і науки України; Міністерство культури України; Київський національний університет культури і мистецтв. – Київ: ВЦ КНУКіМ, 2017. – Ч.1. – С.48-50.
6. *Дубук В.І., Коцун В.І.* Особливості розробки людино-машинного інтерфейсу програмного забезпечення для автоматизованого аналізу даних [Текст] // Теорія і практика сучасної науки (частина ІІІ): матеріали ІІ Міжнародної науково-практичної конференції м. Київ, 15-16.06.2017 р. – Київ.: Міжнародний центр наукових досліджень, 2017. – С.40-43.
7. *Дубук В.І., Чорний М.В., Чорний В.М.* Особливості розробки програмного забезпечення з графічним людино-машинним інтерфейсом для оцінки ринку послуг [Текст] // Технічні вісті, 2017/1(45), 2(46) – С.100-102.
8. Порядок визначення ринків певних телекомунікаційних послуг, проведення їх аналізу та визначення операторів, провайдерів телекомунікацій з істотною ринковою перевагою на ринках таких послуг. – Рішення Національної комісії, що здійснює державне регулювання у сфері зв'язку та інформатизації від 14.10.2014 р. – № 703 [Електронний ресурс]. – Режим доступу: URL: http://http://www.nkrzi.gov.ua/index.php?r=site/index&pg= 158&id=4995&language=uk

Поступила 8.02.2018р.

УДК 519.711

М.Ю. Комаров, Київ
С.Ф. Гончар, Київ
А.В. Ониськова, Київ

НОРМАТИВНИЙ АСПЕКТ ПОБУДОВИ ТА ВПРОВАДЖЕННЯ СИСТЕМИ УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ НА ОБ'ЄКТАХ КРИТИЧНОЇ ІНФРАСТРУКТУРИ

Abstract. A review of the standards of the ISO 2700x series. The basic principles and methods of building a system for information security are considered.

Вступ

Безперервний розвиток інформаційних технологій, а також обрана Україною стратегія інтеграції до міжнародних політичних та економічних інституцій, вимагає всебічної та чіткої гармонізації національних стандартів України в галузі інформаційної безпеки з відповідними міжнародними стандартами, зокрема стандартами серії ISO 2700x.

Побудова та впровадження систем управління інформаційною безпекою на об'єктах критичної інфраструктури є актуальною задачею в контексті забезпечення комплексного підходу захищеності інформаційних ресурсів, які на них розміщені [1].

Основна частина

Управління інформаційною безпекою – це циклічний процес, що включає усвідомлення ступеня необхідності захисту інформації та постановку завдань; збір та аналіз даних про стан інформаційної безпеки в організації; оцінку інформаційних ризиків; планування заходів з обробки ризиків; реалізацію та впровадження відповідних механізмів контролю, розподіл ролей і відповідальності, навчання і мотивацію персоналу, оперативну роботу із здійснення заходів захисту; моніторинг функціонування механізмів контролю, оцінку їх ефективності та відповідні коригувальні дії.

Згідно ISO 27001, система управління інформаційною безпекою (СУІБ) – це «та частина загальної системи управління організації, заснованої на оцінці бізнес ризиків, яка створює, реалізує, експлуатує, здійснює моніторинг, перегляд, супровід і вдосконалення інформаційної безпеки». Система управління включає в себе організаційну структуру, політики, планування, посадові обов'язки, практики, процедури, процеси і ресурси.

Створення та експлуатація СУІБ вимагає застосування такого ж підходу, як і будь-яка інша система управління. Використовувана в ISO 27001 для опису СУІБ процесна модель передбачає безперервний цикл заходів: планування, реалізацію, перевірку, дію (ПРПД).

Процес безперервного вдосконалення зазвичай вимагає початкового інвестування: документування діяльності, формалізація підходу до управління ризиками, визначення методів аналізу і виділення ресурсів. Ці заходи застосовуються для приведення циклу в дію. Вони не обов'язково повинні бути завершені, перш ніж будуть активовані стадії перегляду.

