МІНІСТЕРСТВО ВНУТРІШНІХ СПРАВ УКРАЇНИ
ХАРКІВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ
ВНУТРІШНІХ СПРАВ

Кафедра протидії кіберзлочинності, факультет № 4

МЕТОДИЧНІ РЕКОМЕНДАЦІЇ ДЛЯ ПІДГОТОВКИ ДО ЛАБОРАТОРНИХ ЗАНЯТЬ

з навчальної дисципліни **«Аудит безпеки комп'ютерних систем та мереж»**
вибіркових компонент
освітньої програми *першого (бакалаврського)* рівня вищої освіти
125 «Кібербезпека» (Поліцейські)

Харків 2024

ЗАТВЕРДЖЕНО
Науково-методичною радою
Харківського національного
університету внутрішніх справ
Протокол від 29.01.2024 № 1

СХВАЛЕНО
Вченою радою факультету № 4
Протокол від 17.01.2024 № 1

ПОГОДЖЕНО
Секцією Науково-методичної ради
ХНУВС з технічних дисциплін
Протокол від 26.01.2024 № 1

Розглянуто на засіданні кафедри протидії кіберзлочинності.
Протокол від 10.01.2024 № 1

Розробник:
викладач кафедри протидії кіберзлочинності Калякін С.В.

Рецензенти:
завідувач кафедри інформаційних управляючих систем ХНУРЕ, д.т.н., професор Петров К.Е.;
доцент кафедри кібербезпеки та DATA-технологій факультету №6 ХНУВС, к.т.н., доцент Тулупов В.В.

1. Загальні положення

Форми проведення занять

Програмні результати навчання за навчальною дисципліною «Кримінальна розвідка у кіберсфері» формуються за допомогою лабораторних занять, проведення яких поєднується із самостійною роботою.

Лабораторні заняття проводяться з основних, найбільш складних тем навчальної дисципліни.

Метою лабораторних занять є: перевірка, поглиблення і закріплення теоретичних знань отриманих здобувачами та здобувачками вищої освіти на лекціях і під час самостійних занять, надання допомоги в самостійному оволодінні матеріалом, вдосконалення навичок усної подачі матеріалів, ведення полеміки.

Участь здобувачів та здобувачок вищої освіти у лабораторних заняттях є обов'язковою умовою успішного виконання навчального плану. Якщо здобувач/здобувачка вищої освіти з яких-небудь поважних причин не змогли бути присутнім/присутньою на лабораторному занятті, він/вона зобов'язаний/зобов'язана провести індивідуальну співбесіду з викладачем за пропущеною темою та її відпрацювати.

Підготовку до заняття варто починати з вивчення вимог навчально-методичних матеріалів.

Для підготовки до занять здобувачі і здобувачки вищої освіти повинні використовувати рекомендовану літературу, яка знаходиться у бібліотечному фонді університету та у кафедральному літературному фонді. Також допускається використання інформації з мережі Інтернет, з зазначенням певного режиму доступу (адреси).

План лабораторних занять з навчальної дисципліни

Тема	Форма діяльності (заняття) / форматпроведення	Години
Тема № 1. Загальний підхід до управління ризиками ІБ	лабораторна робота / очно	4
Тема № 2. Загальна оцінка та обробка ризиків інформаційної безпеки.	лабораторна робота / очно	4
Тема № 3. Міжнародні стандарти в галузі аналізу та оцінювання ризиків	лабораторна робота / очно	4
Тема № 4. Засоби аналізу та оцінювання ризиків	лабораторна робота / очно	8

Критерії оцінювання під час проведення занять

Контрольні заходи оцінювання результатів навчання включають в себе поточний та підсумковий контролі.

Засобами оцінювання результатів навчання можуть бути екзамени (комплексні екзамени); тести; наскрізні проекти; командні проекти; аналітичні звіти, реферати, есе; розрахункові та розрахунково-графічні роботи; презентації результатів виконаних завдань та досліджень; завдання на лабораторному обладнанні, тренажерах, реальних об'єктах тощо; інші види індивідуальних та групових завдань.

Поточний контроль. До форм поточного контролю належить оцінювання:

- рівня знань під час семінарських, практичних, лабораторних занять;
- якості виконання самостійної роботи.

Поточний контроль здійснюється під час проведення семінарських, практичних та лабораторних занять і має на меті перевірку набутих здобувачем вищої освіти (далі – здобувач) знань, умінь та інших компетентностей з навчальної дисципліни.

У ході поточного контролю проводиться систематичний вимір приросту знань, їх корекція. Результати поточного контролю заносяться викладачем до журналів обліку роботи академічної групи за національної системою оцінювання («відмінно», «добре», «задовільно», «незадовільно»).

Оцінки за самостійну роботу виставляються в журналі обліку роботи академічної групи окремою графою за національною системою оцінювання («відмінно», «добре», «задовільно», «незадовільно»). Результати цієї роботи враховуються під час виставлення підсумкових оцінок.

При розрахунку успішності здобувачів враховуються такі види робіт: навчальні заняття (семінарські, практичні, лабораторні тощо); самостійна робота (виконання домашніх завдань, ведення конспектів першоджерел та робочих зошитів, виконання розрахункових завдань, підготовка рефератів, наукових робіт, публікацій, розроблення спеціальних технічних пристроїв і приладів, моделей, комп’ютерних програм, виступи на наукових конференціях, семінарах та інше); контрольні роботи (виконання тестів, контрольних робіт у формі, передбаченій в робочою програмою навчальної дисципліни). Вони оцінюються за національною системою оцінювання («відмінно», «добре», «задовільно», «незадовільно»).

Здобувач, який отримав оцінку «незадовільно» за навчальні заняття або самостійну роботу, зобов’язаний перескласти її.

Загальна кількість балів (оцінка), отримана здобувачем за семестр перед підсумковим контролем, розраховується як середньоарифметичне значення з оцінок за навчальні заняття та самостійну роботу, та для переводу до 100-бальної системи помножується на коефіцієнт **10**.

$$\textit{Загальна кількість балів (перед підсумковим контролем)} = (\ \textit{Результат навчальних занять за семестр} + \textit{Результат самостійної роботи за семестр}\ ) / 2 \ ) * 10$$

Підсумковий контроль. Підсумковий контроль проводиться з метою оцінки результатів навчання на певному ступені вищої освіти або на окремих

його завершених етапах.

Для обліку результатів підсумкового контролю використовується поточно-накопичувальна інформація, яка реєструються в журналах обліку роботи академічної групи. Результати підсумкового контролю з дисциплін відображуються у відомостях обліку успішності, навчальних картках здобувачів, залікових книжках. ***Присутність здобувачів на проведенні підсумкового контролю (заліку, екзамену) обов'язкова.*** Якщо здобувач вищої освіти не з'явився на підсумковий контроль (залік, екзамен), то науково-педагогічний працівник ставить у відомість обліку успішності відмітку «не з'явився».

Підсумковий контроль (екзамен, залік) оцінюється за національною шкалою. Для переводу результатів, набраних на підсумковому контролі, з національної системи оцінювання в 100-бальну вводиться коефіцієнт **10**, таким чином максимальна кількість балів на підсумковому контролі (екзамені, заліку), які використовуються при розрахунку успішності здобувачів, становить **50.**

Підсумкові бали з навчальної дисципліни визначаються як сума балів, отриманих здобувачем протягом семестру, та балів, набраних на підсумковому контролі (екзамені, заліку).

$$\textit{Підсумкові бали навчальної дисципліни} = \textit{Загальна кількість балів (перед підсумковим контролем)} + \textit{Кількість балів за підсумковим контролем}$$

Здобувач вищої освіти, який під час складання підсумкового контролю (екзамен, залік) отримав незадовільну оцінку, складає його повторно. Повторне складання підсумкового екзамену чи заліку допускається не більше двох разів з кожної навчальної дисципліни: один раз – викладачеві, а другий – комісії, до складу якої входить керівник відповідної кафедри та 2-3 науково-педагогічних працівники.

Якщо дисципліна вивчається протягом двох і більше семестрів з семестровим контролем у формі екзамену чи заліку, то результат вивчення дисципліни в поточному семестрі визначається як середньоарифметичне значення балів, набраних у поточному та попередньому семестрах.

$$\textit{Підсумкові бали навчальної дисципліни} = \frac{\textit{Підсумкові бали за поточний семестр} + \textit{Підсумкові бали за попередній семестр}}{2}$$

У цьому розділі також повинні бути розроблені чіткі критерії оцінювання здобувачів вищої освіти під час поточного контролю *(робота на семінарських, практичних, лабораторних та інших аудиторних заняттях, самостійна робота, виконання індивідуальних творчих завдань)* та підсумкового контролю. Кафедра визначає вимоги до здобувачів стосовно засвоєння змісту навчальної дисципліни, а саме: кількість оцінок, яку він повинен отримати під час аудиторної роботи, самостійної роботи. Наприклад:

Робота під час навчальних Занять	**Самостійна робота**	**Підсумковий контроль**
Отримати не менше 4 позитивних оцінок	Підготувати реферат, підготувати конспект за темою самостійної роботи, виконати практичне завдання тощо	Отримати за підсумковий контроль не менше 30 балів

