ДЕРЖАВНИЙ УНІВЕРСИТЕТ «ЖИТОМИРСЬКА ПОЛІТЕХНІКА»

ФАКУЛЬТЕТ ІНФОРМАЦІЙНО-КОМП'ЮТЕРНИХ ТЕХНОЛОГІЙ
(повне найменування інституту, назва факультету)

Кафедра комп'ютерної інженерії та кібербезпеки
(повна назва кафедри)

Пояснювальна записка

до випускної кваліфікаційної роботи бакалавра

на тему:

Інформаційна система оцінки кіберзагроз

Виконав: студент 4 курсу, групи ЗКБ-17
напряму підготовки
125 Кібербезпека
(шифр і назва напряму підготовки, спеціальності)

Храбан Юлія Володимирівна

(прізвище та ініціали)
Керівник к.т.н. доцент Лобанчикова Н.М.
(прізвище та ініціали)
Рецензент Левківський В.Л.
(прізвище та ініціали)

Житомир 2021

ДЕРЖАВНИЙ УНІВЕРСИТЕТ «ЖИТОМИРСЬКА ПОЛІТЕХНІКА»

Факультет інформаційно-комп'ютерних технологій
Кафедра Комп'ютерної інженерії та кібербезпеки
Освітньо-кваліфікаційний рівень бакалавр Спеціальність 125 Кібербезпека_____
_____ (шифр і назва)

ЗАТВЕРДЖУЮ
Завідувач кафедри Комп'ютерної інженерії та кібербезпеки
_____ _Єфіменко А.А.
"__ "_____ 2021 р.

З А В Д А Н Н Я
НА ДИПЛОМНУ РОБОТУ СТУДЕНТУ
_____Храбан Юлії Володимирівні
(прізвище, ім'я, по батькові)

1. Тема Інформаційна система оцінки кіберзагроз

   Керівник роботи к.т.н. Лобанчикова Н.М., доцент кафедри КІ та КБ-_____
   (прізвище, ім'я, по батькові, науковий ступінь, вчене звання)

затверджені наказом вищого навчального закладу від "31" березня 2021 року №112/с

2. Строк подання студентом роботи "29" червня 2021 року
3. Вихідні дані до роботи матеріали звіту про переддипломну практику, проект інформаційної системи оцінки кіберзагроз.
4. Зміст розрахунково-пояснювальної записки (перелік питань, які потрібно розробити) дослідження особливостей протидії кіберзагрозам, аналіз основних загроз, розробка алгоритмів функціонування системи, БД системи, проектування ІС оцінки кіберзагроз.

5. Перелік графічного матеріалу: функціональні схеми, алгоритм роботи

6. Консультанти розділів роботи

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		Завдання видав	Завдання прийняв
1,2,3	к.т.н. Лобанчикова Н.М., доцент		

7. Дата видачі завдання____31.03.2021_____

Календарний план

№	Назва етапів дипломної роботи	Строк виконання дипломної роботи	Примітка
1	Звіт про переддипломну практику	01.02.2021-01.03.2021	виконано
2	Ознайомлення з завданням	01.03.2021-28.03.2021	виконано
3	Аналіз загроз	29.03.2021-08.04.2021	виконано
4	Розроблення схем, формування розділу 1	08.04.2021-24.04.2021	виконано
5	Формування розділу 2	25.04.2021-01.05.2021	виконано
6	Формування розділу 3	02.05.2021-20.05.2021	виконано
7	Виконання роботи	21.05.2021-06.06.2021	виконано

Студент _____ Ю.В.Храбан
(підпис) (прізвище та ініціали)
Керівник роботи _____ Н.М.Лобанчикова
(підпис) (прізвище та ініціали)

ЗМІСТ

ВСТУП 6
1.ТЕОРЕТИЧНІ ОСНОВИ ПОБУДОВИ ІС ОЦІНКИ КІБЕРЗАГРОЗ 8
1.2. Аналіз вразливості інформаційно-телекомунікаційної системи.....14
1.3. Дослідження міжнародного стандарту ISO/IEC 27001 і рішення для покращення захисту 21
1.4. Різносторонні підходи до зменшення ризиків кібернетичних атак на ланцюг поставок 23
1.5 Постановка задач.....25
2. ПРОЕКТУВАННЯ ТА МОДЕЛЮВАННЯ ІС оцінки кіберзагроз 27
2.1 Структура ІС оцінки кіберзагроз 27
2.2 Розробка UML-діаграм функціонування системи 32
2.3 Вибір програмного засобу для реалізації ІС 35
3.ПРОГРАМНА РЕАЛІЗАЦІЯ ІНФОРМАЦІЙНОЇ СИСТЕМИ ОЦІНКИ КІБЕРЗАГРОЗ.....39
3.1. Розробка структури системи 39
3.2 Інтерфейс інформаційної системи оцінки кіберзагроз.....40
ВИСНОВКИ.....47

ПЕРЕЛІК УМОВНИХ СКОРОЧЕНЬ

БД – бази даних

БЗ – бази знань

ЕС – експертні системи

ІзОД – інформація з обмеженим доступом

ІКС – інформаційно-комунікаційна система

НСД – несанкціонований доступ

ОС – операційна система

СЗІ – системи захисту інформації

ІС – інформаційна система

ВСТУП

Формування й ефективна реалізація кібербезпекової політики, в рамках якої розробляється комплекс заходів щодо прогнозування та протидії кіберзагрозам, є необхідною умовою розвитку суспільства знань. В умовах глобалізації інформаційних процесів, їх інтеграції в різні сфери суспільного життя керівництво провідних держав світу приділяє посилену увагу створенню й удосконаленню ефективних систем захисту критичної інфраструктури від зовнішніх і внутрішніх загроз кібернетичного характеру.

Відзначимо, що в багатьох провідних країнах світу вже сформовані загальнодержавні системи кібернетичної безпеки як найбільш оптимальні організаційні структури, що здатні в короткий проміжок часу акумулювати сили та засоби компетентних органів державної влади із залученням громадських для протидії кіберзагрозам.

Кіберзагрози в сучасному суспільстві набирають значного масштабу. Відтепер успішна атака хакерів може знеструмити область або країну, призвести до пограбування банку чи знищити успішну організацію. Наприклад, за різними оцінками, за 2020 рік із рахунків підприємств України зникло близько 700 млн грн. [27].

