SCIENTIFIC COLLECTION INTERCONF+

№ 84
November, 2021

THE ISSUE CONTAINS:

Proceedings of the 5th International Scientific and Practical Conference

THEORY AND PRACTICE OF SCIENCE: KEY ASPECTS

ROME, ITALY

7-8.11.2021

ISSN 2709-4685

InterConf
Scientific Publishing Center

SCIENTIFIC COLLECTION «INTERCONF»

№ 84 | November, 2021

THE ISSUE CONTAINS:

Proceedings of the 5th International Scientific and Practical Conference

THEORY AND PRACTICE OF SCIENCE: KEY ASPECTS

ROME, ITALY

7-8.11.2021

ROME
2021

UDC 001.1

INDEX COPERNICUS INTERNATIONAL

S 40 *Scientific Collection «InterConf»*, (84): with the Proceedings of the 5th International Scientific and Practical Conference «Theory and Practice of Science: Key Aspects» (November 7-8, 2021). Rome, Italy: Dana, 2021. 478 p.

ISBN 978-88-32012-34-7
DOI 10.51582/interconf.7-8.11.2021

EDITOR COORDINATOR

EDITORIAL BOARD

If you have any questions or concerns, please contact a coordinator Mariia Granko.

The recommended styles of citation:

1. Surname N. (2021). Title of article or abstract. *Scientific Collection «InterConf»,* (84): with the Proceedings of the 5th International Scientific and Practical Conference «Theory and Practice of Science: Key Aspects» (November 7-8, 2021) at Rome, Italy; pp. 21-27. Available at: https://interconf.top/...
2. Surname N. (2021). Title of article or abstract. *InterConf,* (84), 21-27. Retrieved from 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

PART I

DOI 10.51582/interconf.7-8.11.2021.042

Таченко Ілля Анатолійович
студент VI курсу, кафедра безпеки інформаційних технологій
Національний університет «Львівська Політехніка», Україна

Коробейнікова Тетяна Іванівна
кандидат технічних наук, доцент, доцент кафедри безпеки інформаційних технологій
Національний університет «Львівська політехніка», Україна

Захарченко Сергій Михайлович
кандидат технічних наук, доцент, доцент кафедри обчислювальної техніки
Вінницький національний технічний університет, Україна

ОГЛЯД СУЧАСНОГО СТАНУ ПИТАННЯ В ГАЛУЗІ ОЦІНЮВАННЯ РИЗИКІВ МЕРЕЖЕВОЇ БЕЗПЕКИ

Анотація. *Ця робота присвячена основним аспектам технологічного ланцюга оцінки та усунення ризиків; перегляду кроків для опису процесу знаходження вразливостей в компанії чи організації; отримання належного аналізу і впровадження контролів згідно із найкращими практиками безпеки та сучасних фреймворків.*
Ключові слова*: інформаційна безпека, ризики, аналіз, вразливості, стандарти, контроли.*

Визначення ризиків мережевої безпеки. Оцінка та управління ризиками мережевої безпеки була створена як наукова галузь приблизно 30-40 років тому. Тоді ж були розроблені принципи та методи, для розробки концепції, оцінки та управління ризиками мережевої безпеки. Ці принципи та методи досі є базовими для цієї галузі і сьогодні, але буквально протягом останньої декади було надбано чимало теоретичних напрацювань та практичних моделей та процедур. *Метою* роботи є огляд цих досягнень з особливим акцентом на нових фундаментальних ідеях та мисленні, на яких вони ґрунтуються. Автори шукають сучасні тенденції в перспективах та підходах до оцінювання ризиків мережевої безпеки, а також розглядають потенційні

галузі для подальшого розвитку сфери менеджменту ризиків мережевої безпеки, для цього пропонують авторську схему визначення та вирішення/прийняття ризиків мережевої безпеки (Рис. 1.1) [1-6].

