DOI: 10.32347/2412-9933.2020.43.67-75
УДК 004.056

Криворучко Олена Володимирівна
Доктор технічних наук, професор, завідувач кафедри інженерії програмного забезпечення та кібербезпеки, *orcid.org/0000-0002-7661-9227*
Київський національний торговельно-економічний університет, Київ
Десятко Альона Миколаївна
Старший викладач кафедри інженерії програмного забезпечення та кібербезпеки, *orcid.org/0000-0002-2284-3218*
Київський національний торговельно-економічний університет, Київ
Сунічук Олена Миколаївна
Директор, *orcid.org/0000-0002-6775-7222*
ТОВ «Новелл Консалтинг», Київ

МОДЕЛЮВАННЯ ІНФОРМАЦІЙНОЇ СИСТЕМИ ПРОВЕДЕННЯ НЕЗАЛЕЖНОГО АУДИТУ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Анотація. *У статті розглядається стан України в світовому інформаційному просторі щодо захищеності від кібератак об'єктів критичної інфраструктури. Отже, є необхідність в розробленні та фукціонуванні такої інформаційної системи, яка б підтримувала аудит інформаційних систем з усіма її складовими – підсистемами. Запропонована інформаційна система має бути інтегрованою, мати ієрархічну структуру. Така інформаційна система дає можливість допускати інтеграцію як зовнішньої і внутрішньої інформації, горизонтальне та вертикальне об'єднання між системами з різною ієрархічною структурою. Процес моделювання інформаційної системи відбувається за допомогою Case-технології ERwin, яка дає можливість описувати всі необхідні процеси з високою точністю, в результаті чого система, що моделюється, визначається як сукупність взаємопов'язаних функцій та активностей. Відповідно проводиться декомпозиція системи, що дає можливість визначити модель цієї інформаційної системи у вигляді ієрархічної сукупності низки підсистем, на кожному з рівнів якої здійснюються деякі процедури з розв'язанням локальних задач. Концептуальні моделі таких підсистем дають наочне моделювання всіх учасників інформаційної системи та наявних потоків інформації (як вхідних, так і вихідних, як внутрішніх, так і зовнішніх впливів). Також в процесах моделювання інформаційної системи застосовується нотація IDEF3, яка своєю чергою використовує графічний опис інформаційних потоків, взаємин між процесами опрацювання інформації та об'єктів, що є частиною цих процесів. Так, в конкретному випадку представляється можливість описати та змоделювати компоненти діаграми декомпозиції процесу системи оцінювання фахової підготовки аудиторів інформаційної безпеки. Інформаційна система зазначеної предметної області має бути спочатку змодельованою системою, тобто мають бути визначені основні вимоги та механізми щодо впровадження незалежного аудиту інформаційної безпеки на об'єктах критичної інфраструктури.*

Ключові слова: інформаційна безпека; аудит інформаційної безпеки; інформаційна система; декомпозиція інформаційної системи; моделювання; Case-технологія ERwin

Вступ

Як відомо, краще запобігти наслідкам, ніж їх усувати. Це стосується не лише повсякденного життя, а й сфери ІТ.

Очевидно, Україна не зможе системно, прозоро і успішно реагувати на виклики щодо своєї критичної інфраструктури, перебуваючи в правовому вакуумі. Тому всі діючі ініціативи є лише логічною відповіддю держави на свій намір закрити цей пробіл [1].

У 2018 р. набрав чинності Закон України "Про основні засади забезпечення кібербезпеки України". Цей Закон запровадив термін об'єкта критичної інфраструктури, визначив повноваження для формування переліку об'єктів критичної інфраструктури, декларував спеціальний режим для операторів критичної інфраструктури, однак не визначив критеріїв, згідно з якими ті чи інші об'єкти можуть бути ідентифіковані як об'єкти критичної інфраструктури. Порядок реалізації таких повноважень відповідно до Закону мав бути прийнятий ще у 2018 р.

Чинний Закон визначає, що до об'єктів критичної інфраструктури можуть належати підприємства, установи та організації, які здійснюють діяльність і надають послуги в галузі енергетики, хімічної промисловості, транспорту, інформаційно-комунікаційних технологій, електронних комунікацій, в банківському і фінансовому секторах [1].

Загальні заходи контролю стосуються структур, правил і процедур, які регулюють усю або головні частини інформаційної безпеки системи установи, такі як: реалізація політик безпеки, стале функціонування інфраструктури організації та налаштування робочих місць кінцевих користувачів з розподіленням доступу. Загальні заходи контролю створюють середовище контролю, в якому функціонують прикладні системи.

Мета статті

Основною метою статті є розкрита процесів моделювання інформаційної системи функціонування методик, які ефективно, надійно та результативно покажуть єдину ідеологічну систему незалежного аудиту інформаційної безпеки з її складовими.

Виклад основного матеріалу

Для проведення ІБ-аудиту аудитору необхідний належний набір критеріїв аудиту, які можна застосувати до об’єкта аудиту.

Критерії аудиту – це принципи (або норми), які використовуються для оцінювання чи тестування об’єкта аудиту, а у разі необхідності для презентації або повідомлення результатів аудиту. Мета розроблення набору критеріїв аудиту полягає у створенні набору норм для відображення реальності. Критерії аудиту узгоджуються з керівництвом.

