки системи при реалізації програми досягнення поставленої мети.

Контроль - процес перевірки інформації про елементи системи і зовнішнього середовища і оцінки відповідності стану системи її завданням.

Облік - процес вимірювання і реєстрації характеристик системи і зовнішнього середовища.

Завдання управління КСЗІ численні, різноманітні, залежать від безлічі факторів і не можуть розглядатися у відриві від конкретної системи ЗІ, конкретного підприємства і умов його функціонування. Завдання управління КСЗІ в загальному вигляді можуть бути класифіковані за різними ознаками. Наведемо деякі з них, які є важливими з точки зору зручності вивчення і формалізації задач.

1. В залежності від приналежності до ланки управління. Кожне завдання більш низького рівня ієрархії повинна бути узгоджене (за програмними

цілями, часом, ресурсами і т.і.) з відповідними завданнями вищого рівня.
2. В залежності від приналежності до функціональних підсистем управління, наприклад, контролю режиму секретності, пропускного режиму, охорони, розмежування доступу, кадрового забезпечення, нормативно-правові, криптографічного захисту, антивірусного захисту, матеріального і технічного забезпечення, обліку та збереження носіїв інформації та ін.
3. За періодичністю рішення: завдання довгострокові, поточні (квартальні, щомісячні, щодобові) і завдання з випадковою періодичністю.
4. За ступенем визначеності вихідної інформації: завдання детерміновані, імовірнісні і невизначені завдання управління.
5. З точки зору форми розумового процесу: завдання аналізу і синтезу.

Завдання аналізу полягають у визначенні значень показників ефективності функціонування системи при заданих структурі, характеристиках елементів і умов функціонування. Сутність завдань синтезу зводиться до визначення структури і (або) її характеристик при заданих обмеженнях на ресурси і вимогах (цілях) до її функціонування.
6. За характером перетворення інформації: завдання, що класифікуються за формою представлення даних, за змістом, але розташуванню в просторі або в часі. Якщо в задачі переважає змістовна обробка, її називають розрахункової, якщо інші види перетворень, - інформаційної. Розрахункові завдання класифікуються як завдання узгодження дій, змагальні, маршрутизації, заміни обладнання, розподілу ресурсів, масового обслуговування, пошуку, упорядкування та ін. До інформаційних завдань відносяться завдання обліку, узагальнення, систематизації, передачі інформації, документування, зберігання і т. п.

Стиль управління - реально використовувана система ефективних способів, засобів, форм і методів повсякденного функціонування посадових осіб і органів управління підприємства в цілому заснована на відповідних принципах і забезпечує раціональне ведення управлінських справ. Стиль - один з чинників раціоналізації управління, узгоджена взаємодія управлінських елементів і людського потенціалу; заснована на синтезі соціальних, організаційних, нормативних, інформаційних та технічних параметрів управління.

Стиль управління повинен складатися з таких необхідних для нього елементів, як:
- цільові, функціональні і організаційні характеристики органів управління, які визначають їх місце і правовий статус в ієрархії керуючої системи

підприємства;
- юридично закріплені і відповідно практично використовувані форми, методи і процедури управлінської діяльності органів управління та посадових осіб підприємства;
- реально притаманні загальнокультурні, професійні та особистісні якості посадових осіб, за допомогою яких формуються соціально-психологічні механізми управління.

Властивості стилю управління створюються акцентом в названих елементах і комбінаціями з них. Виходячи з цього виділено кілька різновидів стилю управління:
- директивний (адміністративно-директивний, автократичний): наявність надмірної централізації влади, єдиноначальності, самовладного рішення великих і дрібних питань, свідомого обмеження контактів з підлеглими;
- демократичний (колегіальний, кооперативний): надання самостійності відповідно до кваліфікації, прийняття рішень за участю підлеглих, повагу до людей, турбота про їхні потреби;
- ліберальний: відсутність розмаху в діяльності, безініціативність і постійне очікування вказівок зверху, небажання прийняти на себе відповідальність за рішення і їх наслідки, коли вони несприятливі.

У чистому вигляді жоден стиль управління не виявляється. Найчастіше має місце поєднання, змішання стилів при явному переважанні якого-небудь одного. Властивість стилю управління, що складається в його системі і підсистемах, безпосередньо залежить від якостей осіб, зайнятих в управлінських процесах. Найбільш доцільним, продуктивним і орієнтованим на тривалу перспективу є демократичний стиль управління. Саме він дозволяє стабілізувати управлінські процеси і за допомогою них налагодити раціональне і ефективне функціонування системи і її розвиток.

Під технологією управління КСЗІ розуміється організація діяльності керівництва і посадових осіб підприємства щодо забезпечення комплексного захисту інформації.

Технологія управління КСЗІ повинна забезпечувати:
- точну і своєчасну реалізацію політики інформаційної безпеки підприємства;
- гнучкість застосування положень політики інформаційної безпеки (врахування особливостей функціонування різних підсистем підприємства);
- мінімізацію витрат на реалізацію керуючих впливів;
- відповідність прийнятих заходів сучасному рівню розвитку інформаційних технологій.

Для реалізації технології управління КСЗІ підприємства необхідно:
- наявність системи взаємопов'язаних нормативно-методичних і організаційно-розпорядчих документів;
- чіткий розподіл функцій і визначення порядку взаємодії підрозділів підприємства при вирішенні питань ЗІ, зафіксовані в організаційно-розпорядчих документах;
- наявність підрозділу захисту інформації, щ наділенийо необхідними повноваженнями і безпосередньо відповідає за формування і реалізацію єдиної політики інформаційної безпеки підприємства, що здійснює контроль і координацію дій інших структурних підрозділів підприємства з питань ЗІ на всіх етапах її життєвого циклу.

Технологія управління КСЗІ повинна передбачати взаємодію і реалізацію функцій по ЗІ підрозділами і посадовими особами підприємства:
- керівництвом підприємства, які приймають стратегічні рішення з питань ЗІ і встановлює основні документи, що регламентують порядок функціонування та розвитку КСЗІ, що забезпечує безпечну обробку і використання інформації, що захищається;
- підрозділом захисту інформації;
- підрозділом, який веде облік і зберігання носіїв інформації, що захищається;
- підрозділом, який відповідає за розробку і / або придбання технічних засобів обробки інформації, що захищається;
- підрозділами, відповідають за забезпечення нормальної роботи обчислювальних засобів, загальних (системних) програмних засобів, засобів телекомунікації;
- підрозділом, який відповідає за проведення перевірок підрозділів підприємства з питань дотримання технології захисту;
- основних підрозділів підприємства, які вирішують завдання з використанням інформації, що захищається.

Реалізація технології ЗІ на конкретному підприємстві вимагає адаптації до його структурно-функціональної організації. Реалізація підрозділами і персоналом підприємства функцій по ЗІ здійснюється на основі і відповідно до розроблених та затверджених керівництвом підприємства організаційно-розпорядчими документами: інструкціями, правилами, посадовими обов'язками, положеннями і т.і.

Контрольні запитання

1. Перерахуйте елементи структури системи з управлінням.
2. Дайте визначення об'єктам управління.
3. Перерахуйте основні процеси управління.
4. За якими признаками здійснюється класифікація завдань управління комплексними системами захисту інформації?
5. Перерахуйте основні процеси технології управління комплексними системами захисту інформації.

12. ПЛАНУВАННЯ ПРОГРАМИ АУДИТУ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Програма аудиту інформаційної безпеки (ІБ) включає заходи, які необхідні для планування та організації певної кількості аудитів інформаційної безпеки та, наприклад, самооцінки інформаційної безпеки, їх контролю, аналізу та вдосконалення, а також надання їм ресурсів, необхідних для ефективного та результативного проведення аудитів інформаційної безпеки та самооцінок інформаційної безпеки в задані терміни.

Програма аудиту інформаційної безпеки розробляється самою організацією. В цілому організація може розробити кілька програм аудиту інформаційної безпеки. У будь-якому випадку список процесів в рамках програми виглядає наступним чином:

- розподіл повноважень за програмою аудиту інформаційної безпеки;
- планування програми аудиту інформаційної безпеки та самооцінка інформаційної безпеки;
- виконання програми аудиту інформаційної безпеки та заходів щодо проведення аудиту інформаційної безпеки та самооцінки інформаційної безпеки;
- контроль та аналіз програми аудиту інформаційної безпеки;
- удосконалення програми аудиту інформаційної безпеки.