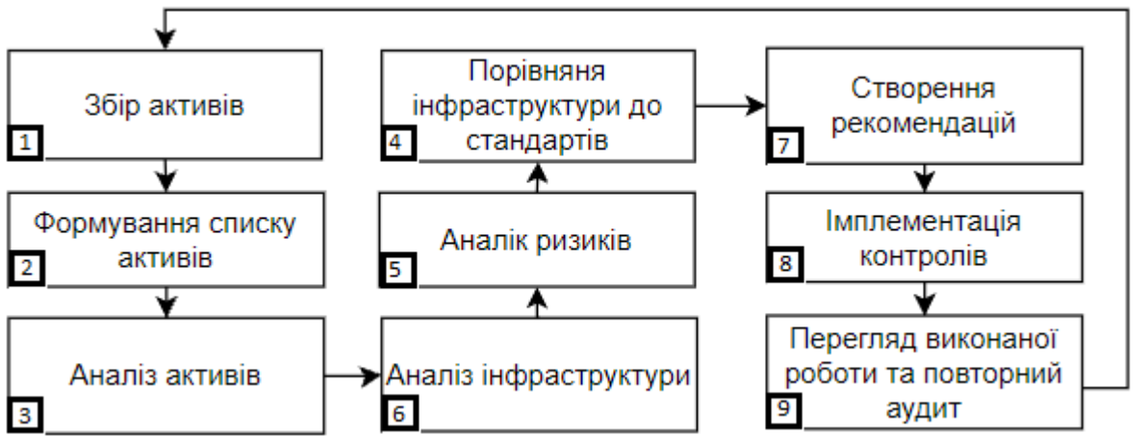

Рис.1. **Схема визначення та вирішення/прийняття ризиків мережевої безпеки**

На Рис. 1.1 зображено схему визначення та вирішення/прийняття ризиків мережевої безпеки. Пояснимо зміст кожного з етапів докладно.

1. Збір активів – це перший етап визначення компанією своїх ризиків. Щоб зрозуміти ризик, необхідно знайти найцінніші активи компанії. Часто це сервери, комунікаційні мережі та інформаційні системи, послуги, політики тощо. Персонал також зараховують до складу активів, оскільки він часто є одним із найбільш вразливих та найцінніших активів одночасно.

2. Формування списку активів – етап подальшого проходження схеми визначення та вирішення/прийняття ризиків мережевої безпеки і є важливим для більшості сертифікатів, таких як SOC та ISO [7].

Потрібно переконатися, що вся робота, яка була зроблена на першому етапі, зараз є у списку, відсортована та чітко описана.

3. Аналіз активів – передбачає сортування виявлених активів. Активи, як правило, класифікуються за трьома способами:

– Конвертованість – класифікація активів на основі того, наскільки легко їх конвертувати в готівку;

– Фізичне існування – класифікація активів на основі їх фізичного існування (іншими словами, матеріальних чи нематеріальних активів);

– Використання – класифікація активів на основі використання та/або призначення їх діяльності.

Фізичне існування та використання є двома найпоширенішими способами, їх також зазвичай об'єднують.

4. Аналіз інфраструктури вважається частиною аналізу та сортування активів, проте він важливий для того, щоб зрозуміти взаємозв'язок між активами, тому допоможе правильно класифікувати активи та відсортувати їх.

5. Аналіз ризиків – це процес виявлення та аналізу потенційних загроз, які можуть негативно вплинути на ключові бізнес-ініціативи або проекти, що містять виявлені активи.

6. Порівняння інфраструктури до стандартів (або оцінка ризиків) – це визначення потенційної шкоди від події із реалізованою загрозою, а також ймовірність того, що ця з подія із реалізованою загрозою відбудеться.

7. Створення рекомендацій – процес створення, коригування, підтримки і вдосконалення списку рекомендацій з мережевої безпеки в своїй організації. Зазвичай особа, з якою це обговорюється, є технічним директором (CTO – Chief Technical Officer – Директор з Технічних Процесів) або його еквівалентом.

8. Імплементація контролів, або впровадження засобів контролю – втілення засобів контролю у реальність. Справедливим є вплив розмірів бюджетів і команд. Іноді засоби контролю імплементуються самостійно або за допомогою DevOps-фахівців чи інженерів з безпеки; частіше – за допомогою команди служби безпеки компанії.