Важливо, щоб ІТ-аудитор знав, що він має обрати правильні критерії аудиту на основі об’єкта аудиту, його ризиків та межі аудиту. Зазвичай критерії аудиту походять з багатьох рамкових основ. Час, який аудитор інформаційної безпеки (аудиторська група) міг витратити на розроблення власних основ для різних об’єктів, він витрачає на аудит. При цьому аудитор (і аудиторська група) мають перевіряти, чи підходять обрані критерії для кожного нового аудиту.

Так чи інакше має бути визначено нормативно та змодельовано загальний порядок проведення атестації аудиторів інформаційної безпеки та ті чи інші вимоги до визначення кваліфікаційної придатності аудиторів та критеріїв їх відповідності атестованим аудиторам.

Періодичність проведення аудиту для різних об’єктів критичної інфраструктури в умовах невизначеності критеріїв та порядку приналежності об’єктів до об’єктів критичної інфраструктури, переліку таких об’єктів, загальних вимог до їх кіберзахисту, у т. ч. щодо застосування індикаторів кіберзагроз мають бути більш чітко зазначені – один раз на рік, чи на два і т.д.

Проблема підготовки та підтримання професійно-відповідного стану фахівців з кібербезпеки на теренах освітнього простору закладів вищої освіти займаються В. Бурячок, І. Пархомея, М. Степанов, В. Толубок; І. Логінов, Є. Скулиш, П. Біленчук, А. Войцехівський, С. Демідюк, В. Марков та ін.

Практичні дослідження і реалізація інформаційної системи проведення незалежного аудиту інформаційної безпеки розглядається в роботах [4; 6 – 9].

Нижче представлено загальну модель розроблення методики, що має умовну назву «Методика аудиту інформаційної безпеки», яка має бути ефективною, надійною, результативною, доцільною. Необхідно розглянути всю єдину ідеологічну систему незалежного аудиту інформаційної безпеки з її складовими та визначити можливості організації елементів.

Основними компонентами, що визначають ефективність створюваної ідеологічної системи, є такі підсистеми (назви умовні, але відображають змістовну характеристику):

– «Оцінка компетентностей аудиторів інформаційної безпеки»;

– «Обробка інформації аудиту ІБ»;

– «Рейтинг аудитора ІБ».

Система аудиту інформаційної безпеки повинна бути інтегрованою і допускати інтеграцію зовнішньої і внутрішньої інформації, горизонтальну та вертикальну інтеграцію між системами з різною ієрархічною структурою.

Принципи, які є складовою моделі декомпозиції ідеологічної системи:

– принцип кінцевої мети – абсолютний пріоритет кінцевої (глобальної) мети;

– принцип єдності – спільний розгляд системи як цілого й як сукупності частин (елементів);

– принцип зв’язку – система розглядається як взаємодія зв’язків між її елементами та навколишнім оточенням;

– принцип модульної побудови – виокремлення модулів у системі й розгляд її як сукупності модулів;

– принцип ієрархії – введення ієрархії частин (елементів) і (або) їх ранжування;

– принцип функціональності – спільний розгляд структури і функцій із пріоритетом функцій над структурою;

– принцип розвитку – врахування змінюваності системи, її здатність до розвитку, заміни елементів, накопичення інформації;

– принцип децентралізації – об'єднання інтересів централізації та децентралізації у висновках, що формуються;

– принцип невизначеності – врахування невизначеності й випадковості в системі.

На основі запропонованих моделей є можливість створювати раціональні технічно-програмні засоби.

Моделювання передбачає проведення розрахунків, спостережень, логічного аналізу на моделях з тим, щоб за результатами такого дослідження можна було судити про явища, які відбуваються в реалії.

Моделювання дає змогу:

– оцінити якість організації системи («Оцінка компетентностей аудиторів інформаційної безпеки»);

– розробити систему збирання та аналізу інформації під час аудиту інформаційної безпеки («Обробка інформації аудиту ІБ»);

– розробити систему рейтингу аудиторів інформаційної безпеки («Рейтинг аудитора ІБ»).

Процес моделювання відбувається на основі середовища Case-технології ERwin. Метою методології є побудова функціональної схеми досліджуваної системи, яка описує всі необхідні процеси з точністю, достатньою для однозначного моделювання діяльності системи загалом. Іншими словами, система моделювання представляє сукупність взаємопов'язаних робіт (функцій, активностей). Case-технології ERwin широко використовується в моделюванні, тому що ця методологія легко представляє такі системні характеристики, як управління, зворотний зв'язок, виконавців.

Для підсистеми «Оцінка компетентностей аудиторів інформаційної безпеки» характерна ієрархічна структура з вертикальною декомпозицією системи на рівні і горизонтальною – на підсистеми. На кожному рівні існує уявлення про пряму і функціональну підлеглість, відповідальність, повноваження. Ієрархічно організаційна система цілей має також ієрархічний характер внаслідок того, що загальна (глобальна) ціль досягається виконанням ієрархічної сукупності окремих операцій (підцілей) різних рангів.

Будь-яка складна система може бути декомпозована на низку підсистем, які своєю чергою також можна розглядати як системи, які володіють тими ж властивостями розчленовування на ще менші компоненти. Відповідно відбувається декомпозиція на кожному з етапів за виокремленими рівнями.

Повна декомпозиція системи дає можливість представити модель цієї системи у вигляді ієрархічної сукупності цілого ряду підсистем, на кожному з рівнів якої здійснюються деякі процедури за рішенням локальних завдань.

Визначаючи вирішення проблеми як систему, представляємо процес вирішення проблеми як процес розроблення, виготовлення і використання системи.