Шкала оцінювання: національна та ECTS

Оцінка в балах	Оцінка за національною шкалою	Оцінка за шкалою ECTS	
		Оцінка	Пояснення
97-100	Відмінно («зараховано»)	A	**«Відмінно»** – теоретичний зміст курсу засвоєний цілком, потрібні практичні навички роботи з освоєним матеріалом сформовані, усі навчальні завдання, які передбачені програмою навчання, виконані в повному обсязі, відмінна робота без помилок або з однією незначною помилкою
94-96			
90-93			
85-89	Добре («зараховано»)	B	**«Дуже добре»** – теоретичний зміст курсу засвоєний цілком, потрібні практичні навички роботи з освоєним матеріалом в основному сформовані, всі навчальні завдання, які передбачені програмою навчання, виконані, якість виконання жодного з них не оцінена мінімальним числом балів, деякі види завдань виконані з помилками, робота з декількома незначними помилками, або з однією-двома значними помилками.
80-84			
75 – 79		C	**«Добре»** – теоретичний зміст курсу освоєний **цілком**, практичні навички роботи з освоєним матеріалом **в основному** сформовані, **всі** навчальні завдання, які передбачені програмою навчання, **виконані**, якість виконання **жодного** з них **не оцінено мінімальним** числом балів, деякі види завдань виконані **з помилками,** робота з декількома незначними помилками або з однією–двома значними помилками.
70-74	Задовільно («зараховано»)	D	**«Задовільно»** – теоретичний зміст курсу засвоєний частково, але прогалини не носять істотний характер, потрібні практичні навички роботи з освоєним матеріалом в основному сформовані, більшість передбачених програмою навчання навчальних завдань виконана, деякі з виконаних завдань містять помилки, робота з трьома значними помилками
65-69			
60-64		E	**«Достатньо»** – теоретичний зміст курсу засвоєний частково, деякі практичні навички роботи не сформовані, частина передбачених програмою навчання навчальних завдань не виконана або якість виконання деяких з них оцінена числом балів, близьким до мінімального, робота, що задовольняє мінімуму критеріїв оцінки
40-59	Незадовільно («не зараховано»)	FX	**«Умовно незадовільно»** – теоретичний зміст курсу засвоєний частково, потрібні практичні навички роботи не сформовані, більшість передбачених програм навчання, навчальних завдань не виконана, або якість їхнього виконання оцінено числом балів, близьким до мінімального; при додатковій самостійній роботі над матеріалом курсу можливе підвищення якості виконання навчальних завдань (з можливістю повторного складання), робота, що потребує доробки
21-40			
1–20		F	**«Безумовно незадовільно»** – теоретичний зміст курсу не освоєний, потрібні практичні навички роботи несформовані, всі виконані навчальні завдання містять грубі помилки, додаткова самостійна робота над матеріалом курсу не приведе до значного підвищення якості виконання навчальних завдань, робота, що потребує повної переробки

2. Методичні вказівки до лабораторних занять

Тема № 3. Виявлення загроз безпеки інформаційним ресурсам.

Лабораторна робота. Побудова моделі порушника та моделі загроз в інформаційній системі.

Навчальна мета заняття: навчитись аналізувати середовища функціонування інформаційної системи об'єкта захисту, будувати модель загроз та модель порушника.

Час проведення: 4 год. Місце проведення: комп'ютерний клас.

Устаткування: персональний комп'ютер (ПК) зі встановленою операційною системою Windows 7 або вище та доступом до мережі «Інтернет», програма Microsoft SDL Threat Modeling Tool (https://www.microsoft.com/en-us/securityengineering/sdl/threatmodeling)

Порядок проведення заняття

Теоретичні відомості

Модель порушника

В загальному виді модель порушника може бути наведена описово. Спочатку треба задатись категоріями користувачів, які потенційно можуть мати доступ до ресурсів інформаційної системи. Наприклад, типовий перелік категорій користувачів:

1.Адміністратори:
1.1.Адміністратор безпеки;
1.2. Адміністратор мережі;
1.3. Адміністратор криптографічної підсистеми;
1.4. Системний адміністратор;
1.5.Адміністратор баз даних.
2.Користувачі.
3.Оператори.
4.Керівники (якщо їх права відрізняються від прав користувачів).
5.Супровідники, розробники, постачальники.
6.Технічний персонал
7.Зовнішні користувачі.

Далі формується модель порушника у вигляді таблиці:

Табл.1. Модель порушника

Категорія порушника	**Кваліфікація**	**Права в системі**	**Засоби, якими володіє порушник**
Наводяться категорії потенційних порушників з числа 1-7.	Припускається високою	Опис прав користувачів відповідної категорії	Доступні порушнику засоби, які можуть бути використані для здійснення порушень

На основі переліку загроз, притаманних даній інформаційній системі формується модель загроз у вигляді таблиці:

Табл.2. Модель загроз

Загроза	**Джерело загрози**	**Мета**	**Порушник**	**Імовір-ність (за вашою думкою), P**	**Наслідки, V**	**Ризик R=P*V**
Формулюється вид загрози відповідно класифікації загроз в даній інфор-маційній системі	Наявність вразливості чи іншого фактора наявності загрози	Ресурси Інформацій-ної системи, які є метою навмисного впливу / вражаються від ненавмисного впливу	Порушник, який може виконати відповідний вплив на систему	Низька/ Середня/ Висока (<0,4/0,4-0,6/>0,6)	Незначні/ Середні/ Високі втрати (<5 тис./5-100 тис./>100 тис.)	Низький/ Середній/ Високий

Класифікація загроз може бути проведена відповідно будь-яких методик класифікації (наприклад, STRIDE).

Підходи до моделювання атак

Існує принаймні 3 загальні підходи до моделювання атак.

1. Зосереджений на атакуючому

Проводиться аналіз мети атакуючого, як він може досягти цієї мети. Цей підхід звичайно починається з розгляду точок доступу, через які може діяти атакуючий, та ресурсів, які є його метою.

2. Зосереджений на програмному забезпеченні

Software-центричне моделювання загроз (також «системоцентричне», чи «архітектуроцентричне») починає з аналізу конструкції системи, та розгляду типів атак, які можуть бути застосовані відносно кожного з елементів системи. Цей підхід використовується в моделюванні загроз в Microsoft's Security Development Lifecycle .

Для моделювання загроз, притаманних визначеним версіям ПЗ, можна користуватись існуючими переліками вразливостей, наприклад, наведених на ресурсі cvedetails.com.

3. Зосереджений на ресурсах, щодо яких здійнюються загрози

Починається з аналізу доступу до сховищ інформації, яка підлягає захисту.

При аналізі вразливостей системи слід проводити її тестування. Тестові спроби вторгень виконують на модельних зразках захищуваних даних із використанням техніки «білої скриньки» (вихідні коди програмного забезпечення, щодо якого шукаються вразливості, відомі, також відомі вхідні

дані тестів та реакція на них) чи «чорної скриньки» (відомі лише вхідні дані та реакція програмного забезпечення на них). Значна кількість вразливостей операційних систем, систем управління базами даних, веб-серверів та іншого системного забезпечення є відомою і навіть описана у відповідних RFC.

Приблизний перелік етапів, які слід здійнити при аналізі загроз:

1.Визначити вимоги щодо прикладного ПЗ:

• Ідентифікувати бізнес-цілі;

• Ідентифікувати ролі користувачів, які будуть взаємодіяти з програмним забезпеченням;

• Ідентифікувати дані, якими оперує ПЗ;

• Ідентифікувати різні випадки використання функцій ПЗ при операціях з даними під керуванням даного ПЗ.

2.Розглянути модель архітектури:

• Моделі компонентів інформаційної системи;

• Модель взаємодії компонентів інформаційної системи;

• Модель взаємодії із зовнішнім середовищем;

• Модель взаємодії ролей користувачів із компонентами та сховищами даних для кожного випадку використання.

3. Ідентифікувати будь-які загрози для конфіденційності, цілісності, доступності даних та ПЗ, засновані на матриці доступа (правилах розмежування доступа);

4. Визначити ризики безпеки, притаманні системі, та їхні наслідки. Визначити процедури по запобіганню ризикам;

5. Неперервно відновлювати модель, базуючись на поточному стані засобів та заходів захисту в інформаційній системі.

Microsoft SDL Threat Modeling Tool дозволяє визначити притаманні системі загрози відповідно класифікації STRIDE. Діаграма інформаційних потоків розподіленої системи задається за допомогою графічних елементів (рис.1). Інформація про притаманні загрози формується у виді звіту, в якому загрози класифіковані по 6 класам STRIDE (рис.2).

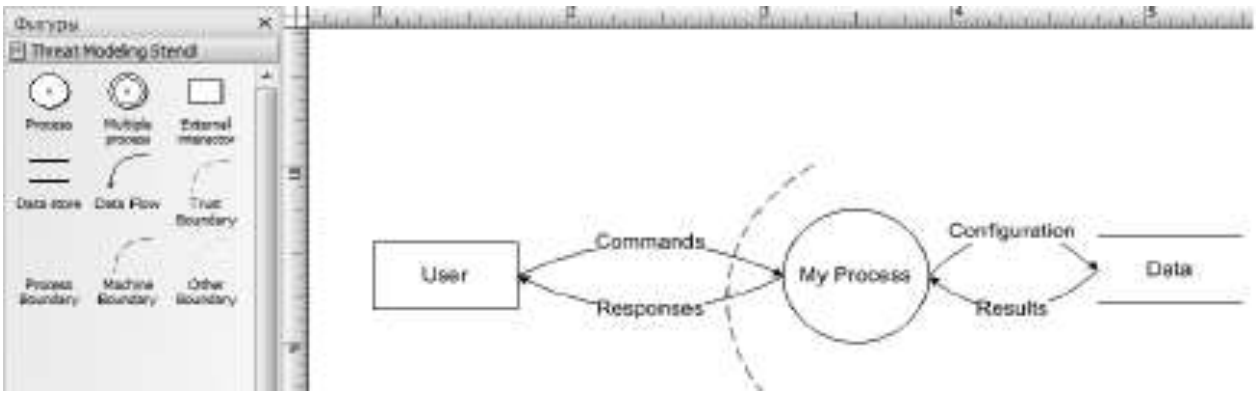


Рис.1. Елементи для побудови інформаційних потоків у системі

ID	Element Name	Element Type	Element Diagram References	Threat Type	Bug ID	Completion
3	Commands (User to ...	DataFlow	Context	Tampering		
4	Commands (User to ...	DataFlow	Context	InformationDisclosure		
5	Commands (User to ...	DataFlow	Context	DenialOfService		
9	Configuration (My Pr...	DataFlow	Context	Tampering		
10	Configuration (My Pr...	DataFlow	Context	InformationDisclosure		
11	Configuration (My Pr...	DataFlow	Context	DenialOfService		
6	Responses (My Proce...	DataFlow	Context	Tampering		
7	Responses (My Proce...	DataFlow	Context	InformationDisclosure		
8	Responses (My Proce...	DataFlow	Context	DenialOfService		
12	Results (Data to My P...	DataFlow	Context	Tampering		
13	Results (Data to My P...	DataFlow	Context	InformationDisclosure		
14	Results (Data to My P...	DataFlow	Context	DenialOfService		
21	Data	DataStore	Context	Tampering		
22	Data	DataStore	Context	Repudiation		
23	Data	DataStore	Context	InformationDisclosure		
24	Data	DataStore	Context	DenialOfService		
1	User	Interactor	Context	Spoofing		
2	User	Interactor	Context	Repudiation		
15	My Process	Process	Context	Spoofing		
16	My Process	Process	Context	Tampering		
17	My Process	Process	Context	Repudiation		
18	My Process	Process	Context	InformationDisclosure		
19	My Process	Process	Context	DenialOfService		
20	My Process	Process	Context	ElevationOfPrivilege		

Рис.2. Загрози, притаманні системі та їх класифікація

Завдання

1. Задати в інтерфейсі Microsoft SDL Threat Modeling Tool об’єкти захисту, діаграму інформаційних потоків в мережі об'єкта, який аналізується.