9. Перегляд виконаної роботи та повторний аудит. Огляд та санація аудиту є останнім кроком схеми визначення та вирішення/прийняття ризиків мережевої безпеки. Необхідно впевнитися в коректній реалізації всіх елементів керування і налаштуваннях інструментів. Через деякий час рекомендується повторити процеси огляду та санації з метою безперервного оновлення інфраструктури організації.

Управління ризиками мережевої безпеки. Полягає у збалансуванні та зменшенні потенційного впливу від різних загроз, для наприклад, зростання прибутку, безпеки, репутації тощо [8-9]. Загалом тут розглядається набір альтернатив, оцінка їх плюсів та мінусів. Управління ризиками мережевої безпеки передбачає прийняття рішень, які найкращим чином відповідають цінностям та пріоритетам decision-maker'а (особи, що приймає рішення). У процесах управління ризиками мережевої безпеки прийнято вводити обмеження, зокрема такі, що стосуються аспектів безпеки, щоб спростити загальні судження та забезпечити певний мінімальний рівень ризиків у конкретних областях створення продукту, щоб уникнути розгляду занадто великої кількості змінних одночасно.

Оцінка ризиків та управління ризиками мережевої безпеки визнані науковою галуззю та надають важливий внесок під час прийняття рішень на практиці. Основні принципи, теорії та методи, що існують – досі розвиваються. Потенційні галузі для подальшого розвитку сфери менеджменту ризиків мережевої безпеки:

1. Галузі, пов'язані з IT;
2. Ресурсна;
3. Переробна;
4. Енергетична.

Аналіз літературних джерел під час огляду сучасного стану питання в галузі оцінювання ризиків мережевої безпеки дозволив запропонувати такі проміжні висновки:

– Наукове підґрунтя оцінки ризиків мережевої безпеки та управління ризиками є досі хитким. Причина у тому, що теоретична робота і практика опираються на неточні вхідні дані, які можуть впливати і впливають на кінцеві рішення;

– Досвід та практичні ситуації з практики аудиторів містять загальне (неточне) уявлення про ризики як очікувану кількісну величину або розподіл ймовірностей;

– Нині є достатньо немало спроб інтегративних досліджень, які

встановлюють ширші погляди на концептуалізацію, оцінювання та управління ризиками мережевої безпеки. Автори вважають цей спосіб мислення важливим для розвитку галузі оцінювання ризиків мережевої безпеки та отримання потужної уніфікуючої наукової платформи.

Базові фреймворки для визначення проблемних місць в мережевій безпеці та безпеці всередині організації.

Міжнародний фреймворк ISO 27001(27002/27701). Фреймворк з кібербезпеки ISO 27001 складається з міжнародних стандартів, які надають вимоги до управління системами управління інформаційною безпекою (ISMS – Information Security Management System – Система з Менеджменту Інформаційної Безпеки) [10]. ISO 27001 розглядає процес, що ґрунтується на оцінці ризиків, який вимагає від підприємств вжити заходів для виявлення загроз безпеці, які впливають на їх інформаційні системи.

Для усунення виявлених загроз стандарти ISO 27001 рекомендують різні засоби контролю. Організація повинна вибрати належний елемент керування, який може зменшити ризики безпеки, щоб гарантувати, що мережа залишається захищеною від атак. Загалом ISO 27001 складається із 114 елементів керування, які формують 14 категорій. Деякі категорії містять політики інформаційної безпеки, що містять 2 елементи керування: 1) захист інформації з 7 елементами контролю, які деталізують відповідальність за виконання різних завдань; 2) категорія безпеки людських ресурсів із 6 елементами управління, які дозволяють працівникам усвідомити свою відповідальність за участь в інформаційній безпеці.

З іншого боку, фреймворк ISO 27002 містить міжнародні стандарти, які детально описують засоби управління, які організація повинна використовувати для управління безпекою інформаційних систем. ISO 27002 призначений для використання разом з ISO 27001, і більшість організацій використовують обидва, щоб продемонструвати свою схильність до дотримання різних вимог, що вимагаються різними нормативними актами. Деякі з засобів захисту інформаційної безпеки, рекомендовані у стандарті ISO 27002, включають політики для підвищення інформаційної безпеки, такі

елементи, як інвентаризація активів для управління IT-активами, засоби контролю доступу для різних бізнес-вимог, управління доступом користувачів та контроль безпеки операцій.

