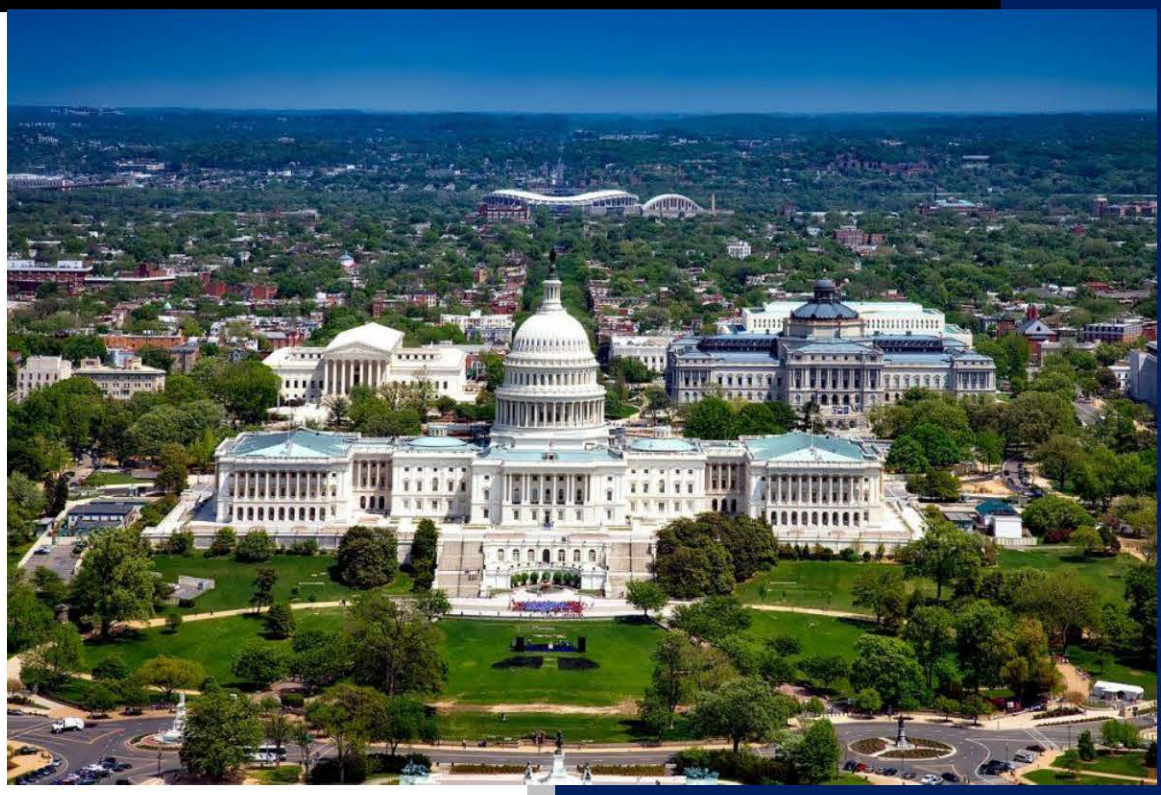
SCIENTIFIC COLLECTION «INTERCONF»

№ 3 (36)
November, 2020

THE ISSUE CONTAINS:

Proceedings of the 7th International Scientific and Practical Conference

CHALLENGES IN SCIENCE OF NOWADAYS



WASHINGTON, USA

26-28.11.2020

InterConf
Scientific Publishing Center

SCIENTIFIC COLLECTION «INTERCONF»

№ 3 (36) | November, 2020

THE ISSUE CONTAINS:

Proceedings of the 7th International Scientific and Practical Conference

CHALLENGES IN SCIENCE OF NOWADAYS

WASHINGTON, USA

26-28.11.2020

WASHINGTON
2020

UDC 001.1

S 40 *Scientific Collection «InterConf»*, (36): with the Proceedings of the 7th International Scientific and Practical Conference «Challenges in Science of Nowadays» (November 26-28, 2020) in Washington, USA: EnDeavours Publisher, 2020. 1495 p.