2. Згенерувати перелік загроз для частини системи, визначеної вимогами. Розглянути звіт, згенерований продуктом.

3. Використовуючи дані звіта, сформувати модель порушника, модель загроз для систем класу визначеного варіантом завдання.

4. Проаналізувати виявлені загрози, виконати ранжирування загроз згідно відповідних ризиків (високий, середній, низький ризик).

Перелік контрольних питань

1. Чи слід включати до моделі загроз загрози типу стихійних та технологічних лих?

2. Стосовно якої інформації, яка обробляється в ІС, повинна будуватись модель загроз: стосовно лише конфіденційної, чи стосовно відкритої та конфіденційної?

3. Які види моделей загроз існують?

4. Перелічіть основні класи загроз згідно моделі STRIDE.

5. Наведіть приклади мережних атак класу Spoofing та Denial Of Service.

Рекомендовані джерела

1. Корченко О.Г. Аудит та управління інцидентами інформаційної безпеки // О.Г. Корченко, С.О. Гнатюк, С.В. Казмірчук, В.М. Панченко, С.В.

Мельник. – К.: Центр навч.-наук. та наук.-пр. видань НА СБ України, 2014. – 193 с.

2. Менеджмент інформаційної безпеки : навчальний посібник для студентів спеціальності 125 "Кібербезпека" / О.Г. Корченко, М.Є. Шелест, С.В. Казмірчук, Ю.М. Ткач, Є.В. Іванченко. – Ніжин: ФОП Лук'яненко В.В. ТПК «Орхідея», 2019. – 408 с.

3. Бурячок В.Л., Толюпа С.В., Аносов А.О., Козачок В.А., Лукова-Чуйко Н.В. Системний аналіз та прийняття рішень в інформаційній безпеці: підручник. / В.Л. Бурячок, С.В.Толюпа, А.О. Аносов, В.А.Козачок, Н.В. Лукова-Чуйко / – К.:ДУТ, 2015. – 345 с.

Тема № 4. Оцінка ризиків для інформаційних ресурсів.

Лабораторна робота «Засіб Microsoft для оцінки ризику, пов'язаного з безпекою (MSAT)»

Навчальна мета заняття: оцінити ризики, пов'язані з безпекою за допомогою програмного засобу Microsoft Security Assessment Tool (MSAT).

Час проведення: 4 год. Місце проведення: комп'ютерний клас.

Устаткування: персональний комп'ютер (ПК) зі встановленою операційною системою Windows 7 або вище та доступом до мережі «Інтернет», Microsoft Security Assessment Tool (MSAT, https://www.microsoft.com/ru-ru/download/details.aspx?id=12273).

Порядок проведення заняття

Теоретичні відомості

Засіб Microsoft для оцінки ризику, пов'язаного з безпекою (MSAT), є програмою для оцінки ризику, яка призначена для забезпечення клієнта відомостями та рекомендаціями про передові методики, пов'язані з безпекою, в рамках інфраструктури інформаційних технологій (IT). Ця програма розроблена для організацій з кількістю настільних комп'ютерів від 50 до 500 та кількістю робітників від 100 до 1000 (Рис.1).

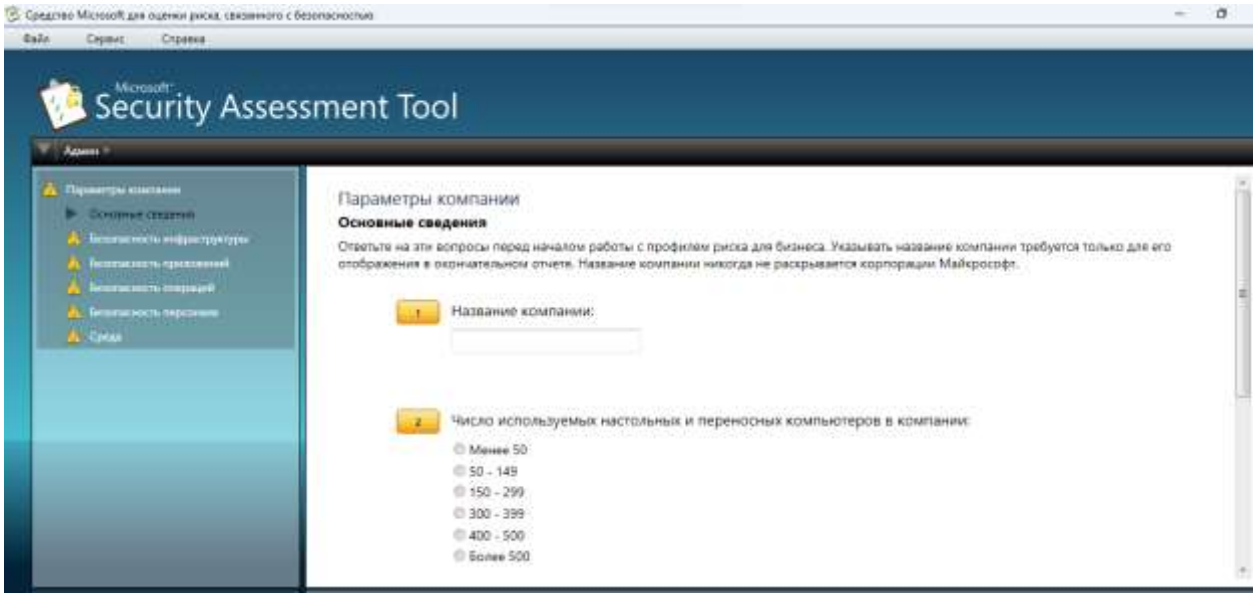


Рис.1. Інтерфейс програми MSAT.

Робота MSAT складається з двох процедур оцінки: оцінки профілю ризику для бізнесу (ПРБ) та ешелонованого захисту (DiD). У ході оцінки ПРБ визначаються ризики, з якими стикається компанія, а під час оцінки DiD

перевіряється наявність надійних методик безпеки у компанії. ПРБ необхідно виконувати лише один раз. При необхідності можна повторити цю процедуру, проте це слід робити лише в тому випадку, якщо інфраструктура компанії була значно змінена.

Щодо оцінки DiD, то її можна виконати кілька разів, щоб відстежити успіхи компанії. Кожна оцінка порівнюється з ПРБ для одержання повної картини системи безпеки. Тому оцінка може мати лише один відповідний ПРБ.

Профіль ризику для бізнесу

Для використання MSAT спочатку потрібно створити профіль. Цей профіль включає кілька основних питань щодо організації, а також повну оцінку профілю ризику для бізнесу.

Основні питання стосуються назви компанії та її розміру. Вони ніколи не розкриваються третім сторонам.

Після введення основних відомостей потрібно буде заповнити профіль ризику для бізнесу. У своїй щоденній діяльності компанія регулярно приймає технічні та ділові рішення, які можуть становити значну загрозу безпеці. Цю загрозу слід спробувати усунути. ПРБ дозволяє виявити ці небезпеки та надає базову лінію щодо якої необхідно виконувати порівняння результатів ешелонованого захисту, отримані в результаті оцінки DiD.

Оцінка ешелонованого захисту (DiD)

Перед початком оцінки DiD необхідно здійснити оцінку ПРБ. Оцінка DiD включає чотири області аналізу:

- Інфраструктура
- Програми
- Операції
- Персонал

Результати оцінки складають індекс ешелонованого захисту.

Порівняння та вивантаження результатів

Після завершення оцінки DiD можна переглянути діаграму порівняння ризику та захисту, де результати ПРБ порівнюються з результатами DiD. Щоб переглянути повний звіт, необхідно завантажити дані на захищений веб-сервер MSAT. Вивантаження буде повністю анонімним.

Окрім перегляду повного звіту, вам також буде надано доступ до функції порівняння. При цьому можна буде порівняти дві власні оцінки, щоб відстежити прогрес, що дасть змогу переглянути результати ПРБ та рівня ризику. Крім того, можна порівняти результати із результатами своїх колег.

Ця можливість порівняння результатів із результатами своїх колег дуже корисна. Вона залежить від інших користувачів, які, як і ви, вивантажують свої дані на анонімній основі.

Звіт

Повний звіт можна зберегти як MHT-файл (архів HTML, що складається з одного файлу). У цьому звіті описується стан компанії з погляду безпеки та наводяться рекомендації та передові методики в основних галузях інфраструктури, додатків, операцій та персоналу. Крім того, у звіті наводяться посилання на ресурси, які допоможуть створити безпечніше середовище.

Повторна оцінка

По мірі реалізації додаткових заходів безпеки індекс DiD компанії може змінюватись. Рекомендується періодично виконувати нову оцінку.

Завдання

1. Задати в інтерфейсі програми MSAT назву та параметри вигаданої компанії.
2. Відповісти на поставлені програмою запитання.
3. Отримати звіт.
4. Змінити параметри компанії таким чином, щоб покращити індекс DiD компанії.

Перелік контрольних питань

1. Визначення ризиків.
2. Джерела ризиків.
3. Вектори атак.
4. Оцінювання ризиків.
5. Сучасні тренди у побудові систем інформаційної бещпеки.

Рекомендовані джерела

1. Корченко О.Г. Аудит та управління інцидентами інформаційної безпеки // О.Г. Корченко, С.О. Гнатюк, С.В. Казмірчук, В.М. Панченко, С.В. Мельник. – К.: Центр навч.-наук. та наук.-пр. видань НА СБ України, 2014. – 193 с.

2. Менеджмент інформаційної безпеки : навчальний посібник для студентів спеціальності 125 "Кібербезпека" / О.Г. Корченко, М.Є. Шелест, С.В. Казмірчук, Ю.М. Ткач, Є.В. Іванченко. – Ніжин: ФОП Лук’яненко В.В. ТПК «Орхідея», 2019. – 408 с.