Основною метою ISO 27001 є захист 3 аспектів інформації:

1. Конфіденційність: лише уповноважені особи мають право на доступ до інформації;

2. Цілісність: змінити інформацію можуть лише уповноважені особи;

3. Доступність: інформація повинна бути доступною для авторизованих осіб, коли це необхідно.

Система управління інформаційою безпекою. Система управління інформаційною безпекою (ISMS – Information Security Management System) - це набір правил, які компанія повинна встановити, щоб [10]:

– визначити зацікавлених сторін та їх очікування від компанії з точки зору інформаційної безпеки;

– визначити, які ризики існують для інформації;

– визначити засоби контролю (запобіжні заходи) та інші методи пом'якшення, щоб відповідати визначеним очікуванням та впоратися з ризиками;

– поставити чіткі цілі щодо того, чого необхідно досягти з інформаційною безпекою;

– впроваджувати всі засоби контролю та інші методи зменшення/послаблення ризиків;

– безперервно вимірювати, чи впроваджені засоби керування працюють належним чином;

– постійно вдосконалюватись, щоб покращити роботу всієї СУБД.

Цей набір правил може бути записаний у вигляді політики, процедур та інших типів документів, або він може бути у формі встановлених процесів та технологій, які не задокументовані. ISO 27001 визначає, які документи потрібні як мінімум. Навіщо потрібна ISMS? Існує чотири основні бізнес-переваги, яких компанія може досягти, впровадивши цей стандарт інформаційної безпеки:

– Дотримання законодавчих вимог;

– Досягнення конкурентних;

– Низькі витрати;

– Краща організація.

Також варто не забувати про доповнення до ISO 27001 – ISO 27701 [11]. ISO/IEC 27701 допоможе вам керувати особистою інформацією (PII) у вашій організації. Це новий стандарт, розроблений для використання будь -якою особою, відповідальною за особисту інформацію у будь-якій організації. Стандарт показує вам, як розробляти, налаштовувати, керувати та постійно вдосконалювати Систему управління інформацією про конфіденційність (PIMS). Це дає вам велику гнучкість у створенні та роботі з вашим PIMS. Гнучкість стандарту ISO 27701 допоможе дотримуватися багатьох відповідних місцевих правил щодо особистої інформації.

Міжнародний фреймворк CISv8. Контроль CIS (Center of Internet Security – Центр Безпеки Інтернету, раніше відомий як критичний контроль безпеки) - це рекомендований набір дій для кіберзахисту, які забезпечують конкретні та дієві способи припинення найпоширеніших і небезпечних атак сьогодні. SANS (SysAdmin, Audit, Network, and Security) підтримує засоби контролю CIS шляхом навчання, досліджень та сертифікації. 18 травня 2021 року СНД запустила версію 8 елементів керування, опубліковану на глобальній конференції RSA 2021 року.

CIS Controls v8 була вдосконалена, щоб не відставати від сучасних систем та програмного забезпечення. Перехід до хмарних обчислень, віртуалізація, мобільність, аутсорсинг, робота від дому та зміна тактики зловмисників викликали оновлення та підтримують безпеку підприємства під час їх переходу як до повністю хмарних, так і до гібридних середовищ.

Список контролів для CISv8 фреймворку:

– CIS Control 1: Inventory and Control of Enterprise Assets – Інвентаризація і контроль Бізнес Активів;

– CIS Control 2: Inventory and Control of Software Assets - Інвентаризація і контроль Активів Програмного Забезпечення;

– CIS Control 3: Data Protection – Захист даних;

– CIS Control 4: Secure Configuration of Enterprise Assets and Software – Безпечна конфігурація бізнес і програмних активів;

– CIS Control 5: Account Management – керування аккаунтами;

– CIS Control 6: Access Control Management – керування доступами;

– CIS Control 7: Continuous Vulnerability Management – постійний менеджмент вразливостей;