Відповідно до визначених ролей з розробки та управління програмою аудиту інформаційної безпеки керівництво організації розподіляє повноваження і покладає відповідальність за розробку і управління програмою аудиту інформаційної безпеки на одну або декількох осіб, які мають уявлення про принципи аудиту інформаційної безпеки, компетентність аудиторів, зміст етапів аудиту інформаційної безпеки, а також володіють знаннями про інформаційну безпеку.

Особи, відповідальні за програму аудиту інформаційної безпеки, повинні:

– планувати, впроваджувати, контролювати, аналізувати та вдосконалювати програму аудиту інформаційної безпеки;

– визначити потребу програми аудиту інформаційної безпеки в ресурсах і полегшити прийняття рішень щодо забезпечення програми необхідними ресурсами.

Програма аудиту може включати, наприклад, наступні види аудиту безпеки організації:

а) внутрішній аудит інформаційної безпеки організації, що проводиться

щорічно;
б) самооцінка інформаційної безпеки, що проводиться кожні шість місяців;
в) сертифікаційні аудити та інспекційні аудити, що проводяться органом з сертифікації систем безпеки в якості третьої сторони в період часу, який узгоджений між органом сертифікації та замовником.

Програма аудиту інформаційної безпеки також включає планування, надання ресурсів, розробку процедур проведення аудитів інформаційної безпеки в рамках програми. Основною метою програми аудиту інформаційної безпеки є вдосконалення системи інформаційної безпеки організації. При цьому можуть бути вирішені і інші цілі, наприклад, оцінка відповідності інформаційної безпеки організації встановленим критеріям інформаційної безпеки, підвищення довіри до організації. На сферу застосування програми аудиту інформаційної безпеки впливають розмір і складність структури організації, обсяг кожного аудиту інформаційної безпеки і самооцінки інформаційної безпеки, частота і тривалість аудитів інформаційної безпеки і самооцінок інформаційної безпеки.

Планування програми аудиту інформаційної безпеки повинно включати визначення цілей, обсягу програми, а також необхідних фінансових, інфраструктурних і людських ресурсів для її реалізації. При визначенні можливості проведення аудиту слід враховувати наступні фактори:
– достатність і доступність необхідної інформації для планування аудиту інформаційної безпеки;
– наявність часу і необхідних ресурсів;
– готовність до співпраці з боку організації, що перевіряється.

При неможливості проведення аудиту необхідно запропонувати замовнику альтернативне рішення, засноване на консультаціях з організацією, що перевіряється, наприклад, перенесення термінів проведення аудиту інформаційної безпеки, залучення іншої аудиторської організації для проведення аудиту інформаційної безпеки. Періодичність перевірок залежить від можливостей і ресурсів організації і встановлюється як компроміс між необхідністю перевірок і витратами на їх проведення.

Залежно від можливостей і ресурсів організації початкова сфера застосування програми аудиту інформаційної безпеки може обмежуватися тими процесами системи інформаційної безпеки організації, яким керівництво відвело найвищий пріоритет. Надалі початкова сфера застосування програми аудиту інформаційної безпеки може бути розширена.

Як визначити найбільш критичні бізнес-процеси, на які процеси інформаційної безпеки звернути особливу увагу при проведенні аудиту інформаційної безпеки або самооцінки інформаційної безпеки, на які процеси в першу чергу слід орієнтуватися програмі аудиту інформаційної безпеки? Такі питання можна вирішити, якщо на етапі планування програми аудиту інформаційної безпеки застосувати ризик-орієнтований підхід для виявлення критичних бізнес-процесів і проблем інформаційної безпеки.

Будь-яка організація при здійсненні своєї діяльності схильна до ризиків, які так чи інакше впливають на специфіку ведення бізнес-процесів, а також можуть негативно позначитися як на фінансових показниках, так і на здатності підприємств продовжувати справу. При цьому частина ризиків, обумовлених незначними наслідками їх реалізації, може прийматися «як є», для інших розробляються і впроваджуються коригувальні заходи. Зокрема, можна приймати на себе ризики, які тягнуть за собою невеликі негативні наслідки і ймовірність реалізації яких малоймовірна.

Згідно з міжнародним стандартом IS0/IEC 17799 інформаційна безпека - це захист інформації від безлічі різних ризиків з метою забезпечення безперервності бізнесу, мінімізації бізнес-ризиків, підвищення віддачі від інвестицій і розширення можливостей для бізнесу. Очевидно, що одні бізнес-процеси є найбільш значущими для організації, інші процеси менш критичні. Причому оцінка ступеня критичності може базуватися не тільки на фінансових показниках, а й на поточних пріоритетах бізнесу, кон'юнктурі та вимогах ринку, вимогах законодавства та ринкових регуляторів, рівні корпоративної культури тощо.

Відповідно, плануючи аудит питань інформаційної безпеки, необхідно в першу чергу виявити найбільш критичні сфери діяльності організацій в рамках застосовності до питань інформаційної безпеки. Немає абсолютно ніякої необхідності проводити детальний аналіз питань, які є незначними для бізнесу. Тому при плануванні аудиту також необхідно враховувати можливість зміни критичності процесів з плином часу, наприклад, при закритті операційного дня банку, відправці платежів, формуванні річних звітів і т.і.

Люди (співробітники, клієнти, постачальники), процеси (внутрішні і зовнішні, політики і процедури) і технології є трьома ключовими аспектами інформаційної безпеки. Тому навіть підприємства, що працюють в одному сегменті ринку, мають схожі організаційно-правові структури, способи ведення бізнесу і бізнес-процеси в силу унікальності рівня корпоративного

управління, технологій і персоналу, мають свої специфічні ризики. Кожна організація повинна розробити власну програму аудиту інформаційної безпеки. При цьому при детальному плануванні аудиту необхідно мати повне уявлення про організацію, що перевіряється, тобто виявлення найбільш значущих сегментів бізнесу і напрямків пріоритетного розвитку, аналіз фінансових показників за основними напрямками діяльності, організаційної структури, використовуваних технологічних рішень, а також інших аспектів, які можуть істотно вплинути на рівень інформаційної безпеки організацій.

Можливо перевірити параметри безпеки для всіх баз даних та операційних систем у організації, що перевіряється, але чи потрібно це? Через обмеженість ресурсів (часових, людських і фінансових) рекомендується обмежуватися найбільш значущими для бізнесу областями, для яких вже були визначені конкретні системи і процедури, що підлягають перегляду. При проведенні такого планування рекомендується використовувати комбінації підходів «зверху-вниз» і «знизу-вгору». Підхід «низхідного аналізу» заснований на тому, що оцінка ризиків інформаційної безпеки здійснюється на основі аналізу критичності бізнес-процесів.

І тільки на основі цього аналізу для обраних процесів проводиться аналіз ризиків і результатів контролю, пов'язаних з використанням конкретних додатків, баз даних, операційних систем, конфігурацій мережевого обладнання та інших питань інформаційної безпеки конкретних критичних бізнес-процесів.

Підхід «аналізу знизу вгору» використовується в зворотному випадку, тобто коли проблема відома або виявлена, і необхідно зрозуміти, на які бізнес-процеси і сегменти бізнесу зачіпається ця проблема і, відповідно, потім зробити висновок про критичність виявленого недоліку.

Існує розділення IT-залежного і ручного управління:

- контроль за реалізацією бізнес-проектів;
- звірка рахунків;
- перевірка та узгодження угод.

Існує розділення програмних елементів управління:

- цілісність;
- авторизація;
- поділ влади;
- верифікація.

Існує розділення елементів керування IT:

- розробка програм;

- управління змінами;
- контроль доступу;
- відновлення IT після збоїв.

Як приклад розглянемо процес управління оновленнями для операційної системи. Той факт, що системний адміністратор вчасно не встановив патч, не є підтвердженням існування проблеми для бізнесу, поки ця операційна система не буде використовуватися для підтримки критичних бізнес-процесів або не може використовуватися як платформа для отримання доступу до критичних систем (підхід «аналіз знизу вгору»). І навпаки, виділяючи критичні процеси, а також системи та додатки, що підтримують IT як частину аудиту інформаційної безпеки, необхідно також забезпечити, щоб усі критичні оновлення встановлювалися своєчасно та належним чином для всіх систем, які підпадають під сферу аудиту (підхід «аналіз зверху вниз»).