Основними складовими будь-якої системи є: Вхід – Input (навантаження системи): середовище, що впливає на механізм процесу (операції); управління; процеси (операції); Вихід - Output (результат): структурна композиція компонентів системи

При цьому є можливість зміни якісних і кількісних характеристик елементів входу і виходу, їх спостереження і корегування.

Відповідно відбувається моделювання "Системи оцінки фахової підготовки аудиторів інформаційної безпеки, збору та аналізу інформації, отриманої під час аудиту інформаційної безпеки". Такий підхід дає змогу проаналізувати детально кожну частину всієї системи, зберігаючи зв'язок частин і цілого, внести необхідні корективи, а у результаті завершення аналізу процесу – виконати синтез системи.

Синтез системи управління складається з:

– виявлення і визначення входу, критерію оптимізації і складання схеми системи;

– побудови моделі системи;

– збирання і використання даних (імітація функціонування системи) в цілях вдосконалення/побудови останньої.

Такою системою, яка застосовується для опису моделі проєктування та управління "Системою оцінки фахової підготовки аудиторів інформаційної безпеки, збору та аналізу інформації, отриманої під час аудиту інформаційної безпеки" є CASE-технологія ERwin.

CASE-технологія ERwin дає змогу не тільки спроєктувати діяльність будь-якої організаційної структури, але й після докладного аналізу і виявлення недоліків побудувати низку нових моделей, визначивши оптимальну по відношенню до базової структури.

При моделюванні система розглядається як довільна підмножина деякого універсуму. При цьому необхідно визначити кожен об'єкт як компонент такої системи, вказавши зовнішні впливи на нього й встановивши залежності від інших елементів системи. Система, яка моделюється, має межу, що відокремлює її від зовнішнього середовища. Взаємодія з універсумом описується так: Input – наявні показники, критерії та інша інформація, що опрацьовується системою; Output – результат діяльності системи; Control – стратегії та процедури, під управлінням яких функціонує система;

Mechanism – ресурси, необхідні для проведення роботи.

Перебуваючи під керуванням, система перетворює входи на виходи, використовуючи певні механізми. Модель у нотації IDEF0 – це сукупність ієрархічно впорядкованих і взаємозалежних діаграм. Моделювання системи розпочинається з розроблення контекстної діаграми, яка є вершиною деревоподібної структури діаграм і містить узагальнений опис системи та її взаємодії із зовнішнім середовищем. Після опису системи в цілому проводиться розбиття її на великі фрагменти. Цей процес називається функціональною декомпозицією, а діаграми, що описують кожен фрагмент і взаємодію фрагментів, називають діаграмами декомпозиції. Після декомпозиції контекстної діаграми проводиться декомпозиція кожного великого фрагмента системи на більш дрібні (за потреби) і так доти, доки не буде досягнуто потрібний рівень деталізації.

Концептуальна модель «Система аудиту інформаційної безпеки системи» зображена на рис. 1.

Робота «Система аудиту інформаційної безпеки», на яку своєю чергою впливає інформація та компоненти (що відображені стрілками входу, виходу, керування, механізму в CASE-технології ERwin), показана стрілками взаємодії системи з універсумом, що охарактеризовано в табл. 1.

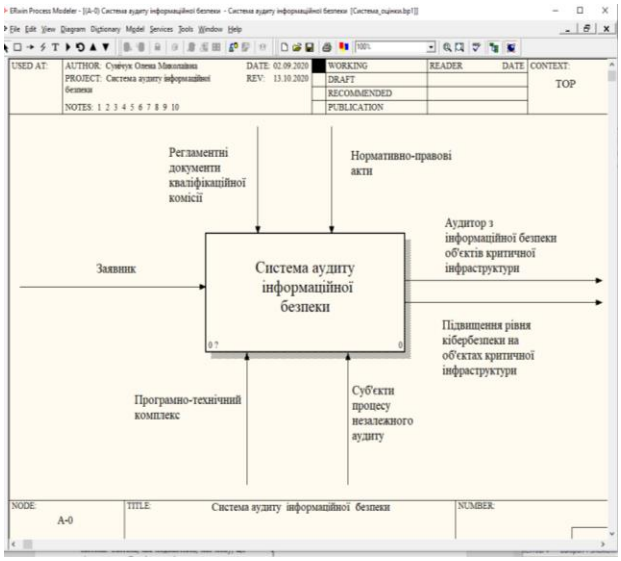

Рисунок 1 – Концептуальна модель «Система аудиту інформаційної безпеки»

Джерело: побудовано в системі ERwin (знімок з екрана)

Таблиця 1 – ***Характеристика стрілок концептуальної моделі «Система аудиту інформаційної безпеки системи»***

Назва	Характеристика	Тип
Заявник	Фізична особа, яка має намір отримати статус аудитора з інформаційної безпеки (аудитора) об'єктів критичної інфраструктури або Технічного спеціаліста, які мають право входити до складу команди з аудиту інформаційної безпеки об'єктів критичної інфраструктури.	Input
Нормативно-правові акти	Закон України "Про основні засади забезпечення кібербезпеки"; Закон України "Про Державну службу спеціального зв'язку та захисту інформації України"; Закон України "Про захист інформації в інформаційно-телекомунікаційних системах"; Указ Президента України від 27.09.1999 № 1229 "Про Положення про технічний захист інформації в Україні" Постанова Кабінету Міністрів України від 19.06.2019 № 518 "Про затвердження Загальних вимог до кіберзахисту об'єктів критичної інфраструктури"; Постанова Кабінету Міністрів України від 23.08.2016 № 563 "Про затвердження Порядку формування переліку інформаційно-телекомунікаційних систем об'єктів критичної інфраструктури держави"; Постанова Кабінету Міністрів України від 29.03.2006 № 373 "Про затвердження Правил забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах"	Control
Регламентні документи кваліфікаційної комісії	Документи, що розробляються кваліфікаційною комісією	Control
Суб'єкти системи незалежного аудиту	Кваліфікаційна комісія. Замовник послуг аудиту інформаційної безпеки Адміністратор спеціального програмного забезпечення аудиту	Mechanism