3. Бурячок В.Л., Толюпа С.В., Аносов А.О., Козачок В.А., Лукова-Чуйко Н.В. Системний аналіз та прийняття рішень в інформаційній безпеці: підручник. / В.Л. Бурячок, С.В.Толюпа, А.О. Аносов, В.А.Козачок, Н.В. Лукова-Чуйко / – К.:ДУТ, 2015. – 345 с.

Тема № 5. Міжнародні стандарти інформаційної безпеки

Лабораторна робота «Порівняння методик управління ризиками інформаційної безпеки»

Час проведення: 4 год. Місце проведення: комп'ютерний клас.

Устаткування: персональний комп'ютер (ПК) зі встановленою операційною системою Windows 7 або вище та доступом до мережі «Інтернет», веббраузер «Google Chrome».

Порядок проведення заняття

Теоретичні відомості

У світі інформаційних технологій та наукових досліджень поняття живучості відоме як властивість, яка характеризує здатність системи (надалі розглядатимемо бізнес-процес компанії) ефективно функціонувати за умови впливу чинників дестабілізації (ЧД): збої в роботі, руйнування, компрометація тощо та відновлювати таку здатність протягом заданого проміжку часу. Згідно з цим визначенням невід'ємною складовою властивості живучості бізнес-процесу компанії є неперервність його виконання. Міжнародний стандарт ISO 27001, який визначає вимоги до систем менеджменту інформаційної безпеки (СМІБ), тлумачить неперервність функціонування як один із рекомендованих контролів у життєвому циклі СМІБ. Отже, неперервність функціонування є не лише запорукою ефективного розроблення та впровадження СМІБ, але й дієвим способом та невід'ємною складовою процесу забезпечення властивості живучості.

За умов швидкого прогресу сучасного суспільства та високого ступеня інформатизації корпоративні мережі зв'язку (КМЗ) є основним методом збору, оброблення, зберігання та передавання інформації. Водночас, відмітимо важливість такого складового компонента КМЗ, як система захисту інформації (СЗІ), від коректності функціонування якої залежить захищеність інформаційних активів компанії. Тому наголошуємо не просто на властивості живучості організації загалом, а на забезпеченні неперервності функціонування СЗІ в КМЗ як невід'ємній та критично важливій частині ефективного та безпечного функціонування компанії, виконання її основних бізнес-процесів.

Розрізнятимемо такі основні категорії чинників дестабілізації нормальної роботи СЗІ як складової КМЗ в контексті забезпечення їхнього неперервного функціонування:

- Стихійні лиха. Порушення ІБ відбувається внаслідок впливу стихійних лих (наприклад потоп, сильний вітер, блискавка, обвал тощо), що непідконтрольні людині.
- Соціальні заворушення. Порушення ІБ, яке зумовлене нестабільністю суспільства (наприклад, акти вандалізму, терористичні акти, війни тощо).
- Фізичні пошкодження. Порушення ІБ, яке зумовлене навмисним або випадковим фізичним впливом на СЗІ або її компоненти (наприклад, вогонь, вода, електростатика, вплив навколишнього середовища (забруднення, пил,

корозія, замерзання), руйнування, крадіжка, втрата, невміле поводження з обладнанням / носієм інформації).

- Порушення ІБ через відмову базових компонентів СЗІ і послуг, що підтримують функціонування КМЗ (наприклад, відмова мережі електроживлення, системи кондиціонування повітря, системи водопостачання).

− Порушення ІБ внаслідок порушень, які зумовлені, наприклад, електромагнітним випромінюванням, коливаннями напруги, електронними завадами.

− Технічний збій. Порушення ІБ, спричинене відмовами СЗІ або пов'язаними з нею нетехнічними можливостями. До такого типу ризиків зараховуємо апаратний, програмний збій, перевантаження, порушення ремонтоздатності.

− Технічні атаки. Порушення ІБ, що зумовлене атакуванням КМЗ та використанням її уразливостей в конфігуруванні, протоколах, програмах тощо. Наприклад, мережеве сканування, експлуатація вразливості / бекдору, спроба входу, втручання, відмова в обслуговуванні (DOS / DDoS).

У роботі розглянуто процес управління ризиками ІБ в контексті забезпечення неперервності функціонування СЗІ в КМЗ як невід'ємної складової ефективної та безпечної роботи компанії.

Метою процесу управління ризиками ІБ є виявлення, контроль та мінімізація невизначеності впливу ЧД. Виділимо чотири основні етапи управління ризиками ІБ, яке здійснюється з метою забезпечення неперервності функціонування КМЗ, зокрема підсистеми СЗІ:

1. Аналіз ризику. Виявлення та оцінка ЧД, які можуть скомпрометувати ІБ важливих інформаційних активів. Дає змогу визначити профілактичні заходи щодо зниження ймовірності виникнення ЧД і визначити контрзаходи з метою успішної нейтралізації цих обмежень ще на етапі проектування.

2. Оцінка ризику. Є процесом визначення рівня ризику. Ризик традиційно обчислюватимемо як функцію важливості активів, ймовірності виникнення загрози і наявності уразливостей, величини завданого збитку.

3. Зниження ризику. Це етап, на якому реалізовуються контролі та заходи щодо запобігання визначеним ризикам, а також впроваджуються засоби відновлення у разі реалізації ризиків, що можуть порушити неперервне функціонування СЗІ.

4. Оцінка уразливостей та контролів. Аналіз основних властивостей КМЗ та виявлення тих, які можна використати з метою реалізації загрози порушення властивості живучості, а також визначення ефективності та адекватності заходів ІБ та виявлення недоліків в її реалізації.

Представимо графічне зображення життєвого циклу процесу управління ризиками ІБ в контексті забезпечення неперервності функціонування (рис. 2.1).

Проаналізуємо три найвідоміші світові методики управління ризиками ІБ, які можна застосувати для аналізу ризиків ІБ у процесі забезпечення неперервності функціонування СЗІ в КМЗ, визначимо переваги та недоліки кожної з них. Аналізу підлягають: методика оцінки NIST 800-30, методика CRAMM та методика OCTAVE.

Однією з найпопулярніших та широковживаних методик управління ризиками є методика оцінки ризиків Національного інституту стандартів і технологій США (National Institute of Standards and Technology) NIST, зазначена в Керівництві з управління ризиками в інформаційних технологіях NIST 800-30 (NIST Special Publication 800-30 Risk Management Guide for Information Technology Systems). Ця методика передбачає попереднє оцінювання двох параметрів: потенційного збитку та ймовірності реалізації загрози.

Рис. 1. Життєвий цикл процесу управління ризиками ІБ

Призначення системи управління ризиками безпосередньо пов’язане з можливістю компанії виконувати свої основні функції за умов постійного розширення сфери використання інформаційних технологій.

Методика оцінки ризиків, яка наведена в спеціальних рекомендаціях 800-30, охоплює широке коло завдань, що пов’язані зі стратегією управління ризиками і є основою для розроблення власної системи управління ризиками. Проте запропонований процес оцінювання ризику ІБ, який представлений у вигляді таблиці, що відображає залежність ризику від двох вхідних змінних: потенційного збитку і ймовірності можливого інциденту. При цьому значення кожної змінної, зокрема ризику, оцінюється за трирівневою шкалою. Такий “жорсткий” механізм отримання оцінок ризику суттєво обмежує точність результатів, забезпечуючи їх оперативність та відтворюваність.

Використання такої методики передбачає такі етапи:

− опис характеристик системи;

− ідентифікація загроз;

− ідентифікація уразливостей; аналіз наявних засобів/заходів захисту;

− визначення значення ймовірності;

− аналіз впливу;
− визначення значення ризику;
− вибір засобів/заходів захисту;
− документування отриманих результатів. Алгоритм цієї методики зображено на рис. 2.

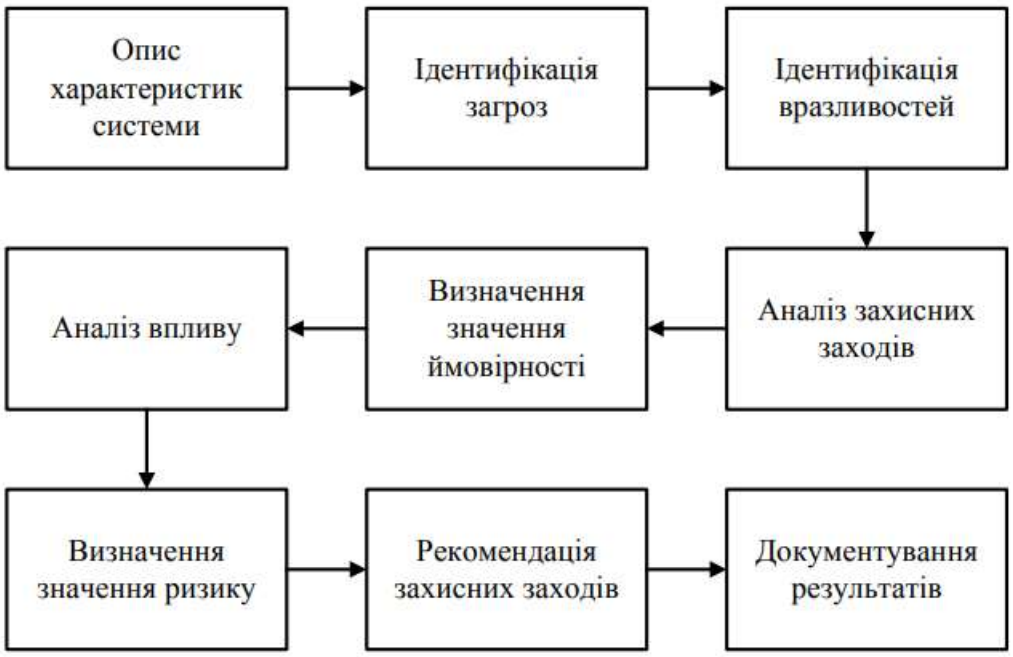


Рис. 2. Алгоритм методики управління ризиками NIST 800-30

Наступною методикою, яку потрібно проаналізувати є методика CRAMM (CCTA Risk Analysis and Managment Method), яку розробило Агентство з комп'ютерів і телекомунікацій Великобританії (Central Computer and Telecommunications Agency) за поданням Британського уряду і яка прийнята за державний стандарт. Цю методику використовують, починаючи з 1985 року, державні та комерційні організації Великобританії. За цей час CRAMM набула популярності у всьому світі. Фірма Insight Consulting Limited займається розробленням і супроводом однойменного програмного продукту, що реалізує метод CRAMM.