Використання цих двох підходів в комплексі допомагає співвіднести конкретні питання інформаційної безпеки (абстрактні точки зору керівництва бізнесу і бізнес-користувачів) з конкретними бізнес-процесами і цілями організації, і передати виявлені проблеми простою і зрозумілою для керівництва мовою, тобто показати чітку залежність бізнес-ризиків і ризиків інформаційної безпеки.

Крім специфічного контролю IT та інформаційної безпеки, існує контроль корпоративного рівня, який формує як організаційну, так і правову основу забезпечення інформаційної безпеки організації. Даний вид контролю включає в себе організацію і управління службою інформаційної безпеки, розробку і впровадження політик інформаційної безпеки, проведення незалежних внутрішніх і зовнішніх аудитів, навчання співробітників інформаційної безпеки і користувачів системи основним аспектам інформаційної безпеки, управління безперервністю бізнесу і т.д. Контроль корпоративного рівня в силу своєї специфіки діє на всій території організації і робить істотний вплив на загальну картину ризиків інформаційної безпеки і поряд з конкретними питаннями безпеки конкретних систем завжди враховується при проведенні аудиту інформаційної безпеки.

Плануючи програму аудиту інформаційної безпеки, необхідно також розглянути та оцінити технології, які можуть підтримувати автоматизовані інструменти та навчання.

Типи автоматизованих інструментів, які можуть знадобитися, включають графічні засоби представлення результатів оцінки, інструменти

аналізу даних та бази даних, а також інструменти збору даних.

Контрольні запитання

1. Перерахуйте заходи, які необхідні для планування та організації аудитів інформаційної безпеки.
2. Хто призначає осіб, які відповідальні за програму аудиту?
3. Які існують види аудиту безпеки організаці?
4. Хто складає Програма аудиту інформаційної безпеки?
5. Наведить приклад критичних бізнес-процесів.

13. ФУНКЦІОНУВАННЯ ГРУП РЕАГУВАННЯ НА ІНЦИДЕНТИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

13.1. Організація груп CERT/CSIRT

Група CERT/CC (CERT Coordination Center), що виникла в 1988 році як Computer Security Incident Response Team (група реагування на інциденти, пов'язані з комп'ютерною безпекою), функціонує у складі Інституту розробки програмного забезпечення при Університеті Карнегі – Меллона (Software Engineering Institute, Carnegie Mellon University) і фінансується урядом США. Починався цей проект з ініціативи студентів та викладачів університету (у відповідь на перше глобальне поширення шкідливого ПЗ під назвою «Хробак Моріса») і дуже швидко перетворився спочатку в проект національного, а незабаром і міжнародного масштабу. Окрім проведення незалежних досліджень та виконання різноманітних завдань щодо забезпечення безпеки глобальної інформаційної інфраструктури, ця організація здійснює централізований збір відомостей про всі уразливості в різних інформаційних системах і підтримку бази знань про такі уразливості в актуальному стані. Відомості про щойно виявлені уразливості, шкідливі програми і способи порушення інформаційної безпеки розсилаються електронною поштою у вигляді бюлетеню. Передплатниками цього бюлетеню є більше 161000 фахівців у всьому світі. CERT/CC здійснює постійну дослідницьку роботу щодо:

- визначення характеру можливих наслідків використання виявлених уразливостей і вірусів;
- аналізу наявних засобів використання уразливостей;
- аналізу того, наскільки активно використовуються уразливості і наскільки широко поширені віруси;
- взаємодії з постачальниками інформаційних систем з метою більш глибокого аналізу виявлення уразливостей.

На основі проведеного аналізу CERT/CC розробляє заходи щодо усунення уразливостей і рекомендації щодо зменшення негативних наслідків. За результатами цієї роботи всім передплатникам розсилається інформація про загрози інформаційній безпеці і можливі способи їх усунення. Також на основі цих даних формується спеціальна довідкова й технічна документація, проводиться подальша дослідницька і методична робота. Зокрема, CERT/CC підтримує програму безпечної розробки ПЗ («Secure Coding»), що ґрунтується на тому, що більша частина уразливостей

виникає внаслідок відносно невеликого числа помилок у програмному коді інформаційних систем. Таким чином, CERT/CC на основі накопичених результатів аналізу уразливостей проводить цілеспрямовану роботу з виявлення типових програмних помилок, вироблення стандартів безпечного програмування та поширення цієї інформації серед розробників ПЗ. Крім основної інформаційної роботи з уразливостями, CERT/CC також займається супутніми видами діяльності:

- організацією навчальних курсів з різних напрямків (мережевої безпеки, управління інформаційними ризиками, організації роботи груп реагування);
- сертифікацією фахівців з реагування на інциденти у сфері інформаційної безпеки;
- підтримкою фундаментальних наукових досліджень у різних галузях інформаційної безпеки, таких як методи розробки безпечних додатків, виявлення уразливостей, аналіз шпигунського ПЗ, вирішення питань безпеки як складова частина процесу розробки тощо ;
- сприяння розвитку локальних (національних і корпоративних) груп реагування на інциденти.

З огляду на те, що CERT – торгова марка, захищена законодавством США, у світовій практиці прийнято вживати для позначення груп реагування на інциденти назву CERT/CSIRT (Computer Emergency Response Team / Computer Security Incident Response Team). Таким чином, функціонування груп CERT/CSIRT можуть надати такі переваги своїм клієнтам:

- централізовану координацію питань, пов’язаних з інформаційною безпекою всередині організації;
- спеціалізовану та централізовану систему обробки повідомлень про ІІБ і своєчасне реагування на них;
- надання експертизи і підтримки в процесі відновлення після впливу ІІБ;
- забезпечення юридичної допомоги та взаємодії з відповідними правоохоронними органами і службами з метою ефективного розслідування ІІБ (зокрема, підтримку у судових процесах);
- відслідковування як методів і способів порушення інформаційної безпеки, так і сучасних методів та засобів захисту інформаційних систем;
- стимулювання партнерів і клієнтів до спільної взаємодії та розвитку у сфері забезпечення інформаційної безпеки;
- збирання статистики, яка буде корисною для розробки, впровадження та удосконалення систем захисту інформації тощо.

На сьогодні у світі функціонує розвинута мережа структур швидкого

реагування на інциденти, що загрожують безпеці інформаційних ресурсів, які мають назви CERT або CSIRT. Координацію діяльності таких структур на міжнародному рівні здійснює міжнародна організація

Форум груп реагування на інциденти і забезпечення безпеки (Forum of Incident Response and Security Teams, FIRST), яка об'єднує зусилля різних груп реагування на інциденти ІБ. На сайті FIRST (http://www.first.org) можна знайти повний список її учасників. У переліку членів FIRST до липня 2009 року не було жодної організації з України (першою стала група CERT-UA, про яку йтиметься далі).

Розглянемо особливості функціонування структур швидкого реагування на ІІБ в деяких державах.

US-CERT. Група готовності до надзвичайних ситуацій в інформаційних системах (United States Computer Emergency Readiness Team, US-CERT) є центральним цілодобово функціонуючим органом, що відповідає за взаємодію з урядовими структурами (як федеральними, так і місцевими), а також іншими суб'єктами з питань захисту інформації. Її основним завданням є збір і поширення інформації з метою реагування на інциденти, підвищення рівня скоординованості дій, зниження рівня уразливості інформаційних систем.