На стадії планування забезпечується правильне завдання контексту і масштабу СУІБ, оцінюються ризики інформаційної безпеки, пропонується відповідний план обробки цих ризиків. У свою чергу, на стадії реалізації впроваджуються прийняті рішення, які були визначені на стадії планування. На стадіях перевірки і дії посилюють, виправляють і вдосконалюють рішення з безпеки, які вже були визначені і реалізовані.

Перевірки можуть проводитися в будь-який час і з будь-якою періодичністю в залежності від конкретної ситуації. У деяких системах вони повинні бути вбудовані в автоматизовані процеси з метою забезпечення негайного виконання і реагування. Для інших процесів реагування потрібно тільки в разі інцидентів безпеки, коли в інформаційні ресурси, які підлягають захисту, були внесені зміни або доповнення, а також коли відбулися зміни загроз і уразливостей. Необхідні щорічні або іншої періодичності перевірки та/або аудити, щоб гарантувати, що система управління в цілому досягає своїх цілей.

Нижче приведений огляд стандартів серії ISO 27000 з метою визначення найбільш пріоритетних із них в рамках створення та впровадження СУІБ на об’єктах енергетичного сектору та критичної інфраструктури [2 – 8].

ISO27000 (ISO/IEC 27000:2009) «Інформаційні технології – Методи забезпечення безпеки – Системи управління інформаційною безпекою –

Визначення та основні принципи».

Даний стандарт містить загальний огляд сімейства стандартів СУІБ. Викладено введення в систему управління інформаційною безпекою. У стандарті наведений короткий опис процесу «План (Plan) – Здійснення (Do) – Перевірка (Check) – Дія (Act)» (PDCA). Також наведені терміни та визначення, які використовуються у сімействі стандартів СУІБ.

ISO27001 (ISO/IEC 27001:2013) «Інформаційні технології – Методи забезпечення безпеки – Системи менеджменту інформаційної безпеки – Вимоги».

Стандарт встановлює вимоги до розробки, впровадження, функціонування, моніторингу, аналізу, підтримки та покращення документованої СУІБ серед спільних бізнес-ризиків організації. Крім того стандарт встановлює вимоги до впровадження заходів управління інформаційною безпекою та її контролю, які можуть бути використані організаціями у відповідності із встановленими цілями та задачами забезпечення інформаційної безпеки.

ISO27002 (ISO/IEC 27002:2013) «Інформаційні технології – Методи забезпечення безпеки – Практичні правила управління інформаційною безпекою».

Цей стандарт надає рекомендації та основні принципи введення, реалізації, підтримки та покращення управління інформаційною безпекою в організації. Цілі, які викладені в стандарті, забезпечують повне керівництво за загальними цілями управління інформаційною безпекою.

Стандарт може служити практичним посібником з розробки стандартів безпеки організації, для ефективної практики управління безпеки організацій та сприяє зміцненню довіри у відносинах між організаціями.

ISO27003 (ISO/IEC 27003:2010) «Інформаційні технології – Методи забезпечення безпеки – Керівництво з впровадження системи управління інформаційною безпекою».

У цьому стандарті розглядаються найважливіші аспекти, необхідні для успішної розробки і впровадження СУІБ відповідно до стандарту ISO / IEC 27001: 2005. У ньому описується процес визначення і розробки СУІБ від запуску до складання планів впровадження. У ньому описується процес отримання схвалення керівництвом впровадження СУІБ, визначається проект впровадження СУІБ (згадується в даному міжнародному стандарті як проект СУІБ) та надані рекомендації з планування проекту СУІБ, в результаті якого виходить остаточний план впровадження СУІБ.

ISO27004 (ISO/IEC 27004:2009) «Інформаційні технології – Методи забезпечення безпеки – Системи менеджменту інформаційної безпеки - Вимірювання».

Даний стандарт містить рекомендації по розробці і використанню вимірювань і заходів вимірювання для проведення оцінки ефективності реалізованої СУІБ, а також заходів і засобів контролю та управління або їх груп за ISO / IEC 27001.