Метою кваліфікаційної роботи є розробка інформаційної системи оцінки кіберзагроз у кібернетичному просторі господарських підприємств.

Розробка такого роду програмного продукту дасть змогу керівникам підприємств одержати реальну оцінку засобів та заходів захисту від безпосереднього та віддаленого доступу до елементів ІКС, організаційних та програмно-технічних засобів захисту.

Об’єктом дослідження є процеси побудови інформаційної системи оцінки кіберзагроз.

Предмет дослідження – підходи, методи, засоби та технології побудови інформаційної системи оцінки кіберзагроз щодо оцінки захищеності інформаційно-телекомунікаційної системи господарських підприємств.

Для досягнення вказаної мети необхідним є вирішення наступних задач:

- аналіз методів, засобів та технологій побудови ІС;
- аналіз методів, засобів та технологій побудови систем захисту ІКС;
- моделювання інформаційної системи оцінки кіберзагроз;
- розробка структурної схеми інформаційної системи оцінки кіберзагроз;
- програмна реалізація інформаційної системи оцінки кіберзагроз.

Методологія роботи – системний аналіз, методи об’єктно–орієнтованого проектування та моделювання, методи та засоби побудови СППР, методи проектування баз знань, мова моделювання UML.

1.ТЕОРЕТИЧНІ ОСНОВИ ПОБУДОВИ ІС ОЦІНКИ КІБЕРЗАГРОЗ

1.1 Аналіз загроз інформаційної безпеки в інформаційно-телекомунікаційній системі

Ціллю інформаційної безпеки є протидія виникненню, реалізації та зменшення руйнівної дії у випадку усе ж таки реалізації загрози інформаційній безпеці.

Сукупність умов і дій, які загрожують інформаційній безпеці, такі як несанкціоновані або неумисні дії проти неї – це ми і вважаємо загрозою інформаційній безпеці (ІБ) [1-10].

Загальні параметри загроз ІБ:

- джерело загрози;
- слабкі сторони системи (вразливість);
- методи відтворення загрози;
- певні дії для відтворення загрози.

Слабким місцем ІКС (тобто вразливістю) є певна характеристика, яка створює можливість для відтворення загрози. Якщо точніше, то небезпечні дії можуть відтворюватися як раз за існування слабкого місця ІС.

Дії, виконувані людиною для відтворення певних загроз ІБ ІКС називаються атакою на ІКС. Мається на увазі пошук і використання вразливості системи[11-18].

Несанкціонований доступ (порушення прав та правил доступу) – окрема галузь загроз з-поміж усіх[5]. Виділяють такі варіанти НСД: несанкціоноване озна

йомлення з інформацією, несанкціоноване копіювання (розкрадання) інформації і/або несанкціонована дія на інформацію (знищення, блокування і так далі) [19-34].

Кібернетична загроза (кіберзагроза) – наявні й потенційно можливі явища та чинники, що створюють небезпеку інтересам людини, суспільства й держави через порушення доступності, повноти, цілісності, достовірності, автентичності режиму доступу до інформації, яка циркулює в критичних об’єктах національної інформаційної інфраструктури [29].

Цю дефініцію, на нашу думку, варто доповнити правомочностями, які закріплені в Законі України «Про інформацію» як основоположному в інформаційній сфері, в якій мають місце кіберзагрози, а саме: створення небезпеки загроз відносинам щодо створення, збирання, одержання, зберігання, використання, поширення, охорони, захисту інформації.

Зауважимо на тому, що загроза не може бути фактом або подією, у будь-якому випадку це дії.

Розглянемо таке визначення поняття кіберзагрози.

Кібернетичні загрози (кіберзагрози) – наявні й/або потенційно можливі явища та чинники, що створюють небезпеку життєво важливим інтересам людини і громадянина, суспільства й держави, реалізація яких залежить від належного функціонування інформаційних, телекомунікаційних та інформаційно-телекомунікаційних систем [31].

Ця дефініція також потребує низки уточнень, а саме: що становить життєво важливі інтереси людини та громадянина? Чи є нагальною потреба закріплення саме формулювання «людина та громадянин»? Як саме визначити належність функціонування вищезазначених систем? Як співвідноситься це визначення й Законом України «Про основи національної безпеки України», і Стратегією національної безпеки України тощо.

«Кібернетичний» – той, що стосується до кібернетики.

Отже, ґрунтуючись на цих дефініціях, пропонуємо наступне визначення розуміння: «кіберзагрози» – протиправні, карані дії суб'єктів інформаційних правовідносин, які створюють небезпеку життєво важливим інтересам людини, суспільства та держави загалом, реалізація яких залежить від належного функціонування інформаційних, телекомунікаційних та інформаційно-телекомунікаційних систем, а також відносинам щодо створення, збирання, одержання, зберігання, використання, поширення, охорони, захисту інформації [http://pgp-journal.kiev.ua/archive/2017/4/22.pdf].

У Доктрині інформаційної безпеки України (втратила чинність) було зазначено, що в інформаційній сфері України вирізняються такі життєво важливі інтереси:

особи: забезпечення конституційних прав і свобод людини на збирання, зберігання, використання та поширення інформації; недопущення несанкціонованого втручання в зміст, процеси оброблення, передачі й використання персональних даних; захищеність від негативного інформаційно-психологічного впливу;

суспільства: збереження та примноження духовних, культурних і моральних цінностей Українського народу; забезпечення суспільнополітичної стабільності, міжетнічної та міжконфесійної злагоди; формування й розвиток демократичних інститутів громадянського суспільства;

держави: недопущення інформаційної залежності, інформаційної блокади України, інформаційної експансії з боку інших держав і міжнародних структур; ефективна взаємодія органів державної влади та інститутів громадянського суспільства під час формування, реалізації та коригування державної політики в інформаційній сфері; побудова й розвиток інформаційного суспільства; забезпечення економічного та науково-

технологічного розвитку України; формування позитивного іміджу України; інтеграція України у світовий інформаційний простір [32].

Під час визначення термінів пропонується надавати їх у більш широкому розумінні, враховуючи вже наявні напрацювання в таких галузях науки, як кібернетика, інформатика, інформаціологія, безпекознавство, кримінальне й інформаційне право тощо.