– CIS Control 8: Audit Log Management;

– CIS Control 9: Email Web Browser and Protection;

– CIS Control 10: Malware Defense – захист від шкідливого програмного забезпечення;

– CIS Control 11: Data Recovery – Відновлення даних;

– CIS Control 12: Network Infrastructure Management – Керування мережевою інфраструктурою;

– CIS Control 13: Network Monitoring and Defense – Моніторинг і захист мережі;

– CIS Control 14: Security Awareness and Skills Training –Підготовка до розуміння безпеки;

– CIS Control 15: Service Provider Management – менеджмент сервіс провайдерів;

– CIS Control 16: Application Software Security – захист програмного забезпечення;

– CIS Control 17: Incident Response Management – Відповідь на інциденти;

CIS Control 18: Penetration Testing – тестування на проникнення.Групи впровадження (IG – Implementation Groups – групи впровадження) є рекомендованим для визначення пріоритетності впровадження засобів контролю СНД. Прагнучи допомогти підприємствам будь-якого розміру, IG поділяються на три групи. Вони базуються на профілі ризику та ресурсах, якими володіє підприємство для впровадження засобів контролю СНД. Кожна IG визначає набір запобіжних заходів (раніше їх називали підконтролем CIS),

які вони повинні впроваджувати. Всього в CIS Controls v8 153 запобіжні заходи. Кожне підприємство має починатися з IG1. IG1 визначається як «основна кібергігієна», основоположний набір засобів захисту від кіберзахисту, які кожне підприємство повинно застосовувати для захисту від найпоширеніших атак. IG2 базується на IG1, а IG3 складається з усіх елементів управління та запобіжних заходів.

Міжнародний фреймворк SOC 2. Американський інститут сертифікованих бухгалтерів (AICPA) розробив основу SOC 2. Мета фреймворку - дозволити організаціям, які збирають та зберігають особисту інформацію про клієнтів у хмарних сервісах, підтримувати належну безпеку [12]. Фреймворк також надає компаніям SaaS вказівки та вимоги щодо зменшення ризиків порушення даних та посилення їх позицій у сфері кібербезпеки. Крім того, фреймворк SOC 2 деталізує вимоги безпеки, яким повинні відповідати постачальники та треті сторони. Вимоги керують ними при проведенні аналізу зовнішніх та внутрішніх загроз для виявлення потенційних загроз кібербезпеки.

SOC 2 містить 61 вимогу відповідності, що робить його однією з найскладніших систем для впровадження. Вимоги включають керівні принципи щодо знищення конфіденційної інформації, системи моніторингу аномалій безпеки, процедури реагування на події безпеки, вказівки щодо внутрішнього спілкування тощо.

Таким чином, звіти SOC 2 призначені для задоволення потреб широкого кола користувачів, які потребують детальної інформації та впевненості щодо засобів управління в сервісній організації, що мають відношення до безпеки, доступності та цілісності обробки систем, які сервісна організація використовує для обробки даних користувачів та конфіденційність інформації, що обробляється цими системами. Таким чином, звіти SOC 2 відіграють важливу роль у нагляді за організацією, програмах управління постачальниками, корпоративному управлінні та процесах управління ризиками, нагляді за дотриманням нормативних актів тощо.

Щодо критеріїв довірчих послуг (TSP – Trust Service Criteria), варто

звернути увагу на таке: TSP – це критерії контролю для використання в атестаційних або консультаційних завданнях для оцінки та звітування про контроль над інформацією та інфраструктурою підприємства:

– у всьому суб'єкті;

– на рівні дочірнього підприємства, підрозділу або операційного підрозділу;

– у межах функції, що стосується оперативних цілей, звітності чи цілей відповідності;

– щодо певного типу інформації, що використовується суб'єктом господарювання.

TSP класифікуються на такі категорії:

– Безпека. Інформація та системи захищені від несанкціонованого доступу, несанкціонованого розкриття інформації та пошкодження систем, які можуть поставити під загрозу доступність, цілісність, конфіденційність та конфіденційність інформації чи систем та вплинути на здатність організації досягати своїх цілей.