Процес вимірювань стосується політики, менеджменту ризику інформаційної безпеки, заходів і засобів контролю і управління та цілі їх застосування, процесів і процедур, а також підтримує процес перевірки СУІБ, допомагаючи визначити, чи потрібно змінювати або вдосконалювати будь-які з процесів або заходів і засобів контролю і управління СУІБ. Також в стандарті наголошено, що ніякі вимірювання заходів і засобів контролю та управління не можуть забезпечити повну безпеку.

В стандарті процес вимірювань реалізується у вигляді програми вимірювань, пов'язаних з інформаційною безпекою.

ISO27005 (ISO/IEC 27005:2011) «Інформаційні технології – Методи забезпечення безпеки – Управління ризиками інформаційної безпеки».

Цей стандарт являє собою керівництво з управління ризиками інформаційної безпеки в організації, підтримуючи, зокрема, вимоги до СУІБ відповідно до ISO / IEC 27001. Однак цей стандарт не надає будь-якої конкретної методології із управління ризиками інформаційної безпеки.

ISO27006 (ISO/IEC 27006:2007) «Інформаційні технології. Методи забезпечення безпеки – Вимоги до органів аудиту та сертифікації систем управління інформаційною безпекою».

Стандарт на основі стандартів ISO / IEC 17021 та ISO / IEC 27001 встановлює вимоги до органів, що здійснюють аудит і сертифікацію СУІБ, і сприяє проведенню акредитації органів сертифікації.

Будь-який орган, який здійснює сертифікацію СУІБ, повинен продемонструвати в плані компетентності та надійності свою відповідність вимогам даного стандарту, а вказівки, що містяться в стандарті, додатково роз'яснюють ці вимоги до органу, який здійснює сертифікацію СУІБ.

Цей стандарт може використовуватися в якості документа, що містить критерії для акредитації, експертної оцінки або інших процесів аудиту.

ISO27007 (ISO/IEC 27007:2011) «Інформаційні технології – Методи забезпечення безпеки – Керівництво з аудиту Систем управління інформаційної безпеки».

Цей стандарт на додаток до вказівок, що містяться в ISO 19011, надає керівництво з управління програми аудиту СУІБ, з проведення аудитів і за визначенням компетентності аудиторів СУІБ.

ISO27008 (ISO/IEC TR 27008:2011) «Інформаційні технології – Методи забезпечення безпеки – Керівництво для аудиторів з механізмів контролю Систем менеджменту інформаційної безпеки».

Даний стандарт містить вказівки з перевірки реалізації і функціонування заходів і засобів контролю та управління, включаючи перевірку технічної відповідності заходів і засобів контролю та управління інформаційних систем, відповідно до встановлених в організації стандартів з інформаційної безпеки.

ISO27010 (ISO/IEC 27010:2012) «Інформаційні технології – Методи забезпечення безпеки – Управління інформаційною безпекою при комунікаціях між секторами».

Даний стандарт являє собою керівництво із сумісного використання інформації про ризики інформаційної безпеки, механізми контролю, проблеми та/або інциденти, які виходять за межі окремих секторів економіки та держав, особливо, що стосується «критичних інфраструктур».

ISO27011 (ISO/IEC 27011:2008) «Інформаційні технології – Методи забезпечення безпеки – Керівництво з управління інформаційною безпекою для телекомунікацій».

Стандарт надає додаткові рекомендації по реалізації та управлінню інформаційною безпекою в телекомунікаційних організаціях на основі ISO / IEC 27002 (Звід норм і правил менеджменту інформаційної безпеки). Крім цілей безпеки, заходів і засобів контролю та управління, описаних в ISO / IEC 27002, телекомунікаційні організації повинні брати до уваги такі аспекти безпеки: конфіденційність, цілісність, доступність.

ISO27013 (ISO/IEC 27013:2012) «Інформаційні технології – Методи забезпечення безпеки – Керівництво з інтегрованого впровадження ISO/IEC 20000-1 та ISO/IEC 27001».

Цей стандарт надає керівництво щодо спільного використання ISO / IEC 27001 та ISO / IEC 20000-1 для організацій, які планують:

а) реалізувати ISO / IEC 27001, коли стандарт ISO / IEC 20000-1 вже прийнятий, або навпаки;

б) реалізувати одночасно обидва стандарти: ISO / IEC 27001 та ISO / IEC 20000-1;

в) об'єднати існуючі системи управління відповідно до ISO / IEC 27001 та ISO / IEC 20000-1.