Закінченя табл. 1

Програмно-технічний комплекс	Автоматизоване робоче місце для атестації. Спеціальне програмне забезпечення	Mechanism
Аудитор з інформацій ної безпеки об'єктів критичної інфраструктури	Фізична особа, яка довела кваліфікаційну придатність для проведення незалежного аудиту інформаційної безпеки на об'єктах критичної інфраструктури та дані про яку внесено до довірчого списку аудиторів, розробляє та затверджує Звіт про аудит інформаційної безпеки об'єкту критичної інфраструктури	Output
Підвищення рівня кібербезпеки на об'єктах критичної інфраструктури	Удосконалення системи інформаційної безпеки об'єкта критичної інформаційної інфраструктури об'єкта критичної інфраструктури відповідно до звіту незалежного аудитора ІБ та формування додаткових заходів із забезпечення кіберзахисту об'єктів критичної інфраструктури	Output

Під час моделювання «Система аудиту інформаційної безпеки системи» засобами CASE-технології ERwin контекстна діаграма декомпозується, створивши при цьому нижній рівень (рис. 2).

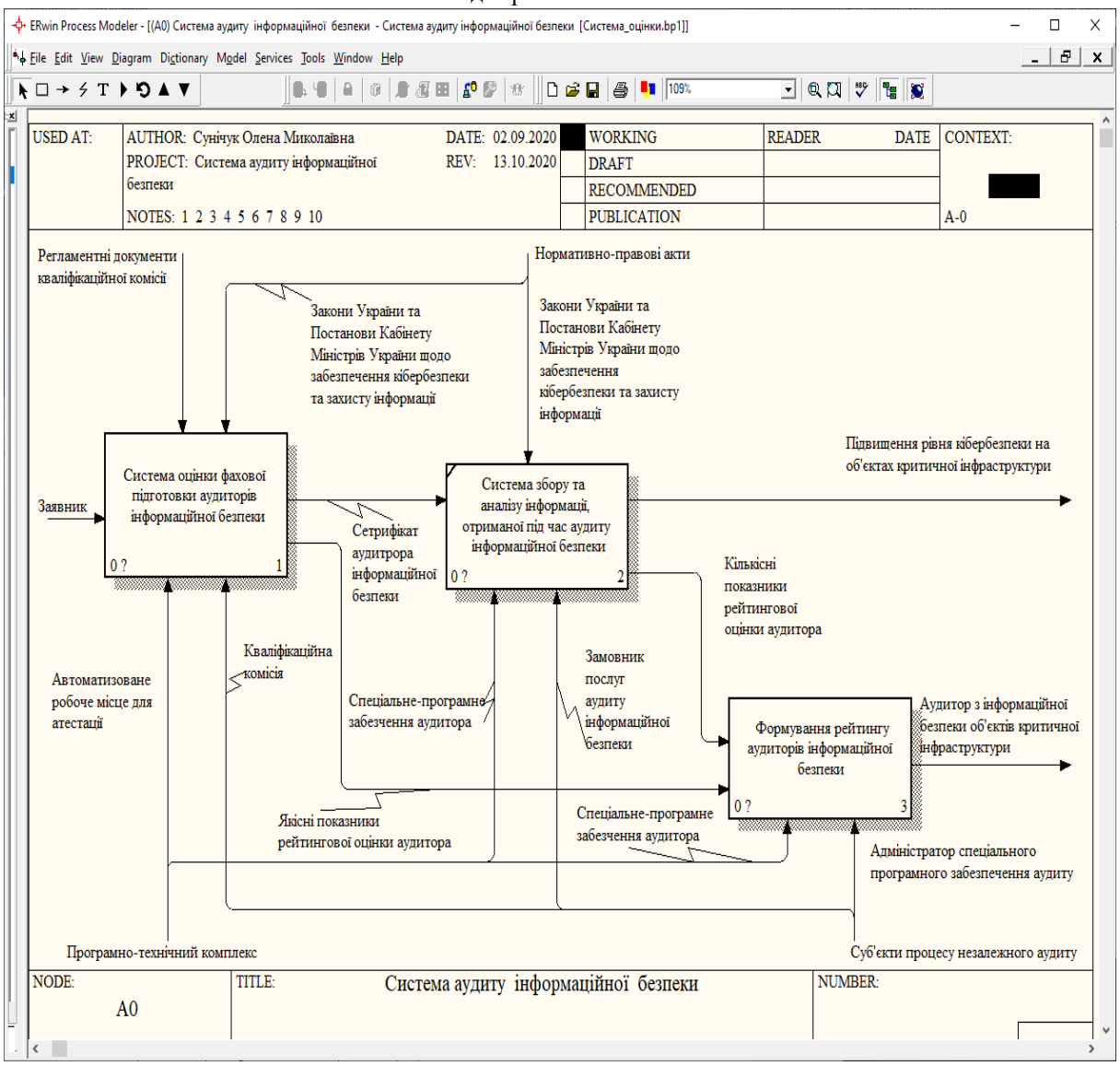

Рисунок 2 – Перша декомпозиція концептуальної моделі системи аудиту інформаційної безпеки
Джерело: побудовано в системі ERwin (знімок з екрану)