ISBN 979-1-293-10109-3

The recommended citation:
Surname N. (2020). Title of article or abstract. *Scientific Collection «InterConf»,* (36): with the Proceedings of the 7th International Scientific and Practical Conference «Challenges in Science of Nowadays» (November 26-28, 2020) in Washington, USA; pp. 21-27. Available at: https://interconf.top/...

This issue of Scientific Collection «InterConf» contains the International Scientific and Practical Conference. The conference provides an interdisciplinary forum for researchers, practitioners and scholars to present and discuss the most recent innovations and developments in modern science. The aim of conference is to enable academics, researchers, practitioners and college students to publish their research findings, ideas, developments, and innovations.

TABLE OF CONTENTS

GENERAL ENGINEERING AND MECHANICS

MODELING AND NANOTECHNOLOGY

INFORMATION AND WEB TECHNOLOGIES

UDC 681.3

Голубничий Дмитро Юрійович

ORCID ID: 0000-0002-6873-7004

кандидат технічних наук, доцент, доцент кафедри Інформаційних систем Харківський національний економічний університет імені Семена Кузнеця, Україна

Коломійцев Олексій Володимирович

ORCID ID: 0000-0001-8228-8404

Заслужений винахідник України, доктор технічних наук, старший науковий співробітник, професор кафедри

Національний технічний університет "Харківський політехнічний університет", Україна

Третяк Вячеслав Федорович

ORCID ID: 0000-0003-2599-8834

кандидат технічних наук, доцент, науковий співробітник наукового центру Повітряних Сил Харківський національний університет Повітряних Сил імені Івана Кожедуба, Україна

Рязанін Сергій Григорович

студент

Харківський національний університет радіоелектроніки, Україна

ТЕХНОЛОГІЇ АУДИТУ КІБЕРБЕЗПЕКИ ІНФОРМАЦІЙНИХ СИСТЕМ

Інформаційна система (ІС) – система, що реалізує автоматизований збір, обробку та маніпулювання даними, і включає: технічні засоби, програмне забезпечення, відповідний персонал і допоміжні засоби (рис. 1) [1-4].

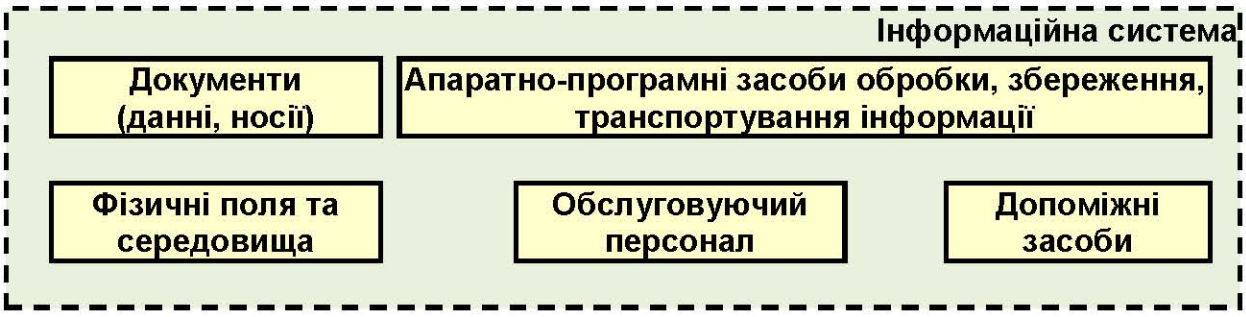


Рис. 1. Складові інформаційної системи

Кібербезпека ІС не є даністю, а створюється шляхом побудови системи захисту інформації (СЗІ) в ІС. Відповідно до нормативних документів і загальноприйнятою практикою можна виділити наступні етапи побудови СЗІ.

1. Визначення інформаційних ресурсів (ІР), які підлягають захисту.
2. Виявлення повної множини загроз кібербезпеки ІР, які підлягають захисту.
3. Проведення оцінки вразливості і ризиків для ІР, які підлягають захисту, при виявленій множині загроз.
4. Розробка проекту (плану) системи захисту інформації, що знижує за обраним критерієм ризики для ІР, які підлягають захисту, при виявленій множині загроз.
5. Реалізація проекту (плану) захисту інформації.
6. Визначення якості реалізованої системи захисту.
7. Здійснення контролю функціонування і управління системою захисту.