В основу методики CRAMM покладено комплексний підхід до оцінки ризиків, що поєднує кількісні та якісні методи аналізу. Методика є універсальною і придатна як для великих, так і для малих організацій, як державного, так і комерційного сектору. Версії програмного забезпечення CRAMM, орієнтовані на різні типи організацій, відрізняються своїми базами знань (profiles). Для комерційних організацій є комерційний профіль (Commercial Profile), для державних організацій – державний профіль (Government profile). Державний варіант профілю також дає змогу проводити
аудит на відповідність вимогам американського стандарту ITSEC ("Помаранчева книга").

Правильне використання методики CRAMM дає змогу економічно обґрунтувати витрати організації на забезпечення інформаційної безпеки та неперервності функціонування. Економічно обґрунтована стратегія управління

ризиками ІБ дає змогу, в кінцевому підсумку, заощаджувати кошти, уникаючи невиправданих витрат.

Методика CRAMM припускає поділ всієї процедури на три послідовні етапи. Завданням першого етапу є відповідь на запитання: “Чи достатньо для захисту системи застосування засобів базового рівня, що реалізують традиційні функції ІБ, чи необхідне проведення детальнішого аналізу?” Надругому етапі здійснюється ідентифікація ризиків і оцінюється їх величина. На третьому етапі вирішується завдання про вибір адекватних контрзаходів. Методика CRAMM для кожного етапу визначає набір вихідних даних, послідовність заходів, анкети для проведення інтерв’ю, списки перевірки і набір звітних документів.

Алгоритм методики CRAMM подано на рис. 3.

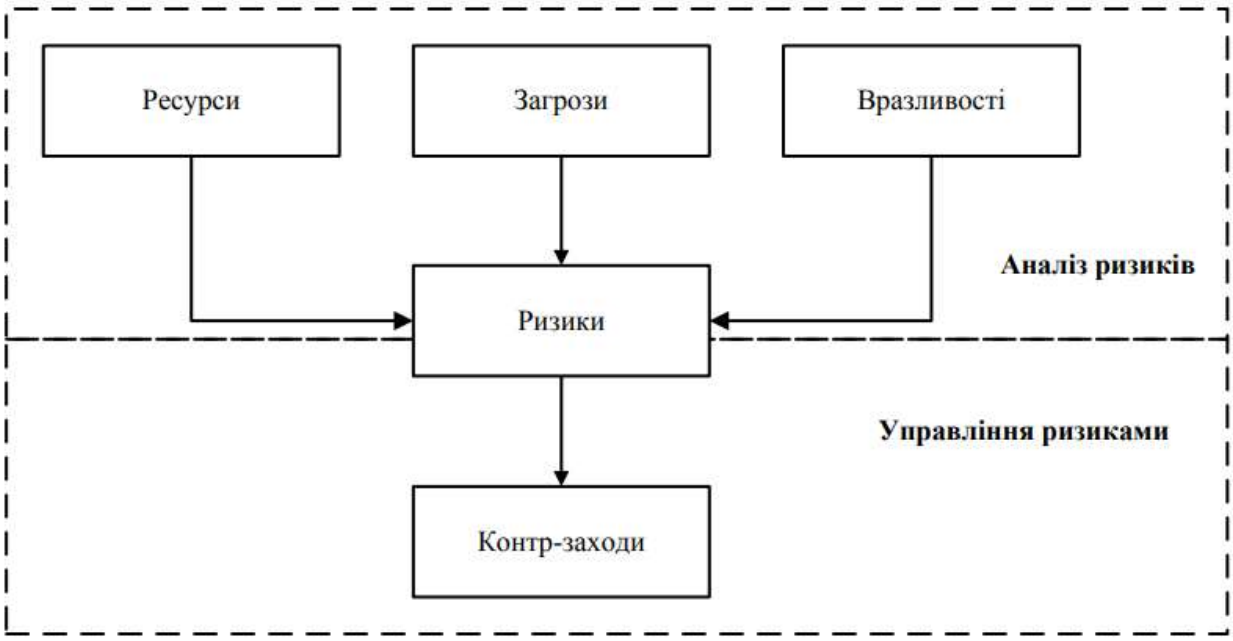


Рис. 3. Алгоритм методики управління ризиками CRAMM

Методика OCTAVE (Operationally Critical Threat, Asset and Vulnerability Evaluation) розроблена в Університеті Карнегі-Мелон (США) і передбачає оцінювання критичності загроз, активів і вразливостей.

Цю методику широко використовують у всьому світі, виконуючи роботи з оцінки ризиків ІБ та впровадження процесів управління ризиками в компанії загалом. Методика має ряд модифікацій, які розраховані на організації різного розміру та галузі діяльності.

Зміст методики OCTAVE полягає в тому, що для оцінки ризиків використовується послідовність відповідно організованих внутрішніх семінарів (workshops). Оцінка ризиків здійснюється в три етапи, яким передує набір підготовчих заходів: узгодження графіка семінарів, призначення ролей, планування, координація дій учасників проектної групи.

На першому етапі, в межах практичних семінарів, здійснюється розроблення профілів загроз, що містять в собі інвентаризацію та оцінку цінності активів, ідентифікацію застосовних вимог законодавства та нормативної бази, ідентифікацію загроз та оцінку їх ймовірності, а також визначення системи

організаційних заходів з підтримки режиму інформаційної безпеки.

На другому етапі проводиться технічний аналіз уразливостей систем організації щодо загроз, чиї профілі розроблено на попередньому етапі, який містить ідентифікацію наявних уразливостей компанії та оцінювання їх величини.

На третьому етапі виконується оцінка та оброблення ризиків інформаційної безпеки, що містить визначення величини та ймовірностізавданої шкоди внаслідок реалізації загроз ІБ з використанням уразливостей, які ідентифіковано на попередніх етапах, визначення стратегії ІБ, а також вибір варіантів і прийняття рішень з оброблення ризиків. Величина ризику визначається як середнє значення річних втрат компанії в результаті реалізації загроз ІБ.

Алгоритм цієї методики зображено на рис. 4

Рис. 4. Алгоритм методики управління ризиками OCTAVE

Охарактеризувавши три найпоширеніші методики з управління ризиками в сфері інформаційної безпеки та здійснивши аналіз основних властивостей цих методик, визначимо основні їх переваги та недоліки, див. табл. 1.

Таблиця 1

Переваги та недоліки методик з управління ризиками ІБ

Методика	Переваги	Недоліки
NIST		
CRAMM		
OCTAVE		

Завдання:

1. Ознайомитись з теоритичними відомостями.
2. Проаналізувати переваги та недоліки методик NIST, CRAMM та OCTAVE.

3. Заповнити таблицю 1, на основі даних аналізу переваг та недоліків NIST, CRAMM та OCTAVE.

Перелік контрольних питань

1. Особливості методики NIST.
2. Особливості методики CRAMM.
3. Особливості методики OCTAVE.

Рекомендовані джерела

1. Корченко О.Г. Аудит та управління інцидентами інформаційної безпеки // О.Г. Корченко, С.О. Гнатюк, С.В. Казмірчук, В.М. Панченко, С.В. Мельник. – К.: Центр навч.-наук. та наук.-пр. видань НА СБ України, 2014. – 193 с.

2. Менеджмент інформаційної безпеки : навчальний посібник для студентів спеціальності 125 "Кібербезпека" / О.Г. Корченко, М.Є. Шелест, С.В. Казмірчук, Ю.М. Ткач, Є.В. Іванченко. – Ніжин: ФОП Лук'яненко В.В. ТПК «Орхідея», 2019. – 408 с.

3. Бурячок В.Л., Толюпа С.В., Аносов А.О., Козачок В.А., Лукова-Чуйко Н.В. Системний аналіз та прийняття рішень в інформаційній безпеці: підручник. / В.Л. Бурячок, С.В.Толюпа, А.О. Аносов, В.А.Козачок, Н.В. Лукова-Чуйко / – К.:ДУТ, 2015. – 345 с.

Тема № 7. Основні підходи до реалізації моніторингу та аудиту безпеки інформації

Лабораторна робота «Аналіз ризиків та основні принципи забезпечення інформаційної безпеки»

Навчальна мета заняття:

1. Поглиблення та закріплення теоретичних знання з наступних питань:
   - поняття ризиків інформаційної безпеки та їх аналіз;
   - основні принципи та методи забезпечення інформаційної безпеки.
2. Ознайомлення та дослідження алгоритму оцінки ризиків інформаційної безпеки організації.
3. Набуття практичних навичок щодо застосування методики матричного аналізу ризиків інформаційної безпеки та надання основних рекомендацій з забезпечення ІБ.

Час проведення: 4 год. Місце проведення: комп'ютерний клас.

Устаткування: персональний комп'ютер (ПК) зі встановленою операційною системою Windows 7 або вище та доступом до мережі «Інтернет», Microsoft Office 2007 або вище.

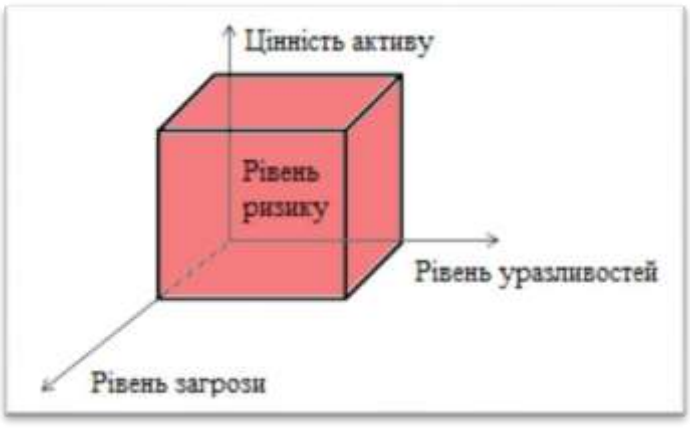
Порядок проведення заняття

Теоретичні відомості

Поняття ризиків інформаційної безпеки

Порушення основних властивостей інформації може стати серйозною загрозою для організацій в даний час. Інформацію важче контролювати і вона піддається зростаючому числу загроз і вразливостей, в тому числі комп'ютерному шахрайству, шпигунству, саботажу, вандалізму, пожежі або повені. Інформаційні ресурси, як і матеріальні, володіють якістю та кількістю, мають собівартість і ціну. Оцінка ризиків є важливою частиною будь-якого процесу інформаційної безпеки. Її використовують для визначення масштабу загроз інформаційної безпеки та ймовірності реалізації цих загрози.