Обговорювання та розширення термінології щодо кіберпростору дасть змогу суспільству більш якісно й безпечно планувати свої дії в сучасному кіберпросторі. Додаткові терміни зроблять можливим лаконічно пояснити, що людська (суспільна) думка – це є аналоговий кібербіопростір, який за допомогою технічних засобів перетікає в технічний кіберпростір, там накопичується, багаторазово копіюється, обробляється та перетікає назад і аналоговий кібербіопростір у новому більш розвинутому й перевіреному всім суспільством вигляді, але вже для масового використання та розвитку суспільства на новому вищому рівні [31].

У міжнародному законодавстві й досі відсутнє єдине визначення понять: «кібернетична безпека», «кібернетична загроза», «кібернетичний захист», «кібернетичний простір», «кібернетична злочинність». Проблема кібербезпеки специфічна та глобальна, тому максимальна ефективність у боротьбі з новими загрозами може бути забезпечена, якщо міжнародні актори, приватні корпорації й асоціації об’єднають свої зусилля. Актуальність визначення змісту понять «кібербезпека» та «кіберзагроза» (авт.) є важливим моментом для покращення ефективності взаємодії на міжнародному рівні [33].

Кібернетичні загрози являють собою загрози, реалізація яких пов’язана з використанням відповідних ресурсів інформаційно-телекомунікаційних систем. Уразливими для реалізації кібернетичних загроз є об’єкти, функціонування комп’ютерних систем яких пов’язане з використанням

ресурсів кіберпростору. Тобто об’єкти, завдання шкоди яким можливе шляхом деструктивного кібернетичного впливу (кібернетичної атаки) – інформаційного впливу з використанням кіберресурсів, спрямованого на уразливості комп’ютерних систем таких об’єктів. До об’єктів національної критичної інфраструктури, що потребують захисту від кібератак, необхідно зарахувати об’єкти, реалізація кібернетичних загроз щодо яких може призвести до настання таких наслідків, як надзвичайна ситуація; блокування роботи або руйнування стратегічно важливих для економіки та безпеки держави підприємств, систем життєзабезпечення й об’єктів підвищеної небезпеки; блокування роботи державних органів; блокування діяльності органів військового управління, Збройних Сил України загалом або втручання в автоматизовані системи керування зброєю; порушення безпечного функціонування банківської або фінансової системи держави; розголошення державної таємниці; масові заворушення [4]. Тобто кіберзагрози не можна обмежувати якоюсь однією сферою, частіше за все настання певних наслідків може спричинити інші, тобто ланцюгова реакція.

Розвиваючи далі ідею загроз у сфері кібербезпеки, зауважимо, що існує залежність країни й в інформаційному, і смисловому вимірах. Це відбувається тоді, коли країні не вистачає власних новин чи власних фільмів, і вона заповнює ці прогалини чужим продуктом. Україна є чітким прикладом цієї ситуації [35

Інформаційні інтервенції становлять суттєву загрозу кібернетичній безпеці, оскільки остання є частиною національної безпеки, може завдавати шкоди як державі загалом, так і окремим фізичним особам. Створення дієвої системи забезпечення кібернетичної безпеки вимагає від державних органів України чіткого визначення правових засад державної політики в цій сфері та своєчасного реагування на динамічні зміни, що відбуваються у світі у сфері

забезпечення кібернетичної безпеки з можливістю застосування міжнародного досвіду.

При цьому вибір конкретних засобів і способів забезпечення кібернетичної безпеки України зумовлюється необхідністю своєчасного вжиття заходів, адекватних характеру й масштабам реальних і потенційних кібернетичних загроз життєво важливим інтересам людини та громадянина, суспільства й держави [35].

Нині виокремлюють такі загрози кібербезпеці й безпеці інформаційних ресурсів: уразливість об’єктів критичної інфраструктури, державних інформаційних ресурсів до кібератак; фізична та моральна застарілість системи охорони державної таємниці й інших видів інформації з обмеженим доступом [37].

Критична інфраструктура України – це системи та ресурси, фізичні чи віртуальні, що забезпечують функції й послуги, порушення яких призведе до найсерйозніших негативних наслідків для життєдіяльності суспільства, соціально-економічного розвитку країни та забезпечення національної безпеки [38, с. 14–15].

Україна має швидко, надійно й ефективно реагувати на будь-які кіберзагрози, що неможливо без інтегрування та чіткої взаємодії всіх наявних ресурсів суб’єктів кібербезпеки. На засіданні Національного центру кібербезпеки розглянуто заходи щодо вдосконалення системи зберігання, передачі та оброблення даних державних реєстрів і баз даних із застосуванням сучасних інформаційно-комунікаційних технологій.

Окрему увагу приділено розбудові інтегрованої захищеної системи державних реєстрів, баз даних і дата-центрів для оброблення та резервного збереження інформації й відомостей державних електронних інформаційних ресурсів. Підготовка відповідних фахівців для державних суб’єктів

забезпечення кібербезпеки визначена актуальним питанням, і така підготовка повинна відбуватись як в Україні, так і за її межами «відповідно до актуальних завдань, що стоять перед державою на цьому важливому напрямі» [39].

Останнім часом фіксується суттєва зміна форм, суб'єктів і наслідків реалізації основних загроз кібербезпеці держав. Так, кібератаки стають усе більш комплексними та складними, їх наслідки становлять загрозу ключовим національним інтересам, а їх організаторами або замовниками все частіше виявляються спецслужби іноземних держав чи терористичні організації.

Потреба реалізації ефективних заходів із протидії сучасним кібернетичним загрозам на національному рівні призводить до збільшення ролі в системах кібербезпеки країн спеціальних служб і правоохоронних органів, що мають контррозвідувальні функції й виконують завдання з протидії протиправній діяльності спецслужб іноземних держав і тероризму.

Аналізуючи системи кібербезпеки провідних країн світу, можна висновувати, що нині не існує уніфікованої моделі побудови кібербезпекової системи. Водночас важливим питанням залишається створення належної нормативно-правової основи для подальшої розбудови ефективних кіберспроможностей, закладення ключових підвалин кібербезпеки.

1.2. Аналіз вразливості інформаційно-телекомунікаційної системи

У 2020 р. хакери активізували атаки на бізнес-користувачів, установи та домогосподарства. Експерти сходяться на думці, що найближчі місяці принесуть нову хвилю кібератак. Ніякого нового типу інцидентів очікувати не варто — злочинці зосередяться на розробці доступних методів та інструментів. Згідно висновку Bitdefender, особливо небезпечними будуть 3 типи загроз: внутрішні інциденти, програми-вимагачі і атаки на ланцюжки поставок.