Цей стандарт спрямований виключно на спільне використання ISO / IEC 27001 та ISO / IEC 20000-1.

ISO27014 (ISO/IEC 27014:2013) «Інформаційні технології – Методи забезпечення безпеки – Базова структура управління інформаційною безпекою».

В стандарті наведено вимоги до базової структури управління інформаційною безпекою.

ISO27031 (ISO/IEC 27031:2011**) «**Інформаційні технології – Методи забезпечення безпеки – Керівництво із забезпечення готовності інформаційних та комунікаційних технологій та їх використання для управління безперервністю бізнесу».

В приведеному стандарті описуються концепції і принципи готовності інформаційно-телекомунікаційних технологій до забезпечення безперервності бізнесу, і надається система методів і процесів визначення та точного викладу всіх аспектів (таких як критерії ефективності, проектування і реалізація) для вдосконалення готовності інформаційно-телекомунікаційних технологій організації до забезпечення безперервності бізнесу.

ISO27032 (ISO/IEC 27032:2012**) «**Інформаційні технології – Методи забезпечення безпеки – Керівництво із забезпечення кібербезпеки**».**

У даному стандарті наведено загальне керівництво із забезпечення

кібербезпеки для організацій будь-якої форми власності.

ISO27033 (ISO/IEC 27033-1:2009**) «**Інформаційні технології – Методи забезпечення безпеки – Мережева безпека – Основні концепції управління мережевою безпекою**».**

Цей стандарт містить огляд мережевої безпеки і пов'язаних з нею визначень. Стандарт визначає і описує концепції, пов'язані з мережевою безпекою, і надає рекомендації з управління мережевою безпекою. (Додатково до безпеки інформації, що передається по лініях зв'язку, мережева безпека стосується безпеки пристроїв, безпеки діяльності з управління даними пристроями, додатків/послуг, а також безпеки кінцевих користувачів).

ISO27033 (ISO/IEC 27033-2:2012) «Інформаційні технології – Методи забезпечення безпеки – Мережева безпека – Керівництво з проектування та впровадження системи забезпечення мережевої безпеки».

В цьому стандарті наведено визначення того, яким чином організації повинні домагатися необхідної якості спеціалізованих архітектур мережевої безпеки, проектування і реалізації, які забезпечать впевненість у мережевій безпеці, що відповідає їх середовищу діяльності. Даний стандарт призначений для всього персоналу, залученого в плануванні, проектуванні і реалізації аспектів архітектури мережевої безпеки.

ISO27033 (ISO/IEC 27033-3:2010) «Інформаційні технології – Методи забезпечення безпеки – Мережева безпека – Базові мережеві сценарії – загрози, методи проектування та механізми контролю».

У цьому стандарті викладені загрози, методи проектування і питання, що стосуються заходів та засобів контролю і управління, пов'язані з типовими мережевими сценаріями. Для кожного сценарію в ній представлені докладні керівництва з питань загроз безпеки, методам проектування безпеки і заходам і засобам контролю і управління, необхідним для зменшення пов'язаних ризиків.

ISO27033 (ISO/IEC 27033-4:2014) «Інформаційні технології – Методи забезпечення безпеки – Мережева безпека – Забезпечення безпеки міжмережевих взаємодій за допомогою шлюзів безпеки – загрози, методи проектування та механізми контролю».

Наведено визначення конкретних ризиків, методів проектування і питань, що стосуються заходів та засобів контролю і управління, для забезпечення безпеки інформаційних потоків між мережами з використанням шлюзів безпеки.

ISO27033 (ISO/IEC 27033-5) «Інформаційні технології – Методи забезпечення безпеки – Мережева безпека – Забезпечення безпеки Віртуальних Приватних Мереж – загрози, методи проектування та механізми контролю».

Визначено конкретні ризики, методи проектування і питання, що стосуються заходів та засобів контролю і управління, для забезпечення безпеки з'єднань, встановлених з використанням Віртуальних Приватних Мереж (Virtual Private Network, VPN).