– Доступність. Інформація та системи доступні для роботи та використання для досягнення цілей суб'єкта господарювання.

– Цілісність обробки. Обробка системи є повною, дійсною, точною, своєчасною та уповноваженою на досягнення цілей організації.

– Конфіденційність. Інформація, визначена як конфіденційна, захищена для досягнення цілей організації.

– Приватність. Персональна інформація збирається, використовується, зберігається, розкривається та розпоряджається тільки для досягнення цілей організації.

Організація мережевої безпеки. Управління мобільними пристроями (MDM – Mobile Device Management – Керування Мобільними пристроями) – це система підвищення корпоративної безпеки даних шляхом моніторингу, управління та захисту мобільних пристроїв, таких як ноутбуки, смартфони та планшети, які використовуються на підприємствах [8-9, 13]. Рішення для керування мобільними пристроями дозволяють IT-командам та

адміністраторам контролювати та поширювати політику безпеки на мобільних пристроях, які отримують доступ до конфіденційних корпоративних даних у своїх організаціях, забезпечуючи безпеку корпоративної мережі. Оскільки все більше і більше співробітників використовують один або всі ці пристрої, організації всіх форм і розмірів тепер звертаються до управління мобільними пристроями для підвищення безпеки даних і мережі та підвищення продуктивності співробітників. Рішення MDM дозволяють IT-адміністраторам налаштовувати корпоративні політики безпеки на мобільних пристроях.

EDR (Endpoint Detection and Response – Моніторинг та Відповідь на Кінцевих Пристроях) може виявляти загрози, які існують у вашому мережному середовищі, а потім реагувати на них. Він може проаналізувати характер загрози та надати вашій IT-команді інформацію про те, як вона була ініційована, які частини вашої мережі вона атакувала, що вона зараз робить і як зупинити атаку взагалі. Рішення EDR ще більше захищає вашу мережу, стримуючи загрозу та не даючи її поширенню. EDR може захистити вашу організацію від загроз, незалежно від того, чи використовуєте ви повністю вбудовану систему, чи хмарну платформу. З повним розумінням EDR і як це може зміцнити ваші заходи безпеки, ви можете вибрати найкращий EDR для вашої мережі. Використання EDR може підвищити безпеку як пристроїв, підключених до мережі, так і загальної інформаційної системи.

Визначення критичних активів для подальшого аналізу ризиків. Критичні активи визначаються частково суб’єктивно, а частково із використанням різних технік [14]. Можна виділити декілька критеріїв для визначення критичних активів:

1) Цінність та ліквідність самого активу (в процентному відношенні до інших активів);

2) Чи має усунення цієї ланки системи якийсь вплив на функціонування самої системи (кількість годин, яку може функціонувати система без цього елементу);

3) Чи цей актив зберігає в собі якусь інформацію, розголошення якої не

може відбутись. (кількість коштів, які будуть втрачені через репутаційні втрати та позови від клієнта).

Після цього вже можна приступати до оцінки критичності ризиків, які пов'язані з даним активом. Досить популярною є матриця оцінки ризиків, зображена у вигляді таблиці 1.1, яка працює за принципом:

1) Спочатку оцінюємо наскільки часто може трапитись інцидент;

2) Оцінюємо, яку шкоду для організації може складати знищення/захоплення/призупинення роботи певного активу (за шкалою від 1 до 5);

3) Показники перемножуються, і порівнюються із матрицею нижче. І, вже відповідно з цього ми і дізнаємось, які ризики для нас важливіші, і що потрібно виправляти першим, а що може зачекати.