CERT/CSIRT. До складу європейської мережі CERT/CSIRT входять п'ять підрозділів:

1) відділ поточної діяльності (Operations Branch). Відповідає за обробку одержуваної інформації про інциденти, забезпечує реагування на інциденти, поширює необхідну інформацію, а також забезпечує аналіз різних даних з метою підвищення якості оцінки відомих або нових загроз для критично важливих елементів національної інфраструктури (зокрема, аналіз мережевої інфраструктури, аналіз шкідливого ПЗ та ін.);

2) відділ ситуаційної поінформованості (Situational Awareness Branch). Відповідає за комплексний аналіз мережевої активності (тенденцій і характеру змін завантаження магістральних мереж) й інформування федеральних структур з метою підвищення рівня їх захищеності. Також забезпечує підтримку у вирішенні інцидентів;

3) слідчий відділ (Law Enforcement and Intelligence Branch). Забезпечує взаємодію з правоохоронними органами при виявленні і розслідуванні протиправних дій;

4) відділ перспективного розвитку (Future Operation Branch). Відповідає за розробку перспективних планів, процедур, регламентів, що забезпечують

роботу US-CERT з реагування на інциденти;
5) відділ підтримки (Mission Support Branch). Забезпечує підтримку засобів комунікації, необхідних для роботи US-CERT, включаючи підтримку веб - сайту, а також відповідає за адміністративну підтримку, безпеку персоналу, постачання та інші допоміжні функції.

Проект CERT-UA. З метою підвищення рівня координації діяльності державних органів щодо виявлення, оцінки і прогнозування загроз ІБ, запобігання таким загрозам та забезпечення ліквідації їх наслідків, здійснення міжнародного співробітництва у цій сфері на базі Державної служби спеціального зв'язку та захисту інформації запроваджено проект CERT-UA (Computer Emergency Response Team of Ukraine). Завданням CERT-UA є координація діяльності органів державної влади, органів місцевого самоврядування, військових формувань, підприємств, установ і організацій незалежно від форм власності з питань запобігання, виявлення та усунення наслідків несанкціонованих дій щодо державних інформаційних ресурсів в інформаційних, телекомунікаційних та інформаційно телекомунікаційних системах. CERT-UA надає консультативну та методичну допомогу суб'єктам координації у вирішенні питань захисту державних інформаційних ресурсів в ІТС. Крім того, CERT-UA:
1) постійно відслідковує світові та українські події у сфері безпеки інформації в ІТС, а також вивчає найбільш важливі проблеми у цій сфері;
2) надає рекомендації щодо методик протидії сучасним видам атак, побудови систем захисту ІТС, використання найбільш ефективних засобів захисту інформації;
3) взаємодіє з правоохоронними органами України;
4) взаємодіє з іноземними та міжнародними організаціями реагування на несанкціоновані дії;
5) здійснює накопичення та аналіз даних про вчинення та/або спроби вчинення несанкціонованих дій щодо державних інформаційних ресурсів в ІТС.

Разом з тим, варто вказати на такі проблеми УІІБ в Україні:
1) CERT-UA обслуговує лише органи державної влади (не працює з пересічними громадянами);
2) на сьогодні Україна входить до вісімки країн Європи (разом з Мальтою, Ісландією, Словаччиною, Болгарією, Грузією, Словенією та Литвою), які мають на своїй території тільки по одному центру CSIRT/CERT. Для

найбільшої за територією європейської країни, яка до того ж щорічно готує значну кількість фахівців у галузі інформаційної безпеки, це критично мало;
3) в Україні сьогодні відсутній єдиний орган або організація, яка б взяла на себе роль координаційного центра з питань реагування на ІІБ всередині країни та з аналогічними закордонними установами. Фактично функції CSIRT/CERT виконують спеціалізовані підрозділи більшості Інтернет-провайдерів та великих ІТ-компаній України, але працюють вони здебільшого у власних інтересах та/або в інтересах своїх клієнтів.
4) у нашій державі відсутня статистика інцидентів ІБ, як наслідок ускладнюється процес аналізу загроз, розробки методів і засобів захисту інформації;
5) відсутні вітчизняні методики та рекомендації щодо УІІБ, які були б корисними як підрозділам, що виконують функції CSIRT/CERT, так і новоствореним групам (центрам).

13.2. Етапи створення груп CERT/CSIRT

З огляду на міжнародний та зарубіжний досвід формування груп CERT/CSIRT можна виділити такі етапи їх створення.
1) визначення середовища функціонування та потенційних клієнтів. Для визначення середовища функціонування і, як наслідок, потенційних клієнтів майбутньої групи CERT/CSIRT, необхідно, перш за все, проаналізувати галузі народного господарства, у яких актуально їх впроваджувати.
2) визначення переліку базових та додаткових послуг. На цьому етапі формується множина послуг (сервісів), які будуть надаватися клієнтам
3) визначення методів взаємодії з клієнтами. За результатами вивчення потреб потенційних клієнтів груп CERT/CSIRT кожна група виробляє свою індивідуальну стратегію взаємодії з ними. Для вивчення потреб клієнтів можуть бути використані методи SWOT- та PEST аналізу. Зазвичай, для обміну інформацією з клієнтами CERT/CSIRT використовують кілька методів одночасно, серед яких застосування: сайтів, форумів, порталів, електронних листів, SMS-повідомлень, паперових листів тощо.
4) протокол про наміри. Протокол про наміри повинен містити чіткий опис основних функцій та сервісів, які будуть надаватися CERT/CSIRT клієнтам (перелік яких теж уточнюється у цьому документі).
5) визначення фінансової моделі. Фінансову модель необхідно подати як синтез моделей витрат та прибутків. Перша модель залежить від графіку роботи та кількості найманого персоналу, а друга може базуватись на

використанні ресурсів компанії (у випадку внутрішньої CERT/CSIRT), членських внесках чи різного роду субсидіях (або певній їх комбінації).

6) визначення організаційної структури. Організаційна структура CERT/CSIRT залежить, насамперед, від типу створюваної групи і може складати з наступнх працівників:

- генеральний менеджер;
- технічний менеджер;
- офіс-менеджер;
- бухгалтер;
- юридичний консультант;
- консультант по комунікаціям;
- техніки.

Згідно з міжнародними рекомендаціями до складу внутрішньої групи рекомендується включати представників таких підрозділів організації:

- служби інформаційної безпеки;
- служби IT;
- служби персоналу;
- юридичної служби;
- бізнес менеджерів профільних підрозділів;
- зовнішніх експертів.

Ще одним варіантом може бути застосування добровільної моделі – коли для створення CERT/CSIRT на добровільній основі об'єднуються незалежні експерти з метою обміну досвідом і взаємної підтримки. Така модель немає чіткої структури і ґрунтується виключно на мотивації учасників.

13.3. Сервіси, що надаються групами реагування на інциденти

Сервісами CERT/CSIRT називають сукупність послуг з розслідування ІІБ та суміжних процесів, які надає група реагування на інциденти для своїх клієнтів в залежності від типу CERT/CSIRT, її структурної та фінансової моделі і цільової аудиторії. Здебільшого, новостворена група CERT/CSIRT надає лише базові сервіси (до яких відносяться сервіси реагування та профілактики), а з часом, в залежності від потреб клієнтів, загроз та змін на ринку ІТС, перелік послуг може розширюватися та уточнюватися. Базові сервіси:

1) Сервіси реагування. Сервіси реагування – це послуги, розроблені для відповіді на клієнтські запити про допомогу, створення звітів про інциденти,

реагування на атаки та загрози інформаційній безпеці. Деякі з цих сервісів можуть надаватися третіми сторонами або шляхом перегляду результатів моніторингу чи повідомлень від систем виявлення та попередження вторгнень.

1.1) Повідомлення та попередження. Цей сервіс передбачає поширення інформації про атаки зловмисників, спроби вторгнення, уразливості, нові віруси та інше шкідливе ПЗ і типові рекомендації клієнтам про заходи, які необхідно вжити у випадку впливу зазначених чинників. Повідомлення про попередження та відповідні рекомендації відправляються як реагування на певну проблему клієнта з метою їх інформування про можливі загрози і надання методики для усунення результатів негативного впливу й відновлення уражених систем.

1.2) Обробка інцидентів. Передбачає отримання запитів про вирішення інцидентів, їх категоризацію, визначення пріоритетів, реагування на ці запити, формування звітів та аналіз інцидентів. Такими заходами є:

- захист ІКС та мереж, які були вражені зловмисником або знаходяться під загрозою нападу;

- відпрацювання рішення та стратегії зменшення ризику відповідно до рекомендацій, наданих попереднім сервісом;

- ідентифікація дій зловмисників в інших сегментах ІКС;

- виправлення помилок та відновлення нормального функціонування системи;

- фільтрація мережевого трафіку та постійне вдосконалення власних стратегій. Після того, як впроваджені різного роду заходи щодо обробки ІІБ, цей сервіс класифікується за типом шкідливої дії та типом наданої допомоги і відображається в таких сервісах.