Інформаційна система є досить складним утворенням, побудованим у багаторівневій архітектурі. Модель таких складових системи оцінювання фахової підготовки аудиторів інформаційної безпеки, збирання та аналізу інформації, отриманої під час аудиту інформаційної безпеки, «Оцінка компетентностей аудиторів інформаційної безпеки та «Рейтинг аудитора ІБ» побудовані в нотації IDEF3. У статті наведемо приклад *декомпозиції другого рівня «Оцінка компетентностей аудиторів інформаційної безпеки».*

IDEF3-методологія моделювання, що використовує графічний опис інформаційних потоків, взаємин між процесами опрацювання інформації та об'єктів, що є частиною цих процесів. IDEF3 дає можливість аналітикам описати ситуацію, коли процеси виконуються в певній послідовності, а також описати об'єкти, які беруть участь спільно в одному процесі. Будь-яка IDEF3-діаграма може містити роботи, зв'язку, перехрестя і об'єкти посилань.

Наведемо пояснення до компонентів «перехрестя» діаграми у табл. 2.

Діаграма декомпозиції другого рівня «Оцінка компетентностей аудиторів інформаційної безпеки», побудована в нотації IDEF3, містить роботи, зв'язки, перехрестя і об'єкти посилань, компоненти яких представлені на рис. 3.

Таблиця 2 – ***Характеристики компонентів діаграми побудована в нотації IDEF3 (перехрестя)***

Позначення	Назва	Fan-in Junction	Fan-out Junction
&	Asynchronous AND	Всі процеси, що передували, повинні бути завершеними	Всі процеси, що йдуть наступними, повинні бути запущені
&	Synchronous AND	Всі процеси, що передували, повинні бути завершеними одночасно	Всі процеси, що йдуть наступними, повинні бути запущені одночасно
O	Asynchronous OR	Один або декілька процесів, що передували, повинні бути завершені	Один або декілька процесів, що йдуть наступними, повинні бути запущені
O	Synchronous OR	Один або декілька процесів, що передували, повинні бути завершені одночасно	Один або декілька процесів, що йдуть наступними, повинні бути одночасно
X	Exclusive OR	Тільки один з попередніх процесів є завершеним	Тільки один з наступних процесів запускається

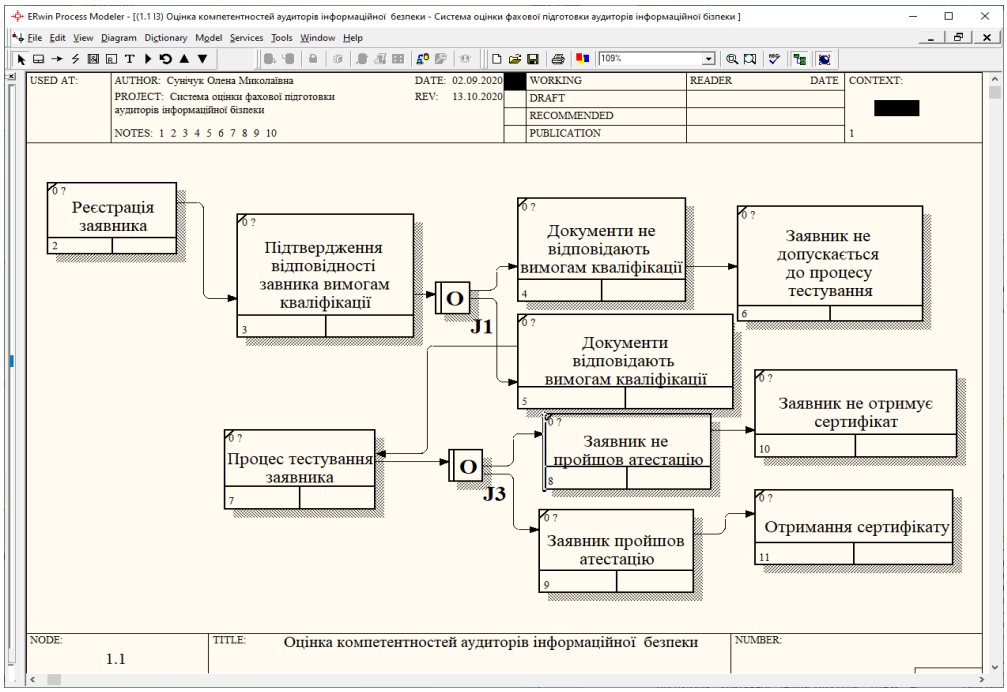

Рисунок 3 – Діаграма декомпозиції другого рівня «Оцінка компетентностей аудиторів інформаційної безпеки»
Джерело: побудовано в системі ERwin (знімок з екрана)

Мета цієї змодельованої системи – визначити основні вимоги та механізми щодо впровадження незалежного аудиту інформаційної безпеки на об'єктах критичної інфраструктури.

Висновки

Наведений сегмент має деякі неузгодженості юридичного аспекту, які перебувають у стані активного завершення, наприклад: немає чіткого визначення переліку об'єктів критичної інфраструктури; немає чітких вимог до аудиторів ІБ; немає чіткості, на яких вимогах національних та міжнародних стандартів інформаційної безпеки, на яких повинен базуватися звіт тощо [2].