Внутрішні загрози

Дистанційні працівники — одна з улюблених цілей кіберзлочинців. Це пов'язано з тим, що люди, які працюють на самоті в квартирах, не можуть розділити робочі і домашні обов'язки і зазвичай не дотримуються корпоративних правил безпеки. Вони часто використовують бізнес-ноутбуки в особистих цілях або відкривають електронні листи з підозрілим вмістом.

Фахівці з безпеки визначають цю групу людей як внутрішню загрозу. Що робити, щоб обмежити свободу віддалених співробітників і таким чином мінімізувати ризик атаки? Один зі способів — впровадити інтегровану платформу захисту кінцевих точок і управління ризиками, доповнену аналізом людських ризиків. IT-відділи великих компаній зазвичай використовують інтегроване управління ризиками та аналітику для постійної оцінки, визначення пріоритетів і усунення помилок, створених людьми.

Програми-вимагачі

Організації, що стали жертвами таких атак, несуть дуже високі витрати. У минулому році атака програм-вимагачів на медичний центр у Вермонті обходилась установі у $1,5 млн на день. Представник установи визнав, що через 42 дні після атаки лікарня оцінила збитки приблизно у $63 млн, не рахуючи витрат на відновлення і експлуатацію систем.

Оскільки це дуже прибутковий сегмент для злочинців, схоже, 2021 р. буде відзначений жорсткою конкуренцією з боку угруповань шкідливих програм. Це призведе до подальшого розвитку інструментів атаки, а також Ransomoware as a Service.

Зловмисники також будуть націлені на середні й малі підприємства. Відтак, меншим організаціям варто переглянути політики безпеки, щоб зосередитися на виявленні тактик і методів, в основному пов'язаних зі складними атаками на корпорації та урядові установи.

Атаки на ланцюжок поставок

Згідно зі спостереженнями Bitdefender, малий і середній бізнес постраждав від рекордної кількості витоків даних. Найчастіше зловмисники використовували невірні конфігурації, що виникли в результаті поспішного переходу в режим віддаленої роботи. Більше того, експерти вважають, що існує ще багато «мертвих» точок безпеки. Проломи в безпеці відкривають двері для атак на ланцюжки поставок. Кіберзлочинці проявляють великий інтерес до секторів охорони здоров'я, освіти і міської інфраструктури [https://yur-gazeta.com/golovna/tri-naybilshi-kiberzagrozi-u-2021-r.html].

Розглянемо проблематику атак на ланцюг постачання докладнше:

Ціль атаки на ланцюг постачання. Ціль зловисників, що впроваджують скомпрометований код у програмний засіб, змінити сценарій дій і налаштування таким чином, щоб можна було контролювати систему віддалено і відкрити доступ до персональних даних користувачів (номер, дата видачі та CVV код) або розмістити інфіковане оновлення. Після отримання даних, здійснюють грошові переведання. Вони отримують кошти та інформацію, після цього виводять систему з ладу.

Принцип дії атаки. Атака на ланцюг поставок – це кібератака, що здійснюється, використовуючи довіру між компанією-виробником та її клієнтами. [6] Вона завдає шкоду організації, орієнтуючись на слабкі місця у ланцюгу постачання. Зловмисник ставить під загрозу один або кілька компонентів процесу розробки чи доставки. Така атака може використовувати підроблені чіпи, що задіяні у виробництві комп’ютера або мережевого обладнання. Або, атака може запровадити скомпрометований код у програмному засобі, що не викликає підозри. Є цілий ряд різних сценаріїв та методів, але головне, що ця атака використовує надійні канали для проникнення, щоб досягти своїх цілей.

Атака такого типу має свої особливості:

Компанії, у яких було здійснено атаку на ланцюг постачання, помічають втрату персональних даних або важливої інформації набагато пізніше, ніж проведено було атаку, таким чином чим більше часу проводиться атака, тим більше даних клієнтів скомпрометовано.

Здійснюється на основі довіри користувачів до продукту, який вони вже використовували, і бездоганної репутації компанії, що піклуючись про клієнтів випускає оновлення свого продукту. • Зараження може відбутися ще в ланцюгу постачання компанії-постачальника, а інфікований продукт з'явиться вже в першій ланці ланцюга постачання компанії, що користується її послугами.

Її можна порівняти з бомбою уповільненої дії, тобто на певному етапі ланцюга постачання впроваджується заражений компонент (виконуваний файл, спеціальний програмний засіб і т.п.), який пізніше, при завантажені користувачами програми, починає діяти за сценарієм зловмисників, і за короткий проміжок часу може інфікувати мільйони комп'ютерів користувачів.

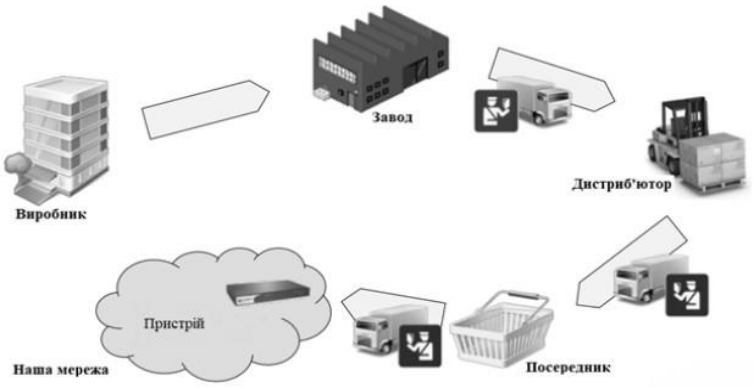


Рис.1.1. Схема атаки

Отже, в який момент можна інфікувати комп'ютер злочинним кодом?! Ми можем роздивитися схему ланцюга поставок на рис. 1. Потенційно кожна

сторона має вразливе місце і на будь-якому етапі можна замінити чіп на підроблений, встановити заражену програму, налаштувати обладнання так, щоб атаку Рис. 1. Схема ланцюга поставок можна було розпочати у будь-який момент. Але це не так просто, адже для ефективного проведення атаки потрібно знати:

яким чином можна інфікувати сайт, де користувачі завантажують програму, або вводять персональні дані;

які технічні засоби використовуються для роботи з веб-сайтом, або мають доступ до персональних даних користувачів;

які є вразливі місця чи помилки в політиці безпеки компанії;

з якими постачальниками співпрацює компанія;

як інфікувати систему, щоб це не було виявлено завчасно і т.д..