Проходження етапів необхідно в тій чи іншій мірі здійснювати безперервно і по замкнутому циклу, з проведенням відповідного аналізу стану СЗІ та уточненням вимог до неї після кожного кроку (рис. 2).

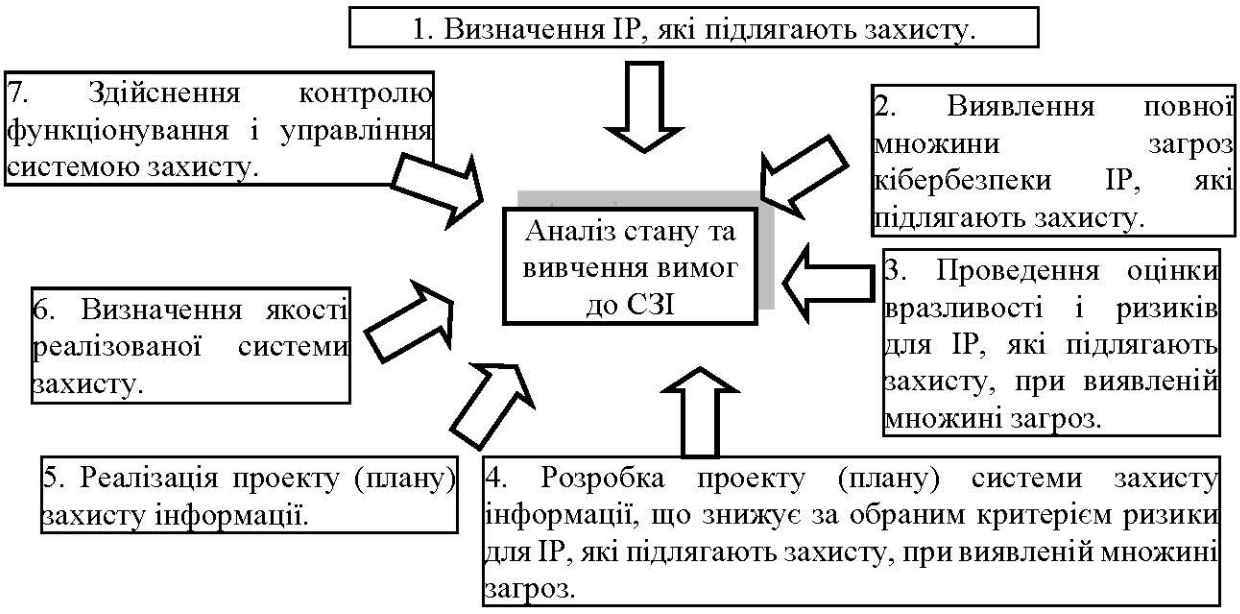


Рис. 2. Етапи побудови системи захисту інформації

Аудит кібербезпеки при створенні СЗІ доцільно здійснювати:

– на третьому етапі при оцінки вразливості ІР в складі ІС;

– на шостому етапі при визначенні якості реалізованої системи захисту;

– на сьомому етапі періодично при здійсненні контролю функціонування СЗІ.

Аудит являє собою незалежну експертизу окремих областей функціонування організації. Розрізняють зовнішній й внутрішній аудит.

Зовнішній аудит кібербезпеки ІС - це зовнішнє захід щодо ІС, підключеної до глобальної мережі Інтернет, з метою оцінки можливості подолання СЗІ ІС з боку зовнішнього зловмисника. Зовнішній аудит рекомендується проводити періодично.

Внутрішній аудит являє собою безперервну діяльність, яка здійснюється на підставі документа, зазвичай носить назву "Положення про внутрішній аудит", і відповідно до плану, підготовка якого здійснюється підрозділом внутрішнього аудиту та затверджується керівництвом організації.

Аудит кібербезпеки ІС є однією зі складових ІТ-аудита. Цілями проведення аудиту кібербезпеки є:

– аналіз ризиків, пов'язаних з можливістю здійснення загроз кібербезпеки щодо ресурсів ІС;

– оцінка поточного рівня захищеності ІС;

– локалізація вузьких місць в системі захисту ІС;

– оцінка відповідності ІС існуючим стандартам в області кібербезпеки;

– вироблення рекомендацій щодо впровадження нових та підвищення ефективності існуючих механізмів кібербезпеки ІС.