В зв'язку з цим, також необхідно володіти таким поняття як ***ризик інформаційної безпеки*** – потенційна можливість використання загрозою вразливостей інформаційного активу або групи активів для заподіяння шкоди об'єктам або інтересам суб'єктів інформаційних відносин. Виходячи з визначення ризику, для проведення аналізу ризиків потрібні наступні дані про інформаційну систему: перелік цінної інформації із зазначенням її рівня критичності, відомості про уразливість інформаційної системи і загрози, які на неї діють.



При цьому необхідно відзначити, що жоден найдосконаліший спосіб зниження ризиків інформаційної безпеки, будь це політика безпеки, що досконально опрацьована, або найсучасніший брандмауер, не може захистити від виникнення в інформаційному середовищі подій, що потенційно несуть загрозу діяльності організації. Складність і різноманітність середовища діяльності сучасного підприємства зумовлюють наявність залишкових ризиків незалежно від якості підготовки і впровадження заходів протидії. Також завжди існує вірогідність реалізації нових, невідомих до теперішнього часу, загроз інформаційній безпеці. Неготовність організації до обробки подібного роду ситуацій може істотно ускладнити відновлення бізнес-процесів та потенційно збільшити завдані збитки. Саме тому й проводиться аналіз та оцінка ризиків ІБ.

Аналіз ризиків інформаційної безпеки – матричний підхід

Розрізняють два методи аналізу та оцінки ризиків: ***кількісний*** та ***якісний***.

Для кількісної оцінки ризиків характерне використання об’єктивних чисельних, а саме фінансових характеристик. На відміну від кількісного, якісний аналіз ризиків не ставить своїм завданням отримання чисельних фінансових характеристик. Для оцінки активів і критичність загроз вводиться якісна неформальна або напівформальна шкала, і основною метою такого аналізу стає ранжування загроз відповідно з обраними критеріями.

Оскільки даний курс присвячений основам інформаційній та кібернетичній безпеці, а не менеджменту ІБ, в лабораторній роботі буде розглянуто один із якісних методів аналізу ризиків, а саме матричний підхід аналізу ризиків ІБ, який пов’язує активи, уразливості, загрози та засоби контролю (міри, які організація може прийняти для мінімізації дій загроз на один чи більше активів) і визначає важливість різних засобів контролю, відповідним активам організації.

Матричний підхід використовує три окремих матриці: матрицю уразливостей, матрицю загроз і матрицю засобів контролю, які дозволяють зібрати всі необхідні дані для аналізу ризиків ІБ.

Матриця уразливостей складається із взаємозв’язків між активами і уразливостями в організації, в свою чергу матриця загроз відображає взаємозв’язки між уразливостями і загрозами, а матриця засобів контролю містить взаємозв’язки між загрозами і засобами контролю. Таким чином, кожна клітинка в таблиці відображає значення взаємозв’язку між елементами рядків та стовпців. В даному методі використовується наступна шкала взаємозв’язку (оцінки впливу): немає впливу, слабкий, помірний, сильний вплив.

При первинному аналізі ризиків формуються списки активів, уразливостей, загроз, засобів контролю, які в подальшому додаються до відповідних таблиць. Матриці заповнюються поступово шляхом додавання даних щодо взаємозв’язку елементів стовпця матриці з елементами рядка. Спершу заповнюється матриця уразливостей, дані якої обчислюються за допомогою формули (1.1), для визначення вагомості (значущість) уразливостей,

після чого останні переносяться до наступної матриці – матриці загроз. Аналогічно, дані в матриці загроз обчислюються за допомогою формули (1.2), таким чином визначаючи потенційні ризики ІБ, а самі загрози переносяться до останньої таблиці. В результаті чого, формується матриця контролю, яка містить відносну важливість різних засобів контролю. Дана матриця визначає необхідність в застосуванні конкретних мір або засобів захисту для мінімізації впливу загроз на один або більше активів організації зменшуючи рівень ризиків (демонструючи «чистий ризик» – ризик з мінімізованою реалізацією загроз).

Таблиця 1. Матриця вразливостей (взаємозв'язок між активами та вразливостями)

Матриця уразливостей Шкала взаємозв'язку немає слабкий помірний сильний 0 1 3 9 Ранг пріоритету (РП) 1 – незначний 2 – невеликий 3 – середній 4 – серйозний 5 – критичний C_j	**Активи:**	Секрети виробництва	Конфіденційна інформація	Репутація (довіра)	Апаратне забезпечення	Програмне забезпечення	Послуги	Комунікації	**Всього**	**Ранжування**
Уразливості:	РП								Σ	
Веб-сервер										
Обчислювальний сервер										
Міжмережевий екран										
Маршрутизатор										
Клієнтський вузол										
База даних										

Припустимо, що є m активів, де відносна вартість активу $a_j \in C_j$ $(j = 1, \cdots, m)$. Також нехай v_{ij} – це відносний вплив уразливості v_i на актив a_j.
Тоді потенційний вплив уразливості V_i на активи організації обчислюється за формулою:

$$V_i = \sum_{j=1}^{m} v_{ij} C_j \qquad 1.1$$

Таблиця 2. Матриця загроз (взаємозв'язок між уразливостями та загрозами)

Матриця загроз Шкала взаємозв'язку немає слабкий помірний сильний 0 1 3 9 Ранг пріоритету (РП) 1 – незначний 2 – невеликий 3 – середній 4 – серйозний 5 – критичний V_i	**Уразливості:**	Веб-сервер	Обчислювальний сервер	Міжмережевий екран	Маршрутизатор	Клієнтський вузол	База даних	Передача даних	**Всього**	**Ранжування**

Загрози:	РП								Σ	
Відмова в обслуговуванні (DoS)										
Шкідливе ПЗ										
Помилки користувача										
Спам										
«Фішинг»										
Ворожий агент										

Припустимо, що існує p загроз, які можуть бути реалізовані за допомогою n уразливостей та t_{ki} – відносна можливість використання загрозою t_k уразливості v_i. Тоді потенційна реалізація конкретної загрози T_k обчислюється за формулою:

$$T_k = \sum_{i=1}^{n} t_{ki} V_i \qquad 1.2$$

Таблиця 3. Матриця контролю (взаємозв'язок між загрозами та засобами захисту)

Матриця контролю Шкала взаємозв'язку немає слабкий помірний сильний 0 1 3 9 Ранг пріоритету (РП) 1 – незначний 2 – невеликий 3 – середній 4 – серйозний 5 – критичний T_k	**Загрози:**	Відмова в обслуговуванні	Шкідливе ПЗ	Помилки користувача	Спам	«Фішинг»	Ворожий агент	Збій електроживлення	**Всього**	**Ранжування**
Засоби контролю:	РП								Σ	
Система виявлення вторгнень (IDS)										
Навчання персоналу										
Міжмережевий екран										
Політика безпеки										
Конфігурація архітектури мережі										
Демілітаризована зона (DMZ)										

Припустимо, що є q засобів контролю (захисту), які можуть пом'якшити (мінімізувати) вплив p загроз, а z_{lk} – відносний вплив засобу контролю z_l на загрозу t_k. Тоді потенційне пом'якшення загроз за допомогою конкретного засобу контролю – Z_l, обчислюється за формулою:

$$Z_l = \sum_{i=1}^{p} z_{lk} T_k \qquad 1.3$$

Таким чином, за допомогою даної методики проводиться якісний аналіз ризиків: оцінюються активи організації, виділяються основні уразливості та критичні загрози, а також визначаються найвагоміші засоби контролю, в результаті чого ми одержуємо демонстрацію «чистого ризику», тобто ризику з

мінімізованим впливом загроз на активи організації. І вже на основі даних результатів визначається доцільність використання тих чи інших механізмів забезпечення безпеки, надаються рекомендацій щодо побудови систем захисту інформації та плануються витрати на ІБ організації.

Приклад використання методики аналізу ризиків ІБ

Дослідження аналізу ризиків за допомогою запропонованої методики буде здійснюватися на прикладі компанії «Cyberstec», яка займається розробкою програмного забезпечення. На даний момент компанія займається розробкою проектів в основному зосереджених в таких областях як: безпека робочих станцій і мережева безпека, віртуалізація та віддалений доступ, управління поведінкою системи, обробка даних, робота з мобільними пристроями. Вона має фрагментовану організаційну структуру, працює у декількох містах України (Київ, Львів, Харків, Одеса), а також має бізнес представництво у місті Мюнхен (Німеччина). Це достатньо конкурентний бізнес, де постійно розвиваються ІТ-технології і виробники постійно намагаються обійти один одного, таким чином, інформаційна безпека – є критичним фактором для захисту активів компанії і запобіганню зриву її діяльності.

Саме тому, для правильної організації системи безпеки, вибору конкретних методів захисту, та планування витрат на ІБ, в компанії проводиться аналіз інформаційних ризиків за допомогою запропонованої методики. Три матриці, які пов’язують активи та уразливості, уразливості та загрози, загрози та засоби контролю, представлені в таблицях 4, 5 та 6 відповідно.

Таким чином, у таблиці 4 представлено матрицю уразливостей, яка пов’язує уразливості та активи компанії «Cyberstec». Для побудови матриці була визначена відносна цінність активів та проведено їхнє ранжування (з права на ліво). Наприклад, успішність компанії залежить від її здатності розвивати і захищати нові технології; тому вони високо оцінюються. Ґрунтуючись на активах, було визначено ключові уразливості, надано їм ранг пріоритету та встановлено відносний вплив уразливостей на активи компанії. Так як зовнішні порушники (хакери) спершу повинні обійти брандмауер, щоб отримати доступ до конфіденційної інформації, він займає перше місце у матриці уразливостей. Окрім того, як було зазначено раніше, філії компанії територіально розкидані, тому передача та синхронізація даних також оцінюються високо.

В результаті, як бачимо, в матриці було проведено обчислення потенційного впливу уразливостей на активи «Cyberstec» за формулою (1.1) для того, щоб відранжувати уразливості і таким чином визначити їхню значущість.