ISO27033 (ISO/IEC 27033-6) «Інформаційні технології – Методи забезпечення безпеки – Мережева безпека – Конвергенція в IP-мережах».

В даному стандарті наведено визначення конкретних ризиків, методів проектування і питань, що стосуються заходів та засобів контролю та управління, для забезпечення безпеки мереж з IP-конвергенцією, тобто з конвергенцією даних, мови і відео.

ISO27033 (ISO/IEC 27033-7) «Інформаційні технології – Методи забезпечення безпеки – Мережева безпека – Керівництво із забезпечення безпеки бездротових мереж – Ризики, методи проектування та механізми контролю».

В стандарті дано визначення конкретних ризиків, методів проектування і питань, що стосуються заходів та засобів контролю та управління, для забезпечення безпеки бездротових мереж і радіомереж.

ISO27034 (ISO/IEC 27034-1:2011) «Інформаційні технології – Методи забезпечення безпеки – Огляд та основні концепції в області забезпечення безпеки додатків».

Стандарт надає організаціям керівництво, яка сприятиме інтеграції безпеки в процеси, які використовуються для менеджменту додатків.

ISO27035 (ISO/IEC 27035:2011) «Інформаційні технології – Методи забезпечення безпеки – Управління інцидентами безпеки».

Стандарт надає рекомендації щодо виявлення, реєстрації та оцінки інформації, випадків порушення безпеки і уразливості. Керівництво спрямоване на допомогу організації реагувати на інциденти порушення безпеки, включаючи відповідні заходи контролю для запобігання та скорочення, відновлення наслідків. Стандарт застосовний до будь-якої організації, незалежно від розміру. Він охоплює діапазон інцидентів інформаційної безпеки, в не залежності від того чи є вони навмисними або аварійними, і будь то вони через технічні або фізичні засоби.

ISO27036 (ISO/IEC 27036-1:2014) «Інформаційні технології – Методи забезпечення безпеки – Інформаційна безпека при взаємодії з постачальниками – Частина 1: Огляд та концепції».

Цей документ є вступною частиною серії ISO/IEC 27036. У ньому подані рекомендації організаціям щодо їх інформаційних систем в контексті взаємин з постачальниками.

ISO27036 (ISO/IEC 27036-2:2014) «Інформаційні технології – Методи забезпечення безпеки – Керівництво із взаємодії з постачальниками – Частина 2: Вимоги».

Документ визначає основні вимоги до інформаційної безпеки проведення процесів закупівлі та постачання товарів і послуг: виготовлення, закупівля бізнес-процесів, програмного забезпечення і апаратних компонентів, процесів знань та хмарних обчислень.

ISO27036 (ISO/IEC 27036-3:2013) «Інформаційні технології – Методи забезпечення безпеки – Інформаційна безпека при взаємодії із постачальниками – Частина 3: Керівні вказівки із захисту ланцюгів поставки

інформаційних та комунікаційних технологій».

Стандарт забезпечує споживачів та постачальників в сфері інформаційно-комунікаційних технологій рекомендаціями з питань реагування та управління ризиками інформаційної безпеки, інтеграції процесів і методів забезпечення інформаційної безпеки в системах програмного забезпечення.

ISO27040 (ISO/IEC 27040:2015) «Інформаційні технології – Методи забезпечення безпеки – Безпека зберігання даних».

В стандарті наводяться детальні технічні вказівки про те, як ефективно управляти всіма аспектами безпеки зберігання даних, від планування і проектування до впровадження і документації.

Стандарт включає в себе рекомендації щодо мінімізації ризиків витоку даних і корупції і бере до уваги нові технології і складності підключення, а також підтримує вимоги до системи менеджменту інформаційної безпеки відповідно до ISO/IEC 27001.

ISO27041 (ISO/IEC 27041:2015) **«**Інформаційні технології – Методи забезпечення безпеки – Керівництво з надання гарантій придатності та адекватності методу розслідування інциденту**».**

Стандарт дає рекомендації щодо механізмів забезпечення того, щоб методи та процеси, що використовуються при розслідуванні інцидентів інформаційної безпеки, були "придатними для цілей". Він охоплює практики щодо визначення вимог, опису методів та надання доказів того, що реалізація методів може бути підтверджена вимогам. Включає в себе розгляд того, як постачальники та сторонні випробування можуть бути використані для сприяння процесу гарантування.