Таблиця 1

Матриця оцінки ризиків для окремого активу

Частота / Величина шкоди, яка може бути завдана	1 – Дуже рідко	2 – Рідко	3 – Можливо	4 – Дуже можливо	5 – Скоріше всього станеться
5 - Критична	5	10	15	20	25
4 – Велика	4	8	12	16	20
3 – Середня	3	6	9	12	15
2 – Невелика	2	4	6	8	10
1 – Незначна	1	2	3	4	5

Наприклад – крадіжка ноутбука працівника. При правильній імплементації контролів доступу, частота таких крадіжок є рідкістю, але якщо на цьому ноутбуці були якісь важливі дані, або збережені паролі до систем, які можуть спинити роботу бізнесу, це може призвести до втрат великого розміру. Тобто частота – 2, величина шкоди – 4. Перемножимо ці значення, отримаємо 8. Це означає, що попередньо наведений ризик помаранчевого рівня, який є одним із чотирьох видів ризику:

– Зелений – ризик незначний, і скоріше всього не станеться;

– Жовтий – ризик не є надто високим, або ймовірність того, що він станеться дуже низька4;

– Помаранчевий – ризик є високим, його потрібно вирішувати, якщо нема критичних ризиків;

– Червоний – ризик є критичним його потрібно негайно вирішувати.

Спосіб розроблення загальних метрик. Розробка метрик є значущим фактором вимірювання рівня безпеки, особливо під час демонстрації керівництву компанії. Автори пропонують такий *спосіб* на основі проведеного аналізу та проміжних висновків:

1. На початковому етапі знаходим *N* основних ризиків (ми пропонуємо, *N=4*, і зауважимо, що для точності потрібна однакова кількість ризиків для кожного активу);

2. На другому етапі, ми знайшли конкретних *N=4* ризиків для активу, оцінили їх за табл. 1 у *12, 8, 6*, і *3* бали відповідно. Фіксуємо, що виник певний "рівень небезпеки";

3. На третьому етапі знаходимо рівень безпеки. Кожне із цих чисел (балів) потрібно віддзеркалити відносно центрального елементу (дев'ятки) згідно табл.1. Таким чином маємо *12* небезпек = *6* безпек, *8* небезпек = *8* безпек, *6* небезпек = *12* безпек і *3* небезпеки = *15* безпек. Отримаємо *6 + 8 + 12 + 15 = 31* бал. Це зафіксований рівень безпеки. Так, як максимальний рівень є *25 * 4 = 100*, то *31:100 = 31%*. Це і буде загальний рівень безпеки для одного активу.

4. На останньому етапі потрібно за таким же алгоритмом обрахувати такий же показник для кожного активу та їх середнє значення. Це буде рівень безпеки на даний момент часу.

Висновки та оцінювання ризиків і стану безпеки в організації. Отже, сформуємо етапи оцінювання ризиків і стану безпеки в організації, базуючись на запропонованому авторами способі:

1. На початковому етапі це є оцінювання ризиків мережевої безпеки необхідно охарактеризувати організацію, та визначити рід її діяльності;

2. Визначення загального переліку активів;

3. Визначення критичних активів із загального переліку активів та надання їм окремого статусу;

4. Після цього, необхідно провести стартовий аудит ризиків мережевої безпеки та розглянути можливі ризики для кожного активу (починаючи із критичних активів). Гарним рішенням було б вибрати по 4 основні ризики (можна менше). Це необхідно для оцінки стану безпеки у відсотковому відношенні;

5. Після знаходження цих ризиків, потрібно їх оцінити за допомогою наведеної вище матриці ризиків. Оцінювання допоможе їх посортувати для полегшення подальшої діяльності;

6. Далі, за допомогою способу, який був описаний вище, оцінити рівень безпеки в організації;

7. Скласти рекомендації щодо, як уникнення/прийняття окремих ризиків. Якщо ризик приймається, то оцінити розмір ймовірних затрат (втрат);

8. Скласти рекомендації щодо оцінювання ризиків мережевої безпеки, та запропонувати їх керівництву. Таким чином, отримаємо початковий аудит, в якому рекомендації аудитора були прийняті до уваги та імплементовані. Різниця (у %) між теперішнім станом безпеки та тим, який може з'явитися – стане рівнем безпеки, на який підніметься компанія якщо втілить запропоновані рекомендації;

9. Впровадити контроли, які були визначені керівництвом як необхідні;

10. За результатами впровадження мережевої безпеки, запропонованої керівництву, виконати повторний аудит ризиків мережевої безпеки для даного підприємства і оцінити рівень безпеки у за допомогою вже згаданого методу. Зробити порівняльний аналіз;

11. У випадку якщо прогнозований рівень безпеки менший за реальний рівень після повторного аудиту, тоді план був виконаний кращим, проте оцінювання ризиків було не зовсім точним. Це потрібно врахувати під час наступного оцінювання ризиків;

12. У випадку якщо прогнозований рівень безпеки більший за реальний після повторного аудиту, тоді план визнається не виконаним до кінця.