Таблиця 4. Матриця уразливостей «Cyberstec»

Матриця уразливостей Шкала взаємозв'язку немає слабкий помірний сильний 0 1 3 9 Ранг пріоритету (РП) 1 – незначний 2 – невеликий 3 – середній 4 – серйозний 5 – критичний C_j	**Активи:**	Новітні розробки (технології)	Конф. інф. (програмний код)	Репутація (довіра)	Доступність сервісів комунікації	Програмне забезпечення	Апаратне забезпечення	**Всього**	**Ранжування**
Уразливості:		7	6	5	4	3	2	1	**Σ**	
Брандмауер	5	9	9	3	9	9	9	9	222	9
Передача даних та лінії зв'язку	5	9	9	3	9	9	3	9	210	8
Фізична безпека	4	9	9	3	1	1	3	9	154	5
Помилки конфігурації серверів екстранет	4	9	9	1	9	3	9	1	186	7
ПК співробітників компанії	3	3	9	1	0	1	9	3	104	2
Бази даних	4	9	9	3	3	1	9	1	166	6
Стійкість паролів	3	9	9	1	1	3	9	1	154	4
Помилки конфігурації серверів інтернет	2	1	1	9	9	3	9	1	122	3
Ненадійне джерело живлення	1	0	0	3	9	9	0	1	79	1

Після цього уразливості були перенесені до наступної матриці.

Беручи до уваги наявні уразливості в активах компанії, було визначено ключові загрози, надано їм ранг пріоритету та аналогічним чином, встановлено відносну можливість використання загрозою уразливості.

Таблиця 5. Матриця загроз «Cyberstec»

Матриця загроз Шкала взаємозв'язку немає слабкий помірний сильний 0 1 3 9 Ранг пріоритету (РП) 1 – незначний 2 – невеликий 3 – середній 4 – серйозний 5 – критичний V_i	**Уразливості:**	Брандмауер	Передача даних та	Помилки конфігурації	Бази даних	Фізична безпека	Стійкість паролів	Помилки конфігурації	ПК співробітників компанії	Ненадійне джерело	**Всього**	**Ранжування**
Загрози:		9	8	7	6	5	4	3	2	1	Σ	
Відмова в обслуговуванні (DoS/DDos)	5	9	9	9	0	1	1	9	1	1	255	5
Шкідливе ПЗ	4	1	1	9	1	1	1	3	9	1	123	2
Помилки працівника	2	1	1	3	3	3	3	3	9	1	111	1
Збої сервера	5	9	9	9	9	9	1	9	1	9	357	8
Вторгнення (атака на пароль)	3	9	3	9	9	1	9	3	3	1	279	6
Фізичне пошкодження ІТС	3	1	9	3	3	9	0	3	3	3	183	3

«Спуфінг» та «Маскарад»	2	1	9	9	3	1	1	9	9	1	217	4
НСД	5	9	3	9	9	9	9	9	9	1	349	7

В результаті обчислень за допомогою формули (1.2), було визначено потенційні ризики ІБ, а самі загрози переносяться до останньої таблиці.

Останньою формується матриця контролю, до якої, окрім загроз, були внесені запропоновані засоби контролю з відповідним рангом пріоритету. Після чого було встановлено відносний вплив засобу контролю на загрозу з використанням суб'єктивних суджень, і обчислено за формулою (1.3) потенційне пом'якшення загроз. Отримані дані були відранжовані з метою визначення пріоритетних засобів контролю. Ця інформація, в поєднанні з вартістю засобів контролю використовується для планування ІБ.

Таким чином, результати аналізу і узагальнення даних, що містяться в матрицях будуть використовуватися під час процесу інтеграції та вибору програмного забезпечення і апаратного устаткування в компанії «Cyberstec».

Таблиця 6. Матриця контролю «Cyberstec»

Матриця контролю Шкала взаємозв'язку немає слабкий помірний сильний 0 1 3 9 Ранг пріоритету (РП) 1 – незначний 2 – невеликий 3 – середній 4 – серйозний 5 – критичний T_k	**Загрози:**	Збої сервера	НСД	Вторгнення (атака на	Відмова в обслуговуванні	«Спуфінг» та «Маскарад»	Фізичне пошкодження		Помилки працівника	**Всього**	**Ранжування**
Засоби контролю:		8	7	6	5	4	3	2	1	Σ	
Система виявлення вторгнень (IDS)	5	9	9	3	9	9	1	3	3	246	6
Навчання персоналу	2	1	0	9	0	3	3	9	9	110	1
Міжмережеві екрани	5	9	9	9	9	9	1	3	1	280	7
Політика безпеки	4	1	9	9	3	9	1	9	3	200	4
Конфігурація архітектури мережі	5	9	3	1	9	1	0	0	1	149	2
Демілітаризована зона (DMZ)	3	9	9	3	9	3	0	0	3	213	5
Контроль території	4	3	9	9	1	1	9	3	1	184	3

Основні принципи та методи забезпечення інформаційної безпеки

З метою протидії основним загрозам ІБ, система забезпечення інформаційної безпеки ІТС повинна вирішувати наступні завдання:

1) розмежування та контроль доступу користувачів до ресурсів ІТС;
2) захист всіх даних, що передаються по каналах зв'язку;
3) реєстрація, збір, зберігання, обробка і видача інформації про всі події, що відбуваються в системі і мають відношення до забезпечення її безпеки;

4) моніторинг роботи користувачів ІТС системою захисту інформації та оперативне сповіщення адміністратора безпеки про спроби несанкціонованого доступу до ресурсів системи;

5) забезпечення замкнутого середовища функціонування вже перевіреного ПЗ з метою захисту від неконтрольованого впровадження в систему потенційно небезпечних програм (які можуть містити «закладки» або критичні помилки) і засобів подолання системи захисту, а також від впровадження та поширення шкідливого ПЗ;

6) забезпечення доступності інформаційних ресурсів шляхом резервного копіювання даних;

7) забезпечення та контроль цілісності критичних ресурсів системи захисту ІТС.

Також необхідно відмітити, що розрізняють зовнішню та внутрішню безпеку ІТС. Зовнішня безпека полягає в захисті ІТС від загроз природного походження, а також від проникнення в систему зловмисників ззовні.

Внутрішня ж безпека повинна створювати надійний і зручний механізм регламентування діяльності усіх законних користувачів та обслуговуючого персоналу ІТС, а також забезпечувати цілісність даних.

Що стосується ***методів забезпечення інформаційної безпеки*** то вони достатньо різноманітні, однак їх можна розділити на наступні основні групи: теоретичні, законодавчі (правові), адміністративні (організаційні), інженерно-технічні (програмно-технічні) та криптографічні.

Теоретичні методи забезпечення інформаційної безпеки вирішують два основних завдання. Перше з яких – формалізація різного роду процесів, пов'язаних із забезпеченням інформаційної безпеки. Так, наприклад, формальні моделі управління доступом дозволяють строго описати всі можливі інформаційні потоки в системі – а значить, гарантувати виконання необхідних властивостей безпеки. Звідси безпосередньо випливає друге завдання – суворе обґрунтування коректності і адекватності функціонування систем забезпечення інформаційної безпеки при проведенні аналізу їх захищеності. Така задача виникає, наприклад, при проведенні сертифікації автоматизованих систем за вимогами безпеки інформації.

Законодавчі міри захисту визначаються діючими в країні нормативно-правовими актами, що регламентують правила поводження з інформацією, що закріплюють права та обов'язки учасників інформаційних відносин у процесі її обробки та використання, а також встановлюють відповідальність за порушення цих правил. Важливе значення мають стандарти в області захисту інформації (у першу чергу, міжнародні). Серед цих стандартів виділяються «Помаранчева книга», рекомендації X. 800 і «Загальні критерії оцінки безпеки інформаційних технологій».

Адміністративні методи захисту – методи організаційного характеру, які регламентують процеси функціонування ІТС, діяльність персоналу, а також порядок взаємодії користувачів із системою таким чином, щоб найбільшою мірою мінімізувати або виключити можливість реалізації загроз безпеки.

Зазвичай вони включають:

- підбір та підготовку персоналу системи;
- організацію охорони та контрольно-пропускного режиму;
- організацію обліку, зберігання, використання та знищення документів та носіїв з інформацією;
- розподіл атрибутів розмежування доступу (паролів, ключів шифрування тощо).

Основою адміністративних методів захисту інформації є формування *політика безпеки* організації – сукупність вимог, правил, обмежень, рекомендацій, які регламентують порядок інформаційної діяльності в організації і спрямовані на досягнення і підтримку стану інформаційної безпеки організації.

Криптографічні методи захисту інформації реалізується шляхом перетворення інформації (шифрування, кодування та інші перетворення) з використанням спеціальних (ключових) даних та алгоритму зворотного перетворення з метою приховування/відновлення змісту інформації, підтвердження її справжності, цілісності, авторства тощо. Можна стверджувати, що на теперішній час, криптографічний метод захисту є одним із найбільш надійніших методів захисту, оскільки захищається безпосередньо сама інформація, а не доступ до неї.

Інженерно-технічні методи захисту інформації засновані на використанні спеціальних інженерно-технічних заходів, апаратних засобів і програмного забезпечення, що входять до складу ІТС і унеможливлюють виток, знищення або блокування інформації, порушення цілісності та режиму доступу до неї.

Однак, необхідно відзначити, що універсальних методів захисту не існує, і тому під час вирішення питання щодо захисту інформації потрібно обов’язково враховувати критичність інформаційних активів, усі наявні ризики, а вже потім використовувати конкретні механізми забезпечення безпеки та планувати витрати на ІБ. Багато в чому успіх при побудові механізмів безпеки для реальної системи буде залежати від її індивідуальних особливостей, облік яких погано піддається формалізації. Тому часто інформаційну безпеку розглядають як певну сукупність неформальних рекомендацій щодо побудови систем захисту інформації того чи іншого типу.

Порядок виконання лабораторної роботи:

1. Ознайомитися з теоретичними відомостями.
2. Провести якісний аналіз та оцінку ризиків інформаційної безпеки організації (згідно варіанту в табл. 7) за допомогою матричного підходу.
3. На основі отриманих результатів, надати основні рекомендації щодо забезпечення ІБ в даній організації.
4. Оформити звіт згідно до вимог.
5. Відповісти на контрольні питання.