Проте це завдання необхідно вирішувати, моделювати та прогнозувати. Так, наочність CASE-технології ERwin робить модель інформаційної «Системи аудиту інформаційної безпеки системи» цілком зрозумілою і для осіб, які не брали участі в проєкті її створення, а також ефективною для проведення та вдосконалення потоків необхідної інформації, зміни рівнів декомпозиції, в решті-решт показів і презентацій. Надалі на базі побудованої моделі можуть бути організовані нові проєкти, націлені на внесення змін в моделі.

Список літератури

1 Всеукраїнське щотижневе професійне юридичне видання «Юридична газета оonline». Юрій Котляров. «Україна рухається до врегулювання системи захисту критичної інфраструктури» Електронний ресурс. URL: https://yur-gazeta.com/gazeta/info/

2 Національне агентство з питань запобігання корупції. Результати перевірок. Електронний ресурс. URL: https://old.nazk.gov.ua/rezultaty-perevirok

3 Methodology Forming for the Approaches to the Cyber Security of Information Systems Management / A. Adranova, L. Yona, O. Kryvoruchko, A. Desiatko. Journal of Theoretical and Applied Information Technology (ISSN: 1992-8645, E-ISSN: 1817-3195). 2020. P. 1993–2005. (Retrieved from www.scopus.com)

4 Криворучко О. В. Аналіз стану захищеності інформаційно-телекомунікаційних систем [Текст] / О. В. Криворучко, О. М. Сунічук, Д. В. Швець, О. В. Мінін // Управління розвитком складних систем. – 2020. – № 42. – С. 56 – 62.

5 Олександр Чаузов Держспецзв'язок: поглиблення системного підходу й розвиток в Україні сучасного захищеного цифрового суспільства. Часопис BUSINESS PANORAMA (Ділова панорама) №3 2019 (спецвипуск "Кібербезпека").

6 Браіловський М. М., Хорошко В. О. Особливості кібербезпеки на підприємствах України. Безпека соціально-економічних процесів в кіберпросторі: матеріали Всеукр. наук.-практ. конф. Київ, 27 березня 2019 р. С. 18–19

7 Problems of information security in enterprise / V. Semidotska, O. Kryvoruchko, M. Tsiutsiura, A. Desyatko. Information Protection and Information Systems Security (VII International Scientific and Technical Conference) = Захист інформації і безпека інформаційних систем: матеріали VII Міжнар. наук.-техн. конф. Львів, 30–31 травня 2019 р. Львів: Вид-во Львівської політехніки, 2019. С. 33 – 35.

8 Desyatko A., Shestak Y., Kryvoruchko O. Cybersecurity as a Part of Business. Безпека ресурсів інформаційних систем: зб. тез І Міжнар. наук.-практ. конф. Чернігів, 16–17 квітня 2020 р. Чернігів: НУЧП, 2020. С. 12 – 15.

9 Криворучко О. В., Сунічук О. М., Десятко А. М. Компетентістна модель формування фахівця з кібераудиту. Соціально-економічні аспекти розвитку суспільства : матеріали Міжнародної науково-практичної конференції (Одеса, 7 серпня 2020 р). Одеса : Східноєвропейський центр наукових досліджень, 2020. С. 58 – 60.

10 ISO/IEC 27001 Information Security Management. Електронний ресурс. URL: https://www.iso.org/isoiec-27001-information-security.html (Дата останнього відгуку 05.09.2020).

11 Закон України «Про основні засади забезпечення кібербезпеки України» (Відомості Верховної Ради (ВВР), 2017, № 45, ст.403).

12 Закон України «Про Державну службу спеціального зв'язку та захисту інформації України» (Відомості Верховної Ради України (ВВР), 2006, № 30, ст.258)

13 Закон України "Про інформацію" (Відомості Верховної Ради України (ВВР), 1992, № 48, ст.650)

14 Про рішення Ради національної безпеки і оборони України від 27 січня 2016 року "Про Стратегію кібербезпеки України" Указ Президента України; Стратегія від 15.03.2016 № 96/2016

15 Закон України «Про основні засади забезпечення кібербезпеки України» від 5 жовтня 2017 року № 2163-VIII. Електронний ресурс. Точка доступу: https://zakon.rada.gov.ua/laws/show/2163-19

16 Порталт газети «Українська правда». Електронний ресурс. Точка доступу: https://www.epravda.com.ua/publications/2016/12/9/613957/

17 Портал «Держкомзв'язок». Шляхи вирішення проблеми інформаційної безпеки в Україні. Електронний ресурс. Точка доступу: http://www.dsszzi.gov.ua/dsszzi/ control/uk/publish/article%3Bjsessionid=CE0C98AFB4AE2CF71790756873D292F6?art_id=38826&cat_id=38712

18 Черевко О. В. Теоретичні засади поняття інформаційної безпеки та класифікація загроз системі інформаційного захисту / Ефективна економіка. № 5, 2020.

19 Кальченко В. В. Огляд методів проведення тестування на проникнення для оцінки захищеності комп'ютерних систем. Системи управління, навігації та зв'язку. 2018. №4. – С. 109-114.

20 Сороковская А. А. Информационная безопасность предприятия: новые угрозы и перспективы [Электронный ресурс]. – Режим доступа: http://nbuv.gov.ua/portal/Soc_Gum/Vchnu_ekon/2010_2_2/032-035.pdf. Гайворонський М.В., Новіков О.М. Безпека інформаційно-комунікаційних систем. – К.: Видавнича група BHV,2009. – 608 с.

21 Дронь М. М., Малайчук В.П., Петренко О. М. Основи теорії захисту інформації: Навч. посібник. – Д.: Вид-во Дніпропетр. ун-ту, 2001. – 312 с.