1.3) Аналіз інцидентів. Існує багато рівнів та підрівнів аналізу інцидентів, який здійснюється шляхом оцінки усієї доступної інформації і додаткових доказів або артефактів, пов’язаних з певним ІІБ. Основною метою аналізу є ідентифікація масштабів інцидентів, обсягу нанесеної ним шкоди, природи інцидентів, а також визначення стратегії їх нейтралізації та відновлення систем. Група CERT/CSIRT може використовувати результати аналізу уразливостей для того, щоб виконати якомога глибший та своєчасний аналіз інциденту, що виник; порівняти його з сучасними тенденціями, шаблонами, виявивши можливі взаємозв’язки з іншими інцидентами та сліди зловмисника. Цей сервіс має два підрівні, які можуть бути реалізовані як частина аналізу інциденту чи як окремі сервіси:

1.3.1) Збір правової інформації – збір, збереження, документування та аналіз фактів про ІКС, що знаходяться в зоні ризику, для визначення змін, які відбуваються в ІКС і підвищення ймовірності прийняття правильного рішення щодо розслідування. Збір інформації має проводитись таким чином, щоб задокументувати весь ланцюг доказів, які можуть бути використані у суді відповідно до національної правової системи. Важливими завданнями цього сервісу є створення побітової копії жорсткого диску враженої системи, виявлення змін у системі (нові програми, файли, сервіси користувачів) перегляд активних процесів та відкритих портів, пошук активного та пасивного ПЗ.

1.3.2) Відслідковування – полягає у стеженні за джерелом проникнення зловмисника та визначенні систем, до яких він має доступ. Передбачає трасування шляхів зловмисника до враженої системи, ідентифікацію засобів зловмисника та інших систем, до яких зловмисник міг отримати доступ або які він міг використовувати для реалізації несанкціонованого доступу до ураженої системи. Часто реалізація цього сервісу відбувається в умовах активної взаємодії з провайдерами телекомунікаційних послуг, правоохоронними та іншими компетентними органами, хоча не виключається і його реалізація самостійно групою CERT/CSIRT.

Крім того, у цій категорії виділяють такі сервіси:

- аналіз уразливостей;
- координація реагування на уразливості;
- обробка уразливостей.

2) Профілактичні сервіси. Використовуються для покращення інфраструктури клієнтів і процесів, що забезпечує їх захист до того, як відбудеться чи буде зафіксовано ІІБ, тобто, головною метою таких сервісів є уникнення інцидентів, зниження негативного впливу, а також відслідковування факту їх виникнення.

2.1) Інформування. Передбачає опублікування інформації про вторгнення, попередження про типові уразливості, рекомендації щодо застосування сучасних ефективних методів та засобів захисту інформації. Цей сервіс інформує, насамперед, клієнтів про тенденції розвитку інструментарію зловмисників, а також про засоби протидії їм, тобто допомагає клієнтам захистити свої інформаційні ресурси від актуальних проблем до того, як зловмисники здійснять несанкціонований вплив на їх ресурси.

2.2) Спостереження за розвитком технології. Спрямований на спрощення процедури ідентифікації загроз і полягає у відслідковуванні розвитку

найновіших технологій, які можуть бути використані зловмисником для злому ІКС, а також полягає у своєчасному розширенні джерел загроз, що відображається у попередньому сервісі. Для реалізації цього сервісу CERT/CSIRT можуть взаємодіяти з науково-дослідними інститутами, які проводять фундаментальні чи прикладні дослідження в галузі інформаційної безпеки, а також фірмами-виробниками апаратних та програмних засобів, що можуть використовуватись як для забезпечення захисту інформації, так і для реалізації руйнівного впливу на ІКС.

2.3) Аналіз та оцінка систем безпеки. Полягає в оцінці стану інформаційної безпеки певної ІКС чи організації в цілому відповідно до вимог, визначених політикою безпеки цієї організації або стандартами, що діють у цій галузі. Крім того, зазначений сервіс може включати в себе оцінку політики безпеки організації. Існує кілька типів цього сервісу:

- аналіз інфраструктури;
- аналіз на відповідність кращим зразкам;
- сканування;
- випробування на проникнення.

Серед інших профілактичних сервісів можна виділити: налаштування і супроводження автоматизованих засобів, застосунків та інфраструктури сервісів для забезпечення безпеки, розробку засобів безпеки, сервіси виявлення та попередження вторгнень тощо.

Додаткові сервіси. Додаткові сервіси можна умовно поділити на дві категорії: обробка артефактів та управління якістю систем безпеки. До перших відносяться сервіси аналізу артефактів, реагування на артефакти та координація реагування на артефакти (під артефактами необхідно розуміти будь-який файл чи об’єкт системи, який міг бути пов’язаним із атакою на систему чи іншими супутніми цілями зловмисників). Друга категорія містить такі сервіси: забезпечення безперервності роботи та відновлення систем, аналіз ризиків та тренінги для клієнтів з питань інформаційної безпеки.

Контрольні запитання

1. Перерахуйте сервіси, які надаються групами реагування на інциденти.
2. Дайте поняття спостереженню за розвитком технології.
3. Для чого здійснюється збір правової інформації?
4. З чого складається аналіз та оцінка систем безпеки?
5. Перерахуйте профілактичні сервіси, які надаються групами реагування на інциденти**.**

14. ДОКУМЕНТАЦІЙНЕ ЗАБЕЗПЕЧЕННЯ ПРОЦЕСУ УПРАВЛІННЯ ІНЦИДЕНТАМИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Міжнародні стандарти ISO/IEC 27001 та ISO/IEC 27035 вводять такі визначення основних понять у галузі управління інцидентами інформаційної безпеки (ІІБ):

- подія інформаційної безпеки – ідентифікований випадок стану системи або мережі, що вказує на можливе порушення політики інформаційної безпеки чи відмову засобів захисту, або раніше невідому ситуацію, яка може істотно впливати на безпеку;
- інцидент інформаційної безпеки – одинична подія або низка небажаних і непередбачених подій інформаційної безпеки, через які існує ймовірність компрометації бізнес-інформації (бізнес-процесів) і загроза інформаційній безпеці.

Серед інших дефініцій поняття ІІБ також можуть бути корисними такі:

- будь-яка небажана та непередбачена подія, яка може порушити діяльність чи інформаційну безпеку. Відповідно до стандарту ISO 13335-1:2004 ІІБ вважається: втрата надання послуг обладнанням чи пристроями; системні збої чи перевантаження; помилки користувачів; недотримання політик і рекомендацій; порушення фізичних заходів захисту; неконтрольовані зміни систем; збої ПЗ і відмови технічних засобів; порушення правил доступу тощо;
- незапланованe переривання послуги або зниження якості послуги (відповідно до ITIL);
- будь-яка подія, яка не є частиною стандартної роботи служби і яка завдає або може спричинити переривання або зниження якості цієї послуги (відповідно до ISO/IEC 20000:2005).

Стандарт ISO/IEC 27035 визначає формальну модель процесу реагування на ІІБ. Цілями впровадження цієї моделі є впевненість у тому, що:

- події та ІІБ виявляються і обробляються ефективним чином, особливо в частині класифікації подій;
- виявлені ІІБ враховуються і обробляються найбільш відповідним і ефективним чином;
- наслідки ІІБ можуть бути мінімізовані у процесі реагування, можливо із залученням процесів відновлення після збоїв та аварій (BCP/DRP, Business Continuity Planning / Disaster Recovery Plan).

Стандарт ISO/IEC 27001 звертає особливу увагу на необхідність

створення процедури управління ІІБ (УІІБ). Очевидно, що без своєчасного реагування на інциденти безпеки й усунення їх наслідків неможливе ефективне функціонування системи УІБ.

Управління інцидентами інформаційної безпеки – це процес або набір процесів, на вхід яких подаються дані, отримані в результаті збору і протоколювання даних про події, що стосуються інформаційних систем, а на виході цих процесів одержують інформацію про причини інциденту, що відбувся, про збиток, нанесений організації, і заходи, які необхідно вжити для того, щоб інцидент не повторився у майбутньому. Таким чином, УІІБ спрямовано на вдосконалення системи забезпечення безпеки організації. Крім того, одержувані на виході дані є, по суті, єдиною об'єктивною інформацією для визначення ймовірності реалізації загроз при аналізі ризиків.