Аналіз досвіду компаній, що постраждали від здійснених вдалих атак на ланцюг постачання

Аналіз фінансових втрат від атаки

Перші атаки були проведені у 2013 році, кожна наступна була хитрішою та витонченою. Їх стратегії ставали складнішими і не зрозумілими. Якщо спочатку злочинці викрадали дані користувачів невеликих компаній з метою отримати гроші, то з часом вони намагалися добратися до великих фірм, де кількість клієнтів набагато більше, використовуючи невеликі, як проміжний етап. [1] [3]

Результат не змусив чекати, компанії втрачають репутацію, клієнтів, і велику кількість грошей, в яку входить і штраф у розмірі 4 % від річного світового обігу за попередній фінансовий рік для підприємства або 20 мільйонів євро, в залежності що більше, бо починаючи з 25 травня 2018 року усі організації мають виконувати основні вимоги нового європейського законодавства із захисту персональних даних

GDPR (General Data Protection Regulation). [3]

На діаграмі на рис. 2 зображено деякі випадки атак на ланцюг поставок великих компаній та їх приблизні фінансові втрати. Target була першою компанією, яка отримала збитки від цієї атаки, втрачено майже 162-мільйона доларів, скомпрометована персональна інформація (повне ім’я, адреса, електронна пошта, номер телефону) 110-мільйонів користувачів. В авіакомпанії пасажири очікували рейс, білети на який було продано, але компанія про це нічого не знала, тоді і була виявлена атака. 75 тисяч пасажирів не вирушило в дорогу, втративши гроші і особисті дані.[2]

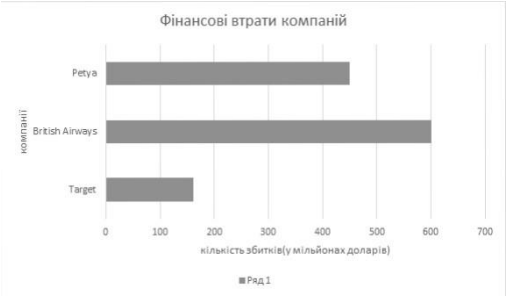


Рис. 1.2. Фінансові збитки компаній, після атаки на ланцюг поставок

Зловмисники змогли отримати доступ не тільки до основної інформації про банківські картки користувачів (ПІБ і номер картки), але також і до кодів перевірки дійсності карток (CVV). Виникло питання, як вони змогли отримати ці коди, якщо навіть сама авіакомпанія їх не зберігає.

Отже, був змінений скрипт на сайті авіакомпанії таким чином, щоб при здійсненні платежів хакери могли отримувати цей код разом з іншими даними. В результаті була здійснена крадіжка дуже великих масштабів та шкода репутації компанії. Схожий випадок був у компанії Ticketmaster, було скомпрометовано дані 40 тисяч клієнтів. Після встановленого оновлення від CCleaner більш ніж 2 мільйони користувачів під’єдналися до сервера зловмисників.

Тенденції атак в ланцюжку поставок програмного забезпечення і різновид методів її здійснення

Отже, компанії отримують великі штрафи, втрачають клієнтів та багаторічну репутацію, яку відновити дуже складно, повинні змінювати політику безпеки та в принципі підхід до захисту даних, і знайти зловмисників, після того як пройшов певний час – майже нереально.

У презентації «Вектор несподіваних атак: засобу оновлення програмного забезпечення» на RSA Conference у 2018-му році було представлено діаграму на рис. 3, в якій зображено яка кількість атак була та як з кожним роком зростає їх кількість. [4]

Схема атаки CCleaner була досить складною і складалася як мінімум з трьох етапів. Шкідливе ПЗ, запроваджене в популярну програму зі 100 млн активних користувачів, поширювалося цілий місяць. Пізніше з'ясувалося, що на командному сервері працював простий скрипт, який вибирав жертв для другого етапу атаки: ними ставали ті, хто, судячи по доменних іменах, міг виявитися співробітником великих IT-компаній та постачальників. На цьому етапі відібрали всього 40 комп'ютерів, на які потім відправили додаткове шпигунське ПЗ.

На наступному етапі злочинці ще більше звузили список жертв: зібравши і проаналізувавши інформацію з цих 40 комп'ютерів (ймовірно, вже вручну), вони вибрали чотири найбільш цікаві цілі. На ці пристрої встановили спеціально доопрацьовану версію ShadowPad – відомого шкідливого ПЗ, яким вже користуються китайські кіберзлочинці. Це і бу-

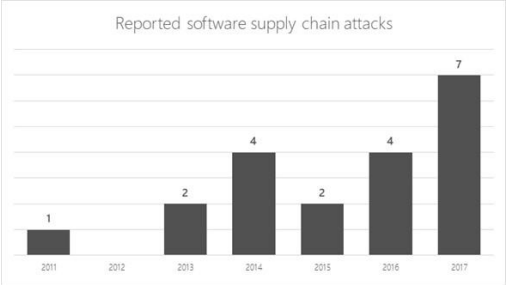


Рис. 1.3. Тенденції атак в ланцюжку поставок програмного забезпечення (джерело: презентація RSA Conference 2018 «Вектор несподіваних атак: засобу оновлення програмного забезпечення») Microsoft Security [7]

ло кінцевою метою атаки – доставити бекдор на комп’ютери певних співробітників великих компаній.

Це означає, що реалізувати атаку дуже складно і не під силу будь-кому. По-перше, для того, щоб знайти вразливе місце та проникнути в середу розробки програмного забезпечення, що є ціллю для зловмисника, потрібно багато часу, ресурсів та інформації про внутрішню роботу компанії. По-друге, сил та знань досвідчених програмістів, щоб створити атаку, що правдоподібно імітує усі процеси та непомітно впровадити злочинний код. Це має бути створена команда з фахівців, що знають яким чином захищена структура, яка є ціллю для нападу, зможуть написати заражений програмний код та впровадити його в певний комп’ютер, що є стратегічно важливим.

Також це потребує не малих коштів. Але якщо атаку вдасться здійснити, то зловмисники зможуть отримати персональні дані клієнтів, вивести з ладу техніку, знищити інформацію та викрасти велику суму грошей.