22 Даник Ю. Г. і Супрунов Ю. М. Деякі підходи до формування системи підготовки кадрів для системи кібернетичної безпеки України // Збірник наукових праць ЖВІ НАУ "Інформаційні системи", 2011, вип. 5, С. 5 – 22.

23 Міночкін А. І. "Інформаційна боротьба: сучасний стан та досвід підготовки фахівців", Оборонний вісник, К., Центр воєнної політики та політики безпеки, 2011, № 2, С. 12 – 14.

24 Сисоєв В. Аналіз рівня освіти та підготовки фахівців з управління IT та інформаційної безпеки в Україні. [Електронний ресурс]. Режим доступу: http://www.auditagency.com.ua/blog/ISACA_research_Education.pdf. Дата звернення: 24 травня 2018.

25 "Перший стандарт вищої освіти стосується кібербезпеки" [Електронний ресурс]. Режим доступу: https://ligazakon.net/lawnews/doc/-nz173112-pershyy-standart-vyshchoyi-osvity-stosuyetsya-kiberbezpeky?type=ep. Дата звернення: 24 травня 2018.

26 "Cybersecurity: A Generic Reference Curriculum (RC). Dear Partners/NATO Members, 4500-1 (OSEM PED)", Oct. 2016, 73 p.

27 "ISO/IEC 27032:2012. Information technology – Security techniques – Guidelines for cybersecurity", 50 p.

28 Center for Internet Security, CIS Controls Version 7 – What's Old, What's New [electronic source] https://www.cisecurity.org/cis-controls-version-7-whats-old-whats-new/. Last access: 24 May, 2019.

29 Center for Internet Security. CIS Controls [electronic source] https://www.cisecurity.org/controls/. Last access: 24 May, 2019.

Стаття надійшла до редколегії 05.09.2020

Kryvoruchko Olena
DSc (Eng.), Professor, Head of the Department of at Software Engineering and Cyber Security, *orcid.org/0000-0002-7661-9227*
Kyiv National University of Trade and Economics, Ukraine
Desiatko Alona
Senior Lecturer at Software Engineering and Cyber Security Department, *orcid.org/0000-0003-3270-4494*
Kyiv National University of Trade and Economics, Ukraine
Synichuk Olena
Director, orcid.org, *orcid.org/0000-0002-6775-7222*
Novell Consulting, LLC, Ukraine

MODELING OF THE INFORMATION SYSTEM OF INFORMATION SECURITY INDEPENDENT AUDIT

Abstract. *This article examines the condition of our country in the global information space in terms of protection against critical infrastructure cyberattacks. Accordingly, there is a need to develop and operate such an information system that would support the audit of information systems with all its components - subsystems. The proposed information system should be integrated, have a hierarchical structure. Such an information system makes it possible to allow the integration of both external and internal information, horizontal and vertical integration between systems with a different hierarchical structure. The process of modeling an information system takes place using ERwin's Case technology, which makes it possible to describe all the necessary processes with high accuracy, as a result of which the modeled system is defined as a set of interrelated functions and activities. Accordingly, the system is decomposed, which makes it possible to determine the model of this information system in the form of a hierarchical set of a number of subsystems, at each level of which some procedures are performed to solve local problems. Conceptual models of such subsystems provide visual modeling of all participants in the information system and existing information flows (both input and output, both internal and external influences). IDEF3 notation is also used in information system modeling processes, which in turn uses a graphical description of information flows, relationships between information processing processes and objects that are part of these processes. Thus, in this case, it is possible to describe and model the components of the decomposition diagram of the process of assessing the professional training of information security auditors. The information system of the specified subject area must first be a simulated system, ie the basic requirements and mechanisms for the implementation of an independent audit of information security at critical infrastructure facilities must be defined.*

Keywords: information security; information security audit; information system; information system; decomposition, modeling; ERwin case technology

References

1. Ukrainian weekly professional legal publication "Legal newspaper online". Yuri Kotlyarov. "Ukraine is moving to regulate the protection of critical infrastructure" [electronic source] https://yur-gazeta.com/gazeta/info/

2. National Agency for the Prevention of Corruption. Results of inspections. [electronic sourse] https://old.nazk.gov.ua/rezultaty-perevirok

3. Adranova, A., Yona, L., Kryvoruchko, O., Desiatko, A. (2020). Methodology Forming for the Approaches to the Cyber Security of Information Systems Management. Journal of Theoretical and Applied Information Technology (ISSN: 1992-8645, E-ISSN: 1817-3195), 1993–2005. (Retrieved from www.scopus.com)

4. Kryvoruchko, O. V., Sunichuk, O. M., Shvets, D. V., Minin, O. V. (2020). Analysis of the state of security of information and telecommunication systems. Management of development of complex systems, 42, 56 – 62.

5. Chauzov, Oleksandr. (2019). State Special Communications: Deepening the System Approach and Development of a Modern Protected Digital Society in Ukraine. BUSINESS PANORAMA Magazine (Business Panorama), 20193.

6. Brailovsky, M.M., Khoroshko, V.O. (2019). Features of cybersecurity at the enterprises of Ukraine. Security of socio-economic processes in cyberspace: Procc. Ukrainian. scientific-practical conf. Kyiv, March 27, Pp. 18 – 19

7. Semidotska, V., Kryvoruchko, O., Tsiutsiura, M., Desyatko, A. (2019). Problems of information security in enterprise / Information Protection and Information Systems Security (VII International Scientific and Technical Conference). Protection of information and security of information systems: Procc. VII International. scientific and technical conf. Lviv, May 30–31, 2019. Lviv: Lviv Polytechnic Publishing House, Pp. 33 – 35.