У більшості організацій процес УІІБ побудований таким чином:

- отримання інформації про інцидент;
- отримання додаткової інформації, пов'язаної з виявленим порушенням;
- аналіз ситуації, локалізація порушення і оперативне застосування контрзаходів;
- встановлення причин, через які стало можливим порушення, що трапилося, і, можливо, визначення відповідальних осіб (розслідування);
- проведення профілактичних заходів, розробка і впровадження заходів з недопущення повторного порушення.

Припущення про те, що в організації стався ІІБ, має базуватися на трьох основних групах порушень:

1) можливі порушення вимог конфіденційності:
- інциденти, через які отримано несанкціонований доступ до інформації;
- втрата носіїв інформації за межами приміщення;
- втрата або крадіжка ноутбука;
- спроби персоналу організації отримати доступ вище наданого рівня;
- спроби зсередини або ззовні отримати доступ до систем (злам).

2) можливі порушення вимог цілісності:
- втрата даних або незавершені транзакції;
- віруси, «троянські коні» (зловмисне ПЗ);
- пошкоджені сектори на жорстких дисках, помилки парності і пам'яті;
- невірні контрольні суми або значення хеш-функцій.

3) можливі порушення вимог доступності:
- зупинка роботи протягом неприйнятного періоду часу. Якщо зупинка

триває довше, ніж обумовлено в SLA, і не може бути усунена протягом певного часу, набирає чинності надзвичайний план;
- віруси, «троянські коні»;
- крадіжка ноутбуків, комплектуючих або носіїв інформації.

У загальному випадку організаційні процедури (регламенти) реагування на ІІБ повинні містити:
- регламенти альтернативних процесів обробки інформації (зокрема, і без використання засобів автоматизації) на період виходу з ладу основних інформаційних ресурсів;
- визначення груп персоналу, відповідальних за виконання тих чи інших функцій у разі виникнення надзвичайної ситуації, а також визначення процедур взаємодії між групами і окремих груп з керівництвом підприємства;
- технічну та організаційну документацію, необхідну для відновлення інформаційних систем і даних після надзвичайної ситуації;
- порядок зберігання архівних (резервних) копій даних і програмних застосунків обробки даних в місцях, захищених від механічного впливу, крадіжок, повеней, пожеж тощо (в т.ч., можливо в місцях, територіально віддалених від основних місць зберігання і обробки інформації);
- угоди з постачальниками програмних і апаратних засобів, що входять в інформаційну інфраструктуру підприємства, про термінове постачання компонент, які вийшли з ладу і потребують заміни у випадку надзвичайної ситуації.

Процес реагування на ІІБ складається з чотирьох основних етапів:
1) виявлення атаки;
2) локалізації атаки;
3) ідентифікації зловмисників;
4) оцінки і подальшого аналізу процесу атаки і його обставин.

Виявлення атак і розпізнавання вторгнень, як правило, є інженерно-технічним завданням, що вирішується за допомогою спеціальних програмних та апаратних засобів. Зокрема, виявлення може здійснюватися шляхом аналізу мережевого трафіку і журналів (лог-файлів), в яких фіксуються різні дії. Виявлення може здійснюватися шляхом аналізу так званих сигнатур - формалізованих наборів ознак певних вірусів, типів атак і т.п. Також, очевидно, джерелом інформації про порушення є повідомлення користувачів про відхилення в роботі інформаційних систем і явні негативні наслідки порушень. З метою своєчасного виявлення порушень необхідно

організувати постійну (при необхідності – цілодобову) роботу фахівців, які відповідають за вирішення інцидентів. Для цього може бути обрано один із можливих підходів:

1) організація власної чергової служби, що складається з компетентних фахівців, які здійснюють позмінне чергування, і оснащені засобами мобільного зв'язку.

2) залучення сторонньої організації, що спеціалізується на наданні подібних послуг. При цьому співробітники підприємства мають знати номери телефонів та інші способи зв'язку, за допомогою яких вони могли б оперативно повідомляти чергового фахівця про всі події. Необхідність забезпечення якомога більш оперативного інформування фахівців з безпеки і, відповідно, якомога більш оперативного реагування, обумовлена тим, що виявлення атаки і запровадження заходів протидії їй у той час, коли напад ще триває, у більшості випадків може бути набагато більш ефективним, ніж реагування після закінчення атаки.

Виявлення порушень здійснюється не тільки за явними ознаками, такими як повідомлення від користувачів про припинення функціонування окремих елементів інформаційних систем, одночасного використання одного облікового запису на декількох робочих станціях або виявлення вірусів у даних, переданих локальною мережею, а й за деякими непрямими ознаками (аномальними явищами), що в окремих випадках можуть свідчити (а можуть і не свідчити) про порушення. Прикладами таких непрямих свідчень можуть бути:

- використання інформаційних систем і певних облікових записів в нехарактерний час (рано вранці, пізно ввечері і т.п.);
- різке нехарактерне підвищення навантаження на інформаційні системи або їх окремі елементи (сегменти мережі, сховища даних тощо);
- зміна характеру поведінки користувачів (наприклад, послідовності певних дій при використанні інформаційної системи) та інші.

Для більш ефективного аналізу таких непрямих ознак і інтерпретації різних фактів фахівцями з реагування на інциденти аналізується функціональність інформаційних систем. Також з метою автоматизації такого аналізу використовуються спеціальні програмні засоби, які забезпечують аналіз статистичних даних мережевого трафіку та інших елементів інформаційної інфраструктури і сигналізують при виявленні аномальної активності, щоб адміністратори могли провести подальший якісний аналіз виявлених відхилень і при необхідності вжити заходи у

відповідь. Розробка і вдосконалення таких засобів аналізу в складі комплексних систем виявлення вторгнень є одним з перспективних напрямків розвитку засобів захисту інформації. Таким чином, основним завданням на початковому етапі реагування є визначення характеру порушень і достовірне встановлення того, що виявлені аномальні події, дії та характеристики є наслідком порушень, а не проявом, наприклад, особливостей роботи програмного забезпечення.

Контрольні запитання

1. Перерахуйте елементи процесу управління інцидентами інформаційної безпеки.
2. Назвіть основні групи порушень.
3. Перерахуйте процедури реагування на інциденти інформаційної безпеки.
4. Перерахуйте етапи процесу реагування на інциденти інформаційної безпеки.
5. Які існують підходи щодо організації роботи фахівців, які відповідають за вирішення інцидентів?

15. ЛОКАЛІЗАЦІЯ ТА УСУНЕННЯ НАСЛІДКІВ ІНЦИДЕНТУ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Локалізація та усунення наслідків є основним етапом, в межах якого, власне, здійснюється реагування на інцидент. На цьому етапі відбувається:

- визначення конкретних параметрів порушення (атаки), його характеру (конкретних сегментів мережі, серверів, груп робочих станцій, застосунків, порушених нападом);
- попередній аналіз дій порушника і сценарію, відповідно до якого відбувається напад, алгоритм роботи виявленого вірусу тощо;
- блокування дій порушника (якщо порушення триває);
- блокування (повне або часткове) роботи інформаційної системи (сервера, бази даних, сегмента мережі тощо) з метою недопущення подальших руйнівних дій, поширення шкідливих програм або витоку конфіденційної інформації.

Припинення нападу і відновлення нормальної роботи інформаційних систем може вимагати скоординованих дій не тільки самих співробітників департаменту інформаційної безпеки, але й:

- фахівців ІТ-підрозділів, відповідальних за інформаційні сервіси, що піддаються атаці;
- користувачів атакованих інформаційних систем;
- підприємств-партнерів, пов’язаних із атакованими інформаційними ресурсами;
- розробників і постачальників атакованих інформаційних систем;
- постачальників телекомунікаційних послуг, через які атака здійснюється;
- сторонніх консультантів, що спеціалізуються на відповідних проблемах інформаційної безпеки.