1.3. Дослідження міжнародного стандарту ISO/IEC 27001 і рішення для покращення захисту

Отже, атаки здійснюються успішно, але як можна від них захиститися?! Звісно, є стандарт ISO/IEC 27001, нова версія якого прийнята в 2013 році, але інформаційні технології розвиваються дуже швидко, тому виконання цього стандарту не гарантує захист від атаки здійсненної на ланцюг постачання. [5]

У стандарті прописано, як потрібно контролювати постачальників і поставлена конкретна задача: «Гарантувати захист активів організації, які доступні постачальникам та підтримувати узгоджений рівень інформаційної безпеки і надання послуг в відповідності з угодою з постачальником». [5] Але постачальник не обов'язково може мати доступ до активів компанії, він може бути роздрібним торговцем, або постачати певну техніку, та все одно його потрібно контролювати. Тим паче, часто постачальник вже передає заражене, але не активоване (тобто сценарій зловмисника ще не виконується) шкідливе програмне забезпечення, або технічне забезпечення, в яке встановлено підслуховуючий пристрій. Тобто загроза може надходити від постачальників, які працюють з постачальниками. Оскільки контрактні виробники часто працюють на тонкій маржі, вони іноді творчо підходять до створення додаткової маржі – наприклад, спокушаються більш дешевими запчастинами від незатверджених продавців. Компанія має уважно слідкувати за такими постачальниками та проводити періодичні перевірки, а також регулярно відвідувати їх співробітників в ділових цілях.

Будь-який тип атаки – це ризик, який жодна компанія не може собі дозволити. У той час як більшість компаній зосереджені на своїх внутрішніх кібер-ризиках, лише деякі в реальному часі можуть оцінити вразливість своїх ланцюжків поставок.

Всі компанії мають як мінімум два рівні (яруси) постачальників – Перший рівень (постачальники з прямим контрактом) та другий рівень (постачальники для постачальників першого рівня). Великі компанії чітко оцінюють

схильність до ризику постачальників першого рівня в процесі первісної оцінки та укладання контрактів. Зазвичай на цьому етапі відбувається невеликий огляд постачальників другого рівня. В результаті цього завантаженого інтерфейсом процесу огляду ризику кібератак може різко зрости після перших кількох місяців терміну дії договору і може продовжувати збільшуватися протягом терміну дії договору.

Для уникнення цієї загрози краще співпрацювати з невеликою кількістю перевірених постачальників, заключати з ними договори про аудит зі сторони замовника та постійний звіт про здійснення усіх заходів для забезпечення ефективного захисту інформації.

1.4. Різносторонні підходи до зменшення ризиків кібернетичних атак на ланцюг поставок

Керівники невеликих компаній помилково вважають, що їх бізнес не такий великий, щоб злочинці продумували атаку на нього, але це не так. По-перше атаку легше провести на таку компанію, бо вони навряд витрачають гроші на захист даних та створення і впровадження КСЗІ. По-друге кожна маленька компанія намагається працювати з великою, бо це постійний заробіток, тому злочинці використовують малі компанії як транспорт для інфікованого об’єкту. Ряд додаткових факторів, які також сприяють збільшенню ризику ланцюжка поставок, в тому числі:

Зростаючий обсяг і серйозність кібератак, що виходять від окремих осіб, організацій та державних установ;

Самозаспокоєність і / або нездатність як компанії-покупця, так і постачальника у моніторингу та оцінці реального / поточного кіберризику;

Підвищення складності кібератак – деякі з яких працюють від імені іноземних урядів;

Збільшення сміливості кібератак через нездатність ідентифікувати і бути осудженими;

Зміна рівня толерантності до ризику в компанії;

Хоча ризик кібератак на ланцюжок поставок не може бути усунутий, можна значно знизити ризик, навчаючи своїх постачальників і, проводячи постійні перевірки для них на всіх рівнях. Цей контроль дуже важливий, оскільки компанії продовжують передавати стороннім постачальникам критично важливі внутрішні і клієнтські процеси.

Конкретні кроки, які характеризують цей недогляд, включають наступне:

Контроль даних постачальників;

Контроль місця і інформації, де фізично зберігаються дані;

Контроль кількісті і імен системних адміністраторів у постачальників, які керують системами, які містять ваші дані;

Шифрування даних при передачі;

Гарантування, що все виправлення програмного забезпечення від відповідних постачальників програмного забезпечення встановлені на комп’ютерах ваших постачальників своєчасно;

Впевненість, що політики постачальника щодо доступу до систем як для активних, так і для звільнених співробітників (включаючи зміну / скасування імені користувача і пароля) часто розглядаються / переглядаються всіма співробітниками;

Перевірка політики постачальника щодо портативних пристроїв і безпеки технічних пристроїв; • Перевірка постачальника процедур безпеки бездротової мережі і можливості моніторингу;

Резервне копіювання всіх важливих даних здійснюється часто;

Контролювання, що постачальники підтримують всі брандмауери та антивірусне програмне забезпечення до останніх версій;

Регулярна перевірка всіх прав доступу / доступу до «критично важливих» файлів (піврічний аналіз бізнес-вимог для авторизації);

Перевірка, що у є документований і протестований план аварійного відновлення та оповіщення про ризики.

Якщо у ланцюжку поставок відбувається кібератака, слід:

Вжити негайних заходів, щоб визначити і ізолювати джерело атаки;

Негайно обмежити доступ до всіх даних;

Негайно повідомити про характер і серйозність атаки;

При необхідності повідомити інших потенційно дотичних постачальників;

Переконайтись, що план аварійного відновлення та оповіщення про ризики дотримується, а дії виконуються;

При необхідності і з вашого попереднього письмового дозволу повідомте про це у відділ по боротьбі з кіберзлочинністю ДБР (Державного бюро розслідувань);

Негайно перевірте, що всі міжмережеві екрани та антивірусне програмне забезпечення оновлено до останньої версії.

1.5 Постановка задач

Назва системи – Інформаційна система оцінки кіберзагроз

Мета існування системи – автоматизація процесу оцінки ІКС підприємства задля визначення ступеню захищеності від атак на логістичні ланцюги.

Запровадження ІС оцінки кіберзагроз є гарним прискорювачем роботи спеціалістів по оцінці захищеності ІКС. Додатково, ІС може підвищити достовірність результату за рахунок використання оцінок групи спеціалістів.