У число додаткових завдань, що стоять перед внутрішнім аудитором, крім надання допомоги зовнішнім аудиторам, можуть також входити:

– розробка політик кібербезпеки та інших організаційно-розпорядчих документів щодо захисту інформації та участь в їх впровадженні в роботу організації;

– постановка завдань для IT-персоналу, що стосуються забезпечення захисту інформації;

– участь в навчанні користувачів і обслуговуючого персоналу ІС питань забезпечення кібербезпеки;

– участь в розборі інцидентів, пов'язаних з порушенням кібербезпеки;

– інші завдання.

Необхідно відзначити, що всі перераховані "додаткові" завдання, які стоять перед внутрішнім аудитором, за винятком участі в навчанні, по суті аудитом не є. Аудитор за визначенням повинен здійснювати незалежну експертизу реалізації механізмів кібербезпеки в організації, що є одним з основних принципів аудиторської діяльності. Якщо аудитор бере діяльну участь в реалізації механізмів кібербезпеки, то незалежність аудитора втрачається, а разом з нею втрачається і об'єктивність його суджень, так як аудитор не може здійснювати незалежний і об'єктивний контроль своєї власної діяльності. Однак на практиці внутрішній аудитор, часом будучи найбільш компетентним фахівцем в організації в питаннях забезпечення кібербезпеки, не може залишатися осторонь від реалізації механізмів захисту.

Етап збору інформації аудита, є найбільш складним і тривалим. Це пов'язане з відсутністю необхідної документації на ІС і з необхідністю щільної взаємодії аудитора з багатьма посадовими особами організації.

Компетентні висновки щодо стану справ в організації з інформаційною кібербезпекою можуть бути зроблені аудитором тільки за умови наявності всіх необхідних вихідних даних для аналізу. Отримання інформації про організацію, функціонування і поточний стан ІС здійснюється аудитором в ході спеціально організованих інтерв'ю з відповідальними особами організації, шляхом вивчення технічної і організаційно-розпорядчої документації, а також дослідження ІС з використанням спеціалізованого програмного інструментарію. Зупинимося на тому, яка інформація необхідна аудитору для аналізу.

Перший пункт аудиторського обстеження починається з отримання інформації про організаційну структуру користувачів ІС і обслуговуючих підрозділів. Зазвичай в ході інтерв'ю аудитор задає опитуваним наступні питання: хто є власником інформації, хто є споживачем інформації, хто є постачальником послуг. Призначення і принципи функціонування ІС багато в чому визначають існуючі ризики і вимоги кібербезпеки, що пред'являються до системи. Тому на наступному етапі аудитора цікавить інформація про призначення та функціонуванні ІС. Далі, аудитору потрібно більш детальна інформація про структуру ІС. Це дозволить усвідомити, яким чином здійснюється розподіл механізмів кібербезпеки за структурними елементами і рівнями функціонування ІС.

Підготовка значної частини документації на ІС зазвичай здійснюється вже в процесі проведення аудиту. Коли всі необхідні дані по ІС, включаючи документацію, підготовлені, можна переходити до їх аналізу.

Використовувані аудиторами методи аналізу даних визначаються вибраними підходами до проведення аудиту, які можуть істотно різнитися.

Перша технологія, сама складна, та базується на аналізі ризиків. Опираючись на методи аналізу ризиків, аудитор визначає для обстежуваної ІС індивідуальний набір вимог кібербезпеки, найбільшою мірою враховуючої особливості даної ІС, середовища її функціонування й існуючі в даному середовищі погрози кібербезпеки. Дана технологія є найбільш трудомістким і вимагає найвищої кваліфікації аудитора. На якість результатів аудита, у цьому випадку, сильно впливає використовувана методологія аналізу й управління ризиками і її застосовність до даного типу ІС.