На цьому етапі обробки інциденту також має значення, якими повноваженнями володіє спеціаліст (черговий), що відповідає за реагування на інциденти. Зокрема, необхідно заздалегідь передбачити можливість оперативного самостійного відключення тих чи інших інформаційних сервісів фахівцями з реагування на інциденти (самостійно, або через відповідний ІТ-підрозділ). Особливо важливою є спроможність відповідальних фахівців оперативно оцінити ситуацію, провести її аналіз (у більшості практичних ситуацій це необхідно робити за неповними даними про нападників) і прийняти рішення про призупинення роботи тих чи інших інформаційних сервісів до моменту виявлення і усунення загроз та/або введення в дію додаткових засобів протидії вторгненням. При прийнятті

такого рішення необхідно враховувати (як правило, на основі експертних оцінок) як можливий збиток, обумовлений виявленим порушенням, так і можливий збиток від зупинки інформаційних сервісів, яка здійснюється з метою запобігання шкоди. Характерним прикладом такої ситуації є напад на систему електронної торгівлі, коли нападник може завдати серйозної шкоди (викрасти конфіденційну інформацію учасників торговельних угод, самостійно вчинити незаконні угоди від імені учасників торгової системи тощо), а зупинка сервісу з метою запобігання такому збитку може призвести до втрат, пов'язаних з упущеною вигодою від недосконалих угод та шкодою для ділової репутації. Іншим прикладом такої ситуації є реагування на розподілені атаки типу «відмова в обслуговуванні» (Distributed Deny of Service, DDoS), які часто здійснюються на сервери в мережі Інтернет, коли виникає необхідність на деякий час повністю відключити сервер, що завдає шкоду і користувачам, і власникам інформаційних ресурсів, розташованих на сервері. Основою для прийняття рішень у таких випадках може бути заздалегідь сформований перелік (довідник) можливих основних інцидентів і ознак порушень (вторгнень), в якому приводиться оцінка ризиків сумарних втрат і рекомендовані заходи для кожного типу порушень (зокрема і перелік ситуацій, коли необхідно здійснити відключення сервісів, щоб уникнути витоку або порушення цілісності інформації, яка є найбільш критичною для діяльності підприємства).

Ідентифікація нападника (або джерела поширення шкідливих програм) є наступним кроком у процесі реагування. Якщо напад здійснювався з локальної мережі підприємства при належному дотриманні внутрішніх режимних правил, це завдання може виявитися відносно простим. Якщо напад було вчинено ззовні, завдання ідентифікації нападників принципово ускладнюється і в деяких ситуаціях проблема стає практично нерозв'язною.

Як правило, для виявлення джерела нападу необхідно:

- детально вивчити всі технічні аспекти атаки;
- провести якісний аналіз процесу атаки у контексті функціонування системи захисту інформації;
- організувати взаємодію зі сторонніми організаціями, які можуть сприяти в ідентифікації нападника.

Однією з найбільш важливих завдань аналізу процесу атаки є встановлення тієї інформації, яка була відома нападаючим до початку атаки і якою вони скористалися для вчинення атаки. Зокрема, в процесі такого аналізу з певним ступенем впевненості можна визначити, що до початку нападу зловмисникам

були відомі:
- інформація про структуру і склад атакованої інформаційної системи (використовувані програмні та апаратні засоби, їх архітектура і налаштування);
- відомості про режим роботи організації та функціонування окремих елементів інформаційної системи, про регламент деяких бізнес-процесів підприємства;
- конкретні ідентифікаційні дані (імена користувачів, паролі), необхідні для проникнення в інформаційну систему та/або правила (алгоритми) їх генерації.

Узагальнення всіх цих відомостей може допомогти встановити, які контакти були у нападників з атакованою компанією (а яких не було), і, зіставляючи факти, а також користуючись методом виключення, намагатися обмежити коло осіб, які потенційно можуть бути причетні до організації даного інциденту.

Одним із завершальних кроків процесу реагування на інцидент є оцінка та аналіз процесу нападу і його обставин. Цей аналіз необхідно проводити в контексті цілей і завдань функціонування всього підприємства, з урахуванням результатів заходів щодо ідентифікації осіб, причетних до нападу.

Завершальним етапом процесу реагування на інциденти є усунення негативних наслідків нападу, локалізація заподіяного збитку. Такими заходами є:
- заміна скомпрометованих паролів окремих користувачів;
- переустановлення пошкоджених операційних систем, а також пошкодженого ПЗ;
- відновлення порушеної конфігурації (налаштувань) ПЗ і операційних систем;
- відновлення пошкодженої інформації (баз даних, файлів) з раніше створених резервних копій або іншими способами.

Крім того, необхідним завершальним кроком може бути додаткова інформаційна робота:
- розсилка користувачам інформації про інциденти, що сталися (у вигляді спеціальних листів та бюлетенів);
- опублікування деяких відомостей про атаки у засобах масової інформації;
- передавання даних про атаки іншим групам реагування на інциденти, а також у науково-дослідні центри, які займаються проблемами захисту

інформації;

- додаткове інформування постачальників інформаційних систем і підрядників, які здійснювали їх постачання, впровадження чи налагодження.

Документування подій ІІБ є необхідним для збору та консолідації свідчень розслідування. Документуванню підлягають всі факти та докази зловмисних дій. Розрізняють технологічні свідчення та операційні свідчення. Технологічними свідченнями є інформація, отримана з технічних засобів збору та аналізу даних (сніфери, системи виявлення вторгнень IDS), операційними – дані або докази, зібрані в процесі опитування персоналу, звернення на Service Desk, дзвінки в call центри.

Типовою практикою є ведення журналу розслідування ІІБ, який не має стандартної форми і розробляється командою реагування. У такому журналі рекомендується фіксувати таку інформацію:

- поточний статус розслідування;
- опис ІІБ;
- заходи, які вживаються командою реагування в процесі обробки інциденту;
- список учасників розслідування з описом їх функцій і ступенем зайнятості в процедурі розслідування;
- перелік свідчень (з обов'язковим зазначенням джерел), зібраних під час обробки інциденту;
- коментарі учасників розслідування інциденту;
- опис подальших заходів та стан процесу (очікування відповіді на запит в call-центр та тощо).

ФОРМА ОТЧЕТА ОБ ИНЦИДЕНТЕ

Пожалуйста, заполните эту форму и отправьте по факсу или email:
*Строки, помеченные *, обязательны для заполнения.*

Имя и организация

1. Имя*:
2. Название организации*:
3. Сектор:
4. Страна*:
5. Город:
6. E-Mail адрес*:
7. Номер телефона*:
8. Другое:

Пораженный компьютер(ы)

9. Количество компьютеров:
10. Hostname и IP*:
11. Функции компьютера*:
12. Часовой пояс:
13. Оборудование (конфигурация):
14. Операционная система:
15. Поврежденное ПО:
16. Поврежденные файлы:
17. Безопасность:
18. Hostname и IP:
19. Протокол/порт:

Инцидент

20. Номер инцидента #:
21. Тип инцидента:
22. Время начала инцидента:
23. Это постоянный инцидент: ДА НЕТ
24. Время и метод обнаружения:
25. Известные уязвимости:
26. Подозрительные файлы:
27. Противомеры:
28. Детальное описание*:

Рисунок 15.1. Типова форма звіту про ІІБ (відповідно до ENISA)

Отчет об инциденте информационной безопасности

Разрешение инцидента

Дата начала расследования инцидента ИБ _____

Фамилия (ии) лица (лиц), проводившего (их) расследование инцидента _____

Дата завершения инцидента ИБ _____

Дата окончания воздействия _____

Дата завершения расследования инцидента ИБ _____

Место хранения отчета о расследовании _____

Причастные к инциденту лица/нарушители

(Один из)

Лицо (PE) ☐ Легально учрежденная организация/учреждение (OI) ☐

Организованная группа (GR) ☐ Случайность (AC) ☐

Отсутствие нарушителя (NP) Например, природные факторы, отказ оборудования, человеческий фактор ☐

Описание нарушителя
Действительная или предполагаемая мотивация

(Один из)

Криминальная/финансовая выгода(CG) ☐ Развлечение/хакерство (PH) ☐

Политика/терроризм (PT) ☐ Месть (RE) ☐

Другие мотивы (OM)

Рисунок 15.2. Фрагмент звіту про ІІБ відповідно до ISO 18044

Типова форма повідомлення про несанкціоновані дії

Всі поля є обов'язковими для заповнення!