Облік відбувається на базі групи спеціалістів, групи документів, кількості документів у відповідності до визначеного часу.

Початкові дані (вхідні) - це БД документів, списки та характеристики спеціалістів, достовірна оцінка захищеності ІКС підприємства.

Характеристики системи за функціональністю:

– надання постійного доступу керівнику або групі керівників організації, а також спеціалістам до інтерфейсу програмного продукту;

– надання постійного доступу колегам до оперативної інформації про ІКС підприємства;

– формування вхідних даних відбувається на основі аналізу ІКС підприємства;

– кількість спеціалізованих робочих місць обмежується можливостями мережі;

– максимальне число клієнтів (місяць) також обмежується можливостями мережі;

– приблизне число записів для зберігання в БД – 10000;

– керівництво організації та відділ безпеки обмежує число споживачів інформації;

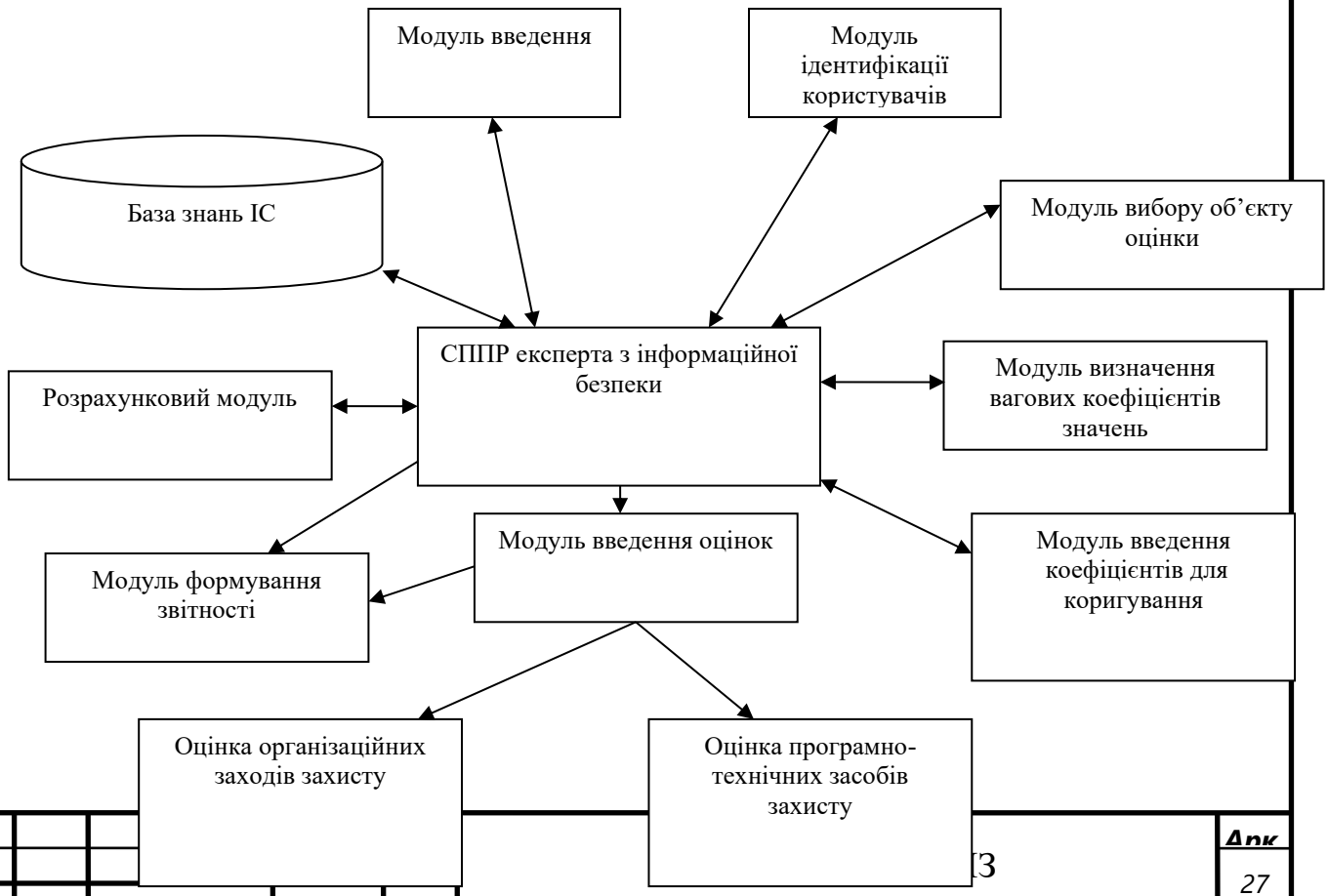
Розробка можливих видів забезпечення ІС оцінки кіберзагроз є результатом науково-дослідної роботи.

Перелік науково-технічної документації, що надається після закінчення робіт: пояснювальна записка; схема функціональної структури ІС оцінки кіберзагроз; опис функцій автоматизації; опис задач; опис інформації; опис створення інформаційної БД; вхідні дані; вихідні дані; алгоритми; опис процесу обробки даних; інструкції.

2. ПРОЕКТУВАННЯ ТА МОДЕЛЮВАННЯ ІС оцінки кіберзагроз

2.1 Структура ІС оцінки кіберзагроз

Проведений аналіз предметної області дослідження дозволив сформувати структурну схему функціональних модулів ланцюг постачання, яка представлена на рисунку 2.1.