Друга технологія, сама практична, та опирається на використання стандартів кібербезпеки. Стандарти визначають базовий набір вимог кібербезпеки для широкого класу ІС, що формується в результаті узагальнення світової практики. Стандарти можуть визначати різні набори вимог кібербезпеки, залежно від рівня захищеності ІС, що потрібно забезпечити, її

приналежності (комерційна організація, або державна установа), а також призначення (фінанси, промисловості, зв'язок і т.п.). Від аудитора в цьому випадку потрібно правильно визначити набір вимог стандарту, відповідність яким потрібно забезпечити для даної ІС. Необхідна також методика, що дозволяє оцінити цю відповідність. Через свою простоту (стандартний набір вимог для проведення аудита вже заздалегідь визначений стандартом) і надійності (вимоги стандарту ніхто не спробує заперечити), описаний підхід найпоширеніший на практиці (особливо при проведенні зовнішнього аудита). Він дозволяє при мінімальних витратах ресурсів робити обґрунтовані висновки про стан ІС.

Третя технологія, найбільш ефективна, та припускає комбінування перших двох. Базовий набір вимог кібербезпеки, пропонованих до ІС, визначається стандартом. Додаткові вимоги, у максимальному ступені враховуючі особливості функціонування даної ІС, формуються на основі аналізу ризиків. Цей підхід є набагато простіше першого, тому що більша частина вимог кібербезпеки вже визначена стандартом, і, у той же час, він позбавлений недоліку другого підходу, що містить у тім, що вимоги стандарту можуть не враховувати специфіки обстежуваної ІС.

Аудиторський звіт є основним результатом проведення аудиту. Його якість характеризує якість роботи аудитора.

Структура звіту може суттєво відрізнятися в залежності від характеру і цілей проведеного аудиту. Однак певні розділи повинні обов'язково бути присутнім в аудиторському звіті.

Він повинен, принаймні, містити опис цілей проведення аудиту, характеристику досліджуваної ІС, вказівку кордонів проведення аудиту і використовуваних методів, результати аналізу даних аудиту, висновки, узагальнюючі ці результати і містять оцінку рівня захищеності ІС або відповідність її вимогам стандартів, і, звичайно, рекомендації аудитора щодо усунення існуючих недоліків та вдосконалення системи захисту.

Аналіз ризиків – це те, із чого повинне починатися побудову будь-якої системи кібербезпеки. Він містить у собі заходу щодо обстеження кібербезпеки ІС, з метою визначення того які ресурси й від яких погроз треба захищати, а також у якому ступені ті або інші ресурси мають потребу в захисті. Визначення набору адекватних контрзаходів здійснюється в ході управління ризиками. Ризик визначається ймовірністю заподіяння збитку й величиною збитку, що наноситься ресурсам ІС, у випадку здійснення погрози кібербезпеки.

Аналіз ризиків полягає в тому, щоб виявити існуючі ризики й оцінити їхню величину (дати їм якісну, або кількісну оцінку). Процес аналізу ризиків ділиться на кілька послідовних етапів:

– ідентифікація ключових ресурсів ІС;

– визначення важливості тих або інших ресурсів для організації;

– ідентифікація існуючих погроз кібербезпеки й вразливостей, що роблять можливим здійснення погроз;

– обчислення ризиків, пов'язаних зі здійсненням погроз кібербезпеки.

Ресурси ІС можна розділити на наступні категорії:

– інформаційні ресурси;

– програмне забезпечення;

– технічні засоби (сервери, робочі станції, мережне обладнання тощо);

– людські ресурси.

У кожній категорії ресурси діляться на класи й підкласи. Необхідно ідентифікувати тільки ті ресурси, які визначають функціональність ІС і істотні з погляду забезпечення кібербезпеки.

Важливість (або вартість) ресурсу визначається величиною збитку, який наноситься у випадку порушення конфіденційності, цілісності або доступності цього ресурсу. Звичайно розглядаються наступні види збитку:

– дані були розкриті, змінені, вилучені або стали недоступні;

– апаратури була ушкоджена або зруйнована;

– порушено цілісність програмного забезпечення.

Збиток може бути нанесений організації в результаті успішного здійснення наступних видів погроз кібербезпеки:

– локальні й вилучені атаки на ресурси ІС;

– стихійні лиха;

– помилки, або навмисні дії персоналу ІС;

– збої в роботі ІС, викликані помилками в програмному забезпеченні або несправностями апаратури.