8. Desyatko, A., Shestak, Y., Kryvoruchko, O. (2020). Cybersecurity as a Part of Business. Security of information systems resources: collection. thesis I International. scientific-practical conf. Chernihiv, April 16–17, 2020. Chernihiv: NUCHP, 2020. P. 12 – 15.

9. Kryvoruchko, O.V., Sunichuk, O.M., Desyatko, A.M. (2020). Competent model of forming a cyber audit specialist. Socio-economic aspects of society development: materials of the International scientific-practical conference (Odessa, August 7, 2020). Odessa: Eastern European Center for Scientific Research, 2020. Pp. 58-60.

10. ISO/IEC 27001 Information Security Management. [electronic source] https://www.iso.org/isoiec-27001-information-security.html (Last access 05.09.2020).

11. Law of Ukraine "About Basic Principles of Ensuring Cyber Security of Ukraine" (Vidomosti Verkhovnoi Rady (VVR), 2017, № 45, p. 403).

12. Law of Ukraine "About Information" (Vidomosti Verkhovnoi Rady Ukrainy (VVR), 1992, № 48, p.650).

13. Law of Ukraine "About Information Protection in Information and Telecommunication Systems" (Vidomosti Verkhovnoi Rady Ukrainy (VVR), 1994, № 31, p. 286).

14. About the decision of the National Security and Defense Council of Ukraine of January 27, 2016 "About the Cyber Security Strategy of Ukraine" Decree of the President of Ukraine; Strategy from 15.03.2016 № 96/2016

15. Law of Ukraine "About Basic Principles of Cyber Security of Ukraine" of October 5, 2017 № 2163-VIII. Electronic resource. Access point: https://zakon.rada.gov.ua/laws/show/2163-19 [electronic source] https://zakon.rada.gov.ua/laws/show/2163-19

16. Portal of the newspaper "Ukrainian Truth". [electronic source] https://www.epravda.com.ua/publications/2016/12/9/613957/

17. Portal «Derzhkomzv"yazok». Ways to solve the problem of information security in Ukraine.. [electronic source] http://www.dsszzi.gov.ua/dsszzi/control/uk/publish/article%3Bjsessionid=CE0C98AFB4AE2CF71790756873D292F6?art_id=38826&cat_id=38712

18. Cherevko, O. V. (2020). Theoretical principles of the concept of information security and classification of threats to the information protection system. Efficient economy, 5.

19. Kalchenko, V. V. (2018). An overview of penetration testing methods for assessing the security of computer systems. Control, navigation and communication systems, 4, 109-114.

20. Sorokovskaja, A. A. (2010). Information security company: new threats and prospects. Available at: http://nbuv.gov.ua/portal/Soc_Gum/Vchnu_ekon/2010_2_2/032-035.pdf (Accessed 28 April 2014).

21. Gaivoronsky, M. V., Novikov, O. M. (2009). Security of information and communication systems. K.: BHV Publishing Group, 608.

22. Dron, M. M., Malaychuk, V. P., Petrenko, O. M. (2001). Fundamentals of information security theory: Textbook. manual. Dnipropetrovsk Publishing House. University, 312.

23. Danyk, Yu. G. & Suprunov, Yu. M. (2011). Some approaches to the formation of the training system for the cybersecurity system of Ukraine. Collection of scientific works of ZhVI NAU "Information Systems, 5 – 22.

24. Minochkin, A. I. (2011). Information struggle: the current state and experience of training. Defense Bulletin. K., Center for Military and Security Policy, 2, 12 – 14.

25. Sysoev, V. (2018). Analysis of the level of education and training of specialists in IT management and information security in Ukraine. [electronic source] http://www.auditagency.com.ua/blog/ISACA_research_Education.pdf. Last access: 24 May 2018.

26. "The first standard of higher education concerns cybersecurity" [electronic source] https://ligazakon.net/lawnews/doc/-nz173112-pershyy-standart-vyshchoyi-osvity-stosuyetsya-kiberbezpeky?type=ep. Data zvernennya: 24 May 2018

27. Cybersecurity: A Generic Reference Curriculum (RC). (2016). Dear Partners/NATO Members, 4500-1 (OSEM PED), 73.

28. "ISO/IEC 27032:2012. Information technology – Security techniques – Guidelines for cybersecurity", 50.

29. Center for Internet Security, CIS Controls Version 7 – What's Old, What's New [electronic source] https://www.cisecurity.org/cis-controls-version-7-whats-old-whats-new/. Last access: 24 May, 2019.

30. Center for Internet Security. CIS Controls [electronic source] https://www.cisecurity.org/controls. Last access: 24 May, 2019.

Посилання на публікацію

APA *Kryvoruchko, Olena, Desiatko, Alona & Synichuk, Olena, (2020). Modeling of the information system of information security independent audit. Management of Development of Complex Systems, 43, 67 – 75, [in Ukrainian]; dx.doi.org\10.32347/2412-9933.2020.43.67-75.*

ДСТУ *Криворучко О.В. Моделювання інформаційної системи проведення незалежного аудиту інформаційної безпеки [Текст] / О. В. Криворучко, А. М. Десятко, О. М. Сунічук // Управління розвитком складних систем. – 2020. – № 43. – С. 67 – 75; dx.doi.org\10.32347/2412-9933.2020.43.67-75.*