Тема повідомлення:

Повна назва організації:

Посада, прізвище та ім'я посадової особи, що повідомляє про несанкціоновані дії:

Контактні дані посадової особи (телефон, факс, e-mail):

Дата та час виявлення несанкціонованих дій (у форматі дд.мм.рррр год:хв:сек):

Опис несанкціонованих дій (дата, спосіб, методи та засоби реалізації, версії та види програмного забезпечення, деталі використання вразливостей програмних та/або апаратних засобів, джерело та об'єкт атаки, лог-файли серверів, будь-яка інша важлива інформація):

c2ck4g

Введіть код:

Відправити

Рисунок 15.3. Форма повідомлення про ІІБ (CERT-UA)

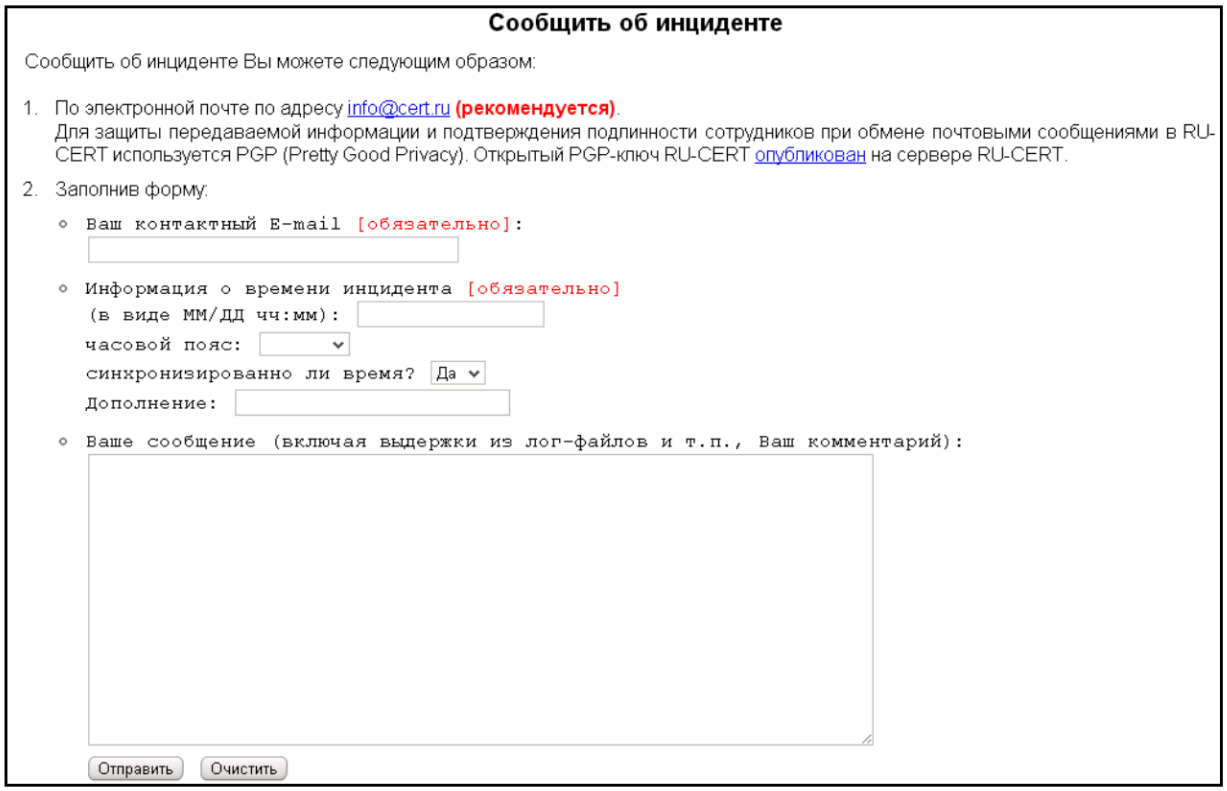

Рисунок 15.4. Форма повідомлення про ІІБ (RU-CERT)

У процесі розслідування ІІБ всі свідчення повинні бути захищені від дискредитації та компрометації, оскільки такі дані можуть містити інформацію про існуючі уразливості інформаційної системи. Серед найбільш важливих документів, які потребують розробки і використання групами CSIRT/CERT, маю бути звіт про інцидент (рис.15.1-15.2) та повідомлення про інцидент (рис.15.3-15.4).

Контрольні запитання

1. Хто здійснює аналіз дій порушника і сценарію, відповідно до якого відбувається напад?
2. Хто здійснює блокування дій порушника?
3. Хто здійснює блокування роботи інформаційної системи?
4. Як здійснюється виявлення джерела нападу?
5. Хто здійснює відновлення нормальної роботи інформаційної системи?

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

Основна література

1. Антонюк А.О. Моделювання систем захисту інформації: Монографія. – Ірпінь: Національний університет ДПС України, 2015. – 273 с.
2. Гаврилова Л.В. Практична методологія ІТ-аудиту. – К.: Наукова думка, 2015. – 304 с.
3. Ус Р.Л. Моделі аудиту інформаційних технологій. – К.:Фенікс, 2013. – 146 с.
4. Міжнародні стандарти контролю якості аудиту: 2-е вид., пер. з англ. Біндера К.С. – К.: Новий формат, 2016. – 613 с.
5. Гузик С.С. Управління та аудит інформаційних технологій. – К.: Jet Info, 2009. – 263 с.
6. Славкова О.П. Особливості проведення аудиту в інформаційному середовищі. – Харків: Ранок, 2011. – 351 с.
7. Значення ІТ-аудиту та його перспективи в Україні: Монографія. – Львів: Видавництво Лева, 2012. – 286 с.

Допоміжна література

1. Родіонов А.М. Логіко-імовірнісна модель захищеності компонентів інформаційно-комунікаційних систем / Новіков О.М., Родіонов А.М. // Інформаційні технології та комп`ютерна інженерія, 2008. – № 1 (11). – С. 170- 175.
2. НД ТЗІ. Загальні положення щодо захисту інформації в комп'ютерних системах від несанкціонованого доступу: НД ТЗІ 1.1–002–99. – К.:: ДСТСЗІ СБ України, 1999. – 16 с.
3. НД ТЗІ. Критерії оцінки захищеності інформації в комп’ютерних системах від несанкціонованого доступу: НД ТЗІ 2.2–004–99. – К.: ДСТСЗІ 497 СБ України, 1999. – 55 с.
4. НД ТЗІ. Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу: НД ТЗІ 2.2–005–99. – К.:ДСТСЗІ СБ України, 1999. – 23 с.
5. НД ТЗІ. Термінологія в галузі захисту інформації в комп’ютерних системах від несанкціонованого доступу: НД ТЗІ 1.1–003–99. –

К.:ДСТСЗІ СБ України, 1999. – 26 с.
6. Жора В.В. Аспекти застосування теорії функціонування організаційних систем до вирішення задач керування захистом інформації, – К.: 2007. - № 14.
7. Глушков В.М. Основы безбумажной информатики. – М.: Наука, 1978. – 552 с.
8. Chunxiao Y., Zhongfu W., and Yunqing F. An Attribute-Based Delegation Model and Its Extension // J. Res. Practice Inform. Technol. 2006. - Vol. 38. No. 1. - P. 220-234.
9. McLean J., John D. A Comment on the «Basic Security Theorem» of Bell and LaPadula // Information Processing Letters. - 1985. - Vol. 20, No. 2. - Feb.

ДЛЯ НОТАТОК

ДЛЯ НОТАТОК

ДЛЯ НОТАТОК

Навчальне видання

Хлапонін Юрій Іванович,
Сєлюков Олександр Васильович

МОНІТОРИНГ ТА АУДИТ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ СИСТЕМ

Конспект лекцій

Редагування та коректура *М.М. Власенко*
Комп’ютерне верстання *М.М. Власенко*

Підписано до друку 25.01.2024 Формат 60x84 1/ 16
Ум. друк. арк. 8,37 Обл.-вид. арк. 6,42
Електронний документ. Вид. № 10/І-16 Зам. 40/1-16

Видавець і виготовлювач
Київський національний університет будівництва і архітектури

Повітрофлотський проспект, 31, Київ, Україна, 03680

Свідоцтво про внесення до Державного реєстру суб’єктів
видавничої справи ДК № 808 від 13.02.2002 р.