Зміст звіту:

1. Титульний лист.
2. Постановка завдання.
3. Короткі відомості про організацію в якій буде проводитися аналіз та оцінка ризиків ІБ.
4. Сформовані списки та обґрунтування інформаційних активів організації, ймовірних уразливостей, загроз та засобів контролю.
5. Сформовані, заповнені та оброблені 3 матриці: матриця уразливостей, матриця загроз та матриця контролю.
6. Основні рекомендації щодо забезпечення інформаційної безпеки в даній організації.
7. Висновки та відповіді на контрольні питання.

Завдання

Таблиця № 7. (варіант відповідно до номера за списком у журналі)

Номер варіанта	Організація	Кількість інформаційних активів
1	Державний комерційний банк	8
2	Приватна поліклініка	9
3	Страхова компанія	7
4	Інтернет-магазин	9
5	Адвокатська контора	8
6	Агентство нерухомості	7
7	Рекламне агентство	7
8	Науково-проектне підприємство	9
9	Аудиторська компанія	8
10	Туристичне агентство	7
11	Консалтингова фірма	9
12	Фармакологічна компанія	8
13	Архітектурне агентство	7
14	Інтернет-провайдер	7
15	Будівельна компанія	8
16	Система електронних платежів	9
17	Видавництво	7
18	Благодійний фонд	8
19	Рекрутингове агентство	7
20	Міжнародний комерційний банк	9
21	Військове підприємство	6

22	Компанія-розробник ПЗ	9
23	Дизайнерська фірма	8
24	Організація з розробки електроніки	9
25	Державна поліклініка	8
26	Авіакомпанія	9
27	Редакція газети	7

Контрольні питання

1. Надати визначення наступним поняттям: ризик ІБ, загроза ІБ.
2. Коротко описати алгоритм аналізу ризиків інформаційної безпеки організації.
3. Які повинна вирішувати завдання система забезпечення інформаційної безпеки ІТС?
4. Коротко охарактеризувати основні групи методів забезпечення ІБ.

Рекомендовані джерела

1. Корченко О.Г. Аудит та управління інцидентами інформаційної безпеки // О.Г. Корченко, С.О. Гнатюк, С.В. Казмірчук, В.М. Панченко, С.В. Мельник. – К.: Центр навч.-наук. та наук.-пр. видань НА СБ України, 2014. – 193 с.
2. Менеджмент інформаційної безпеки : навчальний посібник для студентів спеціальності 125 "Кібербезпека" / О.Г. Корченко, М.Є. Шелест, С.В. Казмірчук, Ю.М. Ткач, Є.В. Іванченко. – Ніжин: ФОП Лук’яненко В.В. ТПК «Орхідея», 2019. – 408 с.
3. Бурячок В.Л., Толюпа С.В., Аносов А.О., Козачок В.А., Лукова-Чуйко Н.В. Системний аналіз та прийняття рішень в інформаційній безпеці: підручник. / В.Л. Бурячок, С.В.Толюпа, А.О. Аносов, В.А.Козачок, Н.В. Лукова-Чуйко / – К.:ДУТ, 2015. – 345 с.

Тема № 8. Програмні засоби для проведення аудиту інформаційної безпеки

Лабораторна робота «Побудова байєсівської мережі довіри для оцінки ризиків»

Навчальна мета заняття: створити байєсівську мережу довіри для оцінки ризиків ІБ за допомогою програмного засобу Hugin Expert.

Час проведення: 8 год. Місце проведення: комп'ютерний клас.

Устаткування: персональний комп'ютер (ПК) зі встановленою операційною системою Windows 7 Pro або вище та доступом до мережі «Інтернет», програмний засіб Hugin Expert.

Порядок проведення заняття

Теоретичні відомості

Метод на основі байєсовских мереж (МБМ)

Метод МБМ розроблений для побудови каузальних моделей оцінки операційних ризиків. В його основі лежить теорема Байєса, цінність якої стосовно оцінки таких ризиків полягає в її здатності комбінувати дані про ймовірність подій, одержаних експертним і статистичними шляхом. Кожній пов'язаній з ризиком події (наприклад «Хакерська атака», «НСД», «НСМ» та ін.) проводиться оцінка ймовірності її реалізації та (за ланцюжком) операційних втрат, що з нею пов'язані.

Байесовские мережі довіри - Bayesian Belief Network - використаються в тих областях, які характеризуються успадкованою невизначеністю. Розглянемо приклад мережі (рис. 1), у якій імовірність перебування вершини «**e**» у різних станах (e_k) залежить від станів (c_i , d_j) вершин «**c**» і «**d**» і визначається вираженням:

$$p(e_k) = \sum_i \sum_j p(e_k | c_i, d_j) \times p(c_i, d_j)$$

де $p(e_k \mid c_i, d_j)$ – імовірність перебування в стані e_k залежно від станів c_i, d_j. Якщо події, представлені вершинами «**c**» і «**d**» незалежні, тоді маємо:

$$p(c_i , d_j) = p(c_i) \cdot p(d_j).$$

І, відповідно:

$$p(e_k) = \sum_i \sum_j p(e_k \mid c_i, d_j) \times p(c_i) \times p(d_j)$$

Нехай e – це «зупинка серверу», а c і d – «хакерська атака» і «зараження вірусом» відповідно. Імовірність реалізації події може бути вказана у вигляді безперервної функції розподілу або у вигляді таблиці ймовірностей (дискретних ймовірностей). Приклад експертного відображення умовної ймовірності показаний в табл. 1.

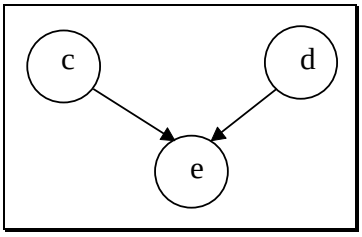


Рис.1. Приклад найпростішої байесовской мережі довіри.

Таблиця 1. Формування ймовірності

	Результати - умови			
Хакерська атака	ТАК		НІ	
Зараження вірусом	Так	Ні	Так	Ні
Ймовірність результату події «Зупинка сервера» для різних умов				
Відбудеться	0,3	0,15	0,10	0,02
Не відбудеться	0,7	0,85	0,90	0,98

Потім додаються так звані вершини корисності (в тому числі - витрати). Визначається абсолютна ймовірність та величина витрат. Розглядаються три категорії наслідків: порушення конфіденційності (К), цілісності (Ц) та доступності (Д). Для матеріальних активів збиток визначається за шкалою – від повної втрати активу до збою (зупинки, неполадки) за несуттєвий проміжок часу. Отримаємо діаграму впливу.

Діаграми впливу використаються для прийняття рішень. Фактично діаграми впливу - це байесовские мережі довіри розширені поняттями користі (utility) і рішення (decisions). Якщо байесовские мережі довіри містили тільки один тип вершин, які ми назвемо вершинами шансів, і які відповідали стану випадкових змінних, то в діаграмах впливу використаються ще, як мінімум, два типи вершин: вершини рішення, позначувані в діаграмах впливи прямокутниками й вершини користі, позначувані в діаграмах впливи у вигляді ромба.

Вершини рішення, а точніше сказати вказівки, що втримуються в них, визначають тимчасове старшинство:

Метод VAR

Метод VAR (Value at Risk) заснований на статистичному підході та дозволяє оцінити ризик в термінах можливих втрат співвіднесених з їх ймовірностями виникнення. Тут описується квантиль прогнозованого розподілу втрат протягом певного періоду часу.

Процес оцінювання включає наступні етапи: ідентифікація загроз, оцінка їх ймовірності, обчислення цінності з урахуванням небезпеки та зменшення ризику. Спочатку реалізується класифікація загроз, таких як, наприклад, шахрайство, зловмисні дії, жарти, спроби отримати доступ до приватної інформації, стихійні лиха, саботаж, помилки користувачів та ін. Коли загрози були ідентифіковані, їх ймовірність (розподіл ймовірності) оцінена, можливі сценарії описані, то визначається небезпека для фірми при реалізації загроз

Завдання

1. Ознайомитись з інтерфейсом Hugin Expert.
2. Побудувати мережу довіри, що модулює стан інформаційної безпеки якоїсь організації, або підрозділу.
3. Задати таблиці умовних та маргінальних імовірностей.
4. Провести дослідження впливу різних чинників на стан безпеки.
5. Побудувати діаграму впливу.
6. Оцінити ефективність рішень через оцінку корисності.

Перелік контрольних питань

1. Формула Байєсса.
2. Експертна оцінка умовних та маргінальних імовірностей.
3. Мережі довіри.
4. Діаграми впливу.

Рекомендовані джерела

1. Корченко О.Г. Аудит та управління інцидентами інформаційної безпеки // О.Г. Корченко, С.О. Гнатюк, С.В. Казмірчук, В.М. Панченко, С.В. Мельник. – К.: Центр навч.-наук. та наук.-пр. видань НА СБ України, 2014. – 193 с.

2. Менеджмент інформаційної безпеки : навчальний посібник для студентів спеціальності 125 "Кібербезпека" / О.Г. Корченко, М.Є. Шелест, С.В. Казмірчук, Ю.М. Ткач, Є.В. Іванченко. – Ніжин: ФОП Лук’яненко В.В. ТПК «Орхідея», 2019. – 408 с.

3. Бурячок В.Л., Толюпа С.В., Аносов А.О., Козачок В.А., Лукова-Чуйко Н.В. Системний аналіз та прийняття рішень в інформаційній безпеці: підручник. / В.Л. Бурячок, С.В.Толюпа, А.О. Аносов, В.А.Козачок, Н.В. Лукова-Чуйко / – К.:ДУТ, 2015. – 345 с.

2. Інформаційні ресурси

1. Національна база даних вразливостей. URL: https://nvd.nist.gov/ (дата звернення: 15.11.2023).
2. Програмне забезпечення для проведення оцінки ризиків. URL: http://secinsight.blogspot.com/2012/01/blog-post.html (дата звернення: 15.11.2023).
3. Microsoft Security Assessment Tool (MSAT), URL: https://www.microsoft.com/ru-ru/download/details.aspx?id=12273 (дата звернення: 15.11.2023).
4. Microsoft SDL Threat Modeling Tool. URL: https://www.microsoft.com/en-us/securityengineering/sdl/threatmodeling (дата звернення: 15.11.2023).