Висновки

Проведено аналіз нормативної бази стандартів серії ISO/IEC 2700х для побудови та впровадження систем управління інформаційною безпекою на об’єктах критичної інфраструктури з метою забезпечення комплексного підходу захищеності інформаційних ресурсів, які на них розміщені.

1. *Гончар С.Ф.* Методика побудови системи управління інформаційною безпекою на об’єктах критичної інфраструктури / С.Ф. Гончар, М.Ю. Комаров // Моделювання та інформаційні технології. Зб. наук. пр. ІПМЕ ім. Г.Є. Пухова НАН України. – Вип. 81. – К.: 2017. – С.12-19.

2. *ISO27001* (ISO/IEC 27001:2013) «Інформаційні технології – Методи забезпечення безпеки – Системи менеджменту інформаційної безпеки – Вимоги».

3. *ISO27002* (ISO/IEC 27002:2013) «Інформаційні технології – Методи забезпечення безпеки – Практичні правила управління інформаційною безпекою».

4. *ISO27003* (ISO/IEC 27003:2010) «Інформаційні технології – Методи забезпечення безпеки – Керівництво з впровадження системи управління інформаційною безпекою».

5. *ISO27004* (ISO/IEC 27004:2009) «Інформаційні технології – Методи забезпечення безпеки – Системи менеджменту інформаційної безпеки - Вимірювання».

6. *ISO27005* (ISO/IEC 27005:2011) «Інформаційні технології – Методи забезпечення безпеки – Управління ризиками інформаційної безпеки».
7. *ISO27006* (ISO/IEC 27006:2007) «Інформаційні технології. Методи забезпечення безпеки – Вимоги до органів аудиту та сертифікації систем управління інформаційною безпекою».
8. *ISO27007* (ISO/IEC 27007:2011) «Інформаційні технології – Методи забезпечення безпеки – Керівництво з аудиту Систем управління інформаційної безпеки».

Поступила 25.01.2018р.

УДК 519.6:504.064

В.О. Артемчук, Київ
А.В. Яцишин, Київ

ІНТЕЛЕКТУАЛЬНИЙ АНАЛІЗ ДАНИХ В СИСТЕМІ МОНІТОРИНГУ СТАНУ АТМОСФЕРНОГО ПОВІТРЯ

Abstract. In the article it's shown that the development of means of intellectual analysis of the data of the monitoring network of atmospheric air is an actual scientific and technical problem that needs to be solved. The existing tools of the intellectual analysis of the data of the monitoring network of atmospheric air are investigated, their main advantages and disadvantages are determined.

Вступ. Аналіз світового досвіду свідчить про ефективність та перспективність сенсорних мереж як аналізаторів якості повітряного середовища. В умовах міст України така система моніторингу стану атмосферного повітря (МСАП) допоможе вирішити проблеми, що склалися у цій галузі, покращити технічне оснащення мережі та підвищити її оперативність в рамках зменшення техногенного впливу об'єктів енергетики на довкілля. Проте обов'язковою складовою моніторингу, окрім власне пунктів спостереження, є засоби аналізу даних, в т.ч. інтелектуального, на основі результатів яких відбувається управління екологічною безпекою. Не дивлячись на певне число робіт, в яких розглядаються питання інтелектуального аналізу даних мережі моніторингу стану атмосферного повітря, можна констатувати, що комплексно ці питання з врахуванням вимог та рекомендацій сучасного міжнародного та Українського законодавства досить докладно не розглядалися. Отже, розробка засобів інтелектуального аналізу даних мережі моніторингу стану атмосферного повітря в рамках зменшення техногенного впливу об'єктів енергетики на довкілля є актуальною науково-технічною проблемою, що потребує вирішення.

Основні задачі системи МСАП [8, 9]:

- оцінка та прогнозування рівня забруднення атмосфери (РЗА);