Під вразливостями звичайно розуміють властивості ІС, що роблять можливим успішне здійснення погроз кібербезпеки.

Величина ризику визначається на основі вартості ресурсу, імовірності здійснення погрози й величини вразливості по наступній формулі:

$$\text{Ризик} = \frac{\text{вартість\_ресурсу} \cdot \text{ймовірність\_погрози}}{\text{величина\_вразливості}}. \quad (1)$$

Завдання управління ризиками полягає у виборі обґрунтованого набору контрзаходів, що дозволяють знизити рівні ризиків до прийнятної величини. Вартість реалізації контрзаходів повинна бути менше величини можливого збитку. Різниця між вартістю реалізації контрзаходів і величиною можливого збитку повинна бути обернено пропорційна ймовірності заподіяння збитку.

Якщо для проведення аудита кібербезпеки обраний підхід, що базується на аналізі ризиків, то на етапі аналізу даних аудита звичайно виконуються наступні групи завдань:

– Аналіз ресурсів ІС, включаючи інформаційні ресурси, програмні й технічні засоби, а також людські ресурси;

– Аналіз груп завдань, розв'язуваних системою, і бізнес процесів;

– Побудова (неформальної) моделі ресурсів ІС, що визначає взаємозв'язку між інформаційними, програмними, технічними й людськими ресурсами, їхнє взаємне розташування й способи взаємодії;

– Оцінка критичності інформаційних ресурсів, а також програмних і технічних засобів;

– Визначення критичності ресурсів з обліком їх взаємозалежності;

– Визначення найбільш імовірних погроз кібербезпеки відносно ресурсів ІС і вразливостей захисту, що роблять можливим здійснення цих погроз;

– Оцінка ймовірності здійснення погроз, величини вразливостей і збитку, що наноситься організації у випадку успішного здійснення погроз;

– Визначення величини ризиків для кожної трійки: погроза – група ресурсів – вразливість.

Перерахований набір завдань, є досить загальним. Для їхнього рішення можуть використовуватися різні формальні й неформальні, кількісні і якісні, ручні й автоматизовані методики аналізу ризиків. Суть підходу від цього не міняється.

Оцінка ризиків може даватися з використанням різних як якісних, так і кількісних шкал. Головне, щоб існуючі ризики були правильно ідентифіковані та проранжовані у відповідності зі ступенем їхньої критичності для організації. На основі такого аналізу може бути розроблена система першочергових заходів щодо зменшення величини ризиків до прийнятного рівня.

Список джерел:

1. Борисенко О. А., Бережна О. В., Новгородцев А. І., Сердюк В. В. & Яковлев М. М. (2019) “Система передачі та відображення інформації із захистом числових даних”, Системи обробки інформації, вип. 2, с. 103 – 108.
2. Коломійцев, О., Третяк, В., Закіров, З., Кукобко, С., Калачова, В., & Мартовицький, В. (2020). Оптимізація завантаження файлів сховища даних в olap-файли на основі рангового підходу. InterConf, (25), 108-117. вилучено із https://ojs.ukrlogos.in.ua/index.php/interconf/article/view/4300.
3. Кучернюк П. В., (2018) “Методи і технології захисту комп’ютерних мереж (фізичний та канальний рівні)”, Мікросистеми, Електроніка та Акустика, т. 22, № 6(101), с. 64 – 70
4. Коломійцев, О., Рябуха, Ю., Калачова, В., & Третьяк, В. (2020). Аналіз методів і процедур шкального оцінювання в задачах прийняття рішень при проектуванні і супроводженні розподілених автоматизованих інформаційних систем. InterConf, (15). вилучено із https://ojs.ukrlogos.in.ua/index.php/interconf/article/view/2309.

SCIENTIFIC EDITION

BN 979-1-293101-09

9 791293 101093

SCIENTIFIC COLLECTION «INTERCONF»

№ 3 (36) | November, 2020

The issue contains:

Proceedings of the 7th International Scientific and Practical Conference

CHALLENGES IN SCIENCE OF NOWADAYS

WASHINGTON, USA
26-28.11.2020

Contacts of the editorial office:

Scientific Publishing Center «InterConf»
E-mail: info@interconf.top
URL: https://www.interconf.top

InterConf
Scientific Publishing Center