Потрібно провести аналіз того, що не було виконано, а також, вияснити причини та врахувати під час наступного оцінювання ризиків.

Список джерел:

1. Tachenko I. The basic aspects of assessment and risk remediation technological chain / I. Tachenko, T. Korobeinikova // "Information protection and information systems security": Materials of VIII-th International Scientific and Technical Conference, November 11 – 12, 2021. – Lviv: NULP, 2021 – C. 17-19.
2. Big Data Processing: methods, models and information technologies: monograph. – edited by Oleg I. Pursky. – Shoida GmBH, Steyr, Austria, 2019. – 234 p. ISBN 978-3-953794-29-8.
3. Рівень розвитку техніки і технологій в XXI столітті. Частина 1: Серія монографій / [авт.кол. : М.В. Князєва, В.М. Крамар, І.Я. Львович, А.П. Преображенський, О.Н. Романюк і ін.]. - Одеса: КУПРІЄНКО СВ, 2019 - 227 с. : іл., табл. - (Серія «Рівень розвитку техніки і технологій в XXI столітті», Частина 1) ISBN 978-617-7414-75-8.
4. Wissenschaft für den modernen Menschen 2021 / Science for modern man 2021. – Innovative engineering and technology, informatics, security systems, transport development, architecture. – Book 4. Part 4. : monograph. – ScientificWorld-NetAkhatAV Lußstr 13, Karlsruhe, Germany, 2021 – 236 p. ISBN 978-3-949059-12-4 DOI: 10.30890/2709-2313.2021-04-04.
5. На шляху до Індустрії 4.0: інформаційні технології, моделювання, штучний інтелект, автоматизація : монографія / кол. авт. : В. Б. Артеменко, Л. В. Артеменко, О. В. Артеменко [та ін.]; за заг. ред. С. В. Котлика. — Одеса : Астропринт, 2021. — 544 с. ISBN 978–966–927–702–2.
6. Intellectual capital is the foundation of innovative development: engineering, computer science, safety, transport, physics and mathematics, biology and ecology, agriculture. Monographic series «European Science». Book 6. Part 4. 2021. ISBN 978-3-949059-32-2 DOI: 10.30890/2709-2313.2021-06-04.
7. The official website of the ISO standards [Electronic resource] // www.iso.org. - 2021. Режим доступу: https://www.iso.org/isoiec-27001-information-security.html - ISO standards.
8. Трояновська Т. І. Побудова захищених мереж на базі обладнання компанії Cisco. // Захарченко С.М., Трояновська Т. І., Бойко О.В. Навчальний посібник. Вінниця : ВНТУ, 2017. – 133 с.
9. Технології захисту локальних мереж на основі обладнання CISCO : навч. посібник / Т. І. Коробейнікова, С. М. Захарченко. – Львів: Видавництво Львівської політехніки, 2021. – 188 с.

10. Information Security Management System SaaS For ISO 27001 [Ел. ресурс] // Alliantist Ltd. – 2021. – Режим доступу: https://www.isms.online/information-security-management-system-isms/.
11. ISMS [Ел. ресурс] // Alliantist Ltd. – 2021. – Режим доступу: https://www.isms.online/information-security-management-system-isms/.
12. ISO/IEC 27701:2019 Security techniques — Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management — Requirements and guidelines [Ел. ресурс] // International Organization for Standardization. – 2019. – Режим доступу: https://www.iso.org/standard/71670.html.
13. What is MDM [Ел. ресурс] // Zoho Corp. – 2021. – Режим доступу: https://www.manageengine.com/mobile-device-management/what-is-mdm.html.
14. Risk analysis. [Electronic resource] // www.project-risk-manager.com/. - 2021. - Resource access mode: https://www.project-risk-manager.com/blog/qualitative-and-quantitative-risk-analysis/.