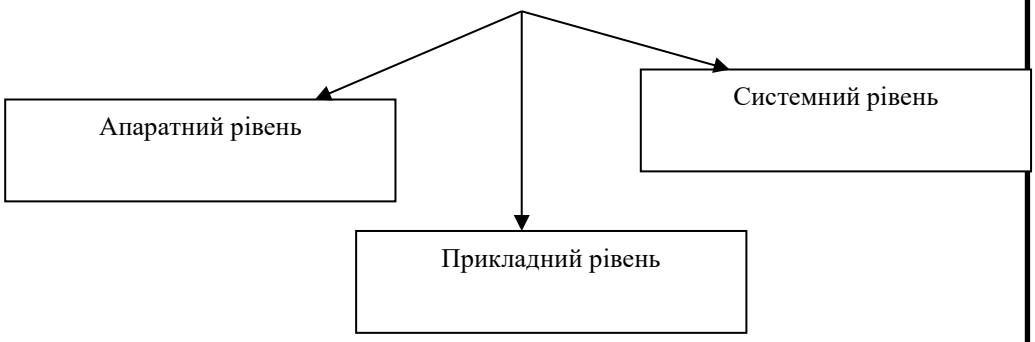


Рис. 2.1. Структурна схема функціональних модулів інформаційної системи

Функціональні модулі ІС оцінки кіберзагроз:

– БЗ ІС;

– Модуль розрахунків;

– Модуль формування звітності;

– Модуль вибору об’єкту;

– Модуль визначення та введення коефіцієнтів для коригування;

– Модуль введення оцінок (оцінка організаційних заходів захисту + оцінка програмно-технічних засобів захисту на усіх рівнях);

– Модуль введення даних про спеціалістів;

– Модуль ідентифікації.

Функціональні задачі кожного пункту – детальніше далі. Модуль вибору об’єкту оцінки – можливість для спеціалістів додавати та видаляти об’єкт з бази даних. Під час формування групи спеціалістів цей пункт є дуже

важливим, так як кожен експерт зможе оцінити один і той же об’єкт, а програма проведе аналіз отриманих результатів, після чого сформує звітність по даним об’єктам.

Модуль визначення та введення коефіцієнтів для коригування – визначення вагомості факторів оцінки та врахування вагомості кожного експерта.

Оцінка експертами вартості інформації підприємства має багато критеріїв. Основою даної моделі є висновки та пропозиції (оцінки). Далі йде узагальнення результатів. Це у своїй суті прогноз, або послідовна реалізація певних правил:

1. Опитування спеціалістів у кілька етапів;
2. Кількісний характер оцінок, наданих групою спеціалістів.
3. Статистика;
4. Інформування спеціалістів задля подальшого коригування їхніх думок.

Головним принципом моделі є незалежне опитування думок спеціалістів (збирання оцінок) у часі. Далі зібрану інформацію потрібно обробити задля формування статистичних даних.

Значення ймовірної величини визначаємо як середню величину оцінок спеціалістів. Нижче формула, де: N – кількість спеціалістів; O_i – оцінка i-го експерта, $i = 1 \div N$.

$$\overline{O} = \frac{1}{N}\sum_{i=1}^{N} O_i \qquad (2.1)$$

Для відображення статистики розбіжності у думках спеціалістів визначаємо дисперсію D_0 отриманих оцінок. Нижче формула:

$$D_o = \frac{1}{N-1}\sum_{i=1}^{N}(\overline{O} - O_i)^2 \quad (2.2.)$$

Середньоквадратичне відхилення:

$$\sigma_o = \sqrt{D_0} \quad (2.3)$$

Далі потрібно визначити єдину загальну оцінку для всієї групи опитуваних. Робимо це через розрахунок коефіцієнту варіації. Нижче формула:

$$K_B = \frac{\sigma_o}{\overline{O}} \quad (2.4)$$

Далі важливим пунктом є компетентність *i*-го експерта в групі опитуваних. Для цього потрібно використати коефіцієнт компетентності. Нижче формула:

$$K_K^i = \frac{O_i - \overline{O}}{\overline{O}} \quad (2.5)$$

Реалізації експертної моделі:

– Вирішення завдання експертної класифікації оцінок ваг з погляду показників, для відображення об'єктивного стану ІКС на підприємстві;

– Ознаки потрібно оцінити (за шкалою балів);

– Розрахунок за пріоритетністю критеріїв долі кожного еталонного показника. Один з таких методів - побудова матриці коефіцієнтів переваг при попарному порівнянні критеріїв.

Визначення оцінки (+ вагомість експерта). Нижче формула:

$$\overline{O}_i = \frac{\sum P_j \cdot O_{ij}}{\sum_{j=1}^{R} \gamma_j} \qquad (2.6)$$

$\overline{O}_i$ – усереднена оцінка за вагомістю експерта, $i=1,N$, O_{ij} – виставлена оцінка j-го експерта для i-го показника, γ_j – ранг j-го експерта.

Далі йде визначення загальної оцінки ступеню захищеності інформації на підприємстві. Нижче формула:

$$S = \sum \overline{O_i} \cdot \gamma_j \qquad (2.7)$$

Модуль введення оцінок - це набір 2 під-модулів. Це:

- оцінка організаційних заходів захисту, які використовуються на об’єкті оцінки;
- оцінки програмно-технічних засобів захисту інформації.

Також, оцінка засобів захисту інформації (програмно-тех) складається з таких 3 рівнів оцінки захисту інформації:

- апаратний;
- системний;
- прикладний.

Формування звітності виконується залежно від користувацьких запитів ІС та форм, які встановлювались.

Модуль розрахунків обробляє результати оцінювання та виконує різного роду розрахунки відповідно до апарату, представленому в БЗ ІС.

БЗ ІС – ключова в ІС оцінки кіберзагроз. Складові:

- математичний апарат для обробки інформації;

– правила формування звітності;

– зберігання оцінкових листків.

Введення спеціалістів потрібне для:

– коригування;

– додавання та видалення спеціалістів;

– зміну вагових коефіцієнтів.

Ідентифікація потрібна для ідентифікації користувачів та їх повноцінної роботи в межах їх повноважень.

Дана структура забезпечує проведення повноцінної та достовірної оцінки об’єкту в плані захищеності ІКС.

2.2 Розробка UML-діаграм функціонування системи

Користувачі ІС оцінки кіберзагроз є системний адміністратор (йому надаються повні права доступу до програмного продукту) та експерт (спеціаліст, який повинен працювати з самою системою). Експерт слідкує за вчасним налагодженням системи, підтримкою працездатності, налагодження БД. Адміністратор має права інших користувачів системи. Сюди входять як права експерта з безпеки інформації, так і керівника самого підприємства.

У інших користувачів права відрізняються (мається на увазі, не перетинаються). Експерт має права на проведення Так, експерт в оцінки документів, маніпуляції з БД, перегляд звітності, зміна критеріїв оцінювання. З іншого боку, керівник має права на перегляд документів, збільшення кількості спеціалістів, маніпуляції з БД (під’єднання/від’єднання), додавання

документів. Графік використання заданої системи у вигляді діаграми на рисунку 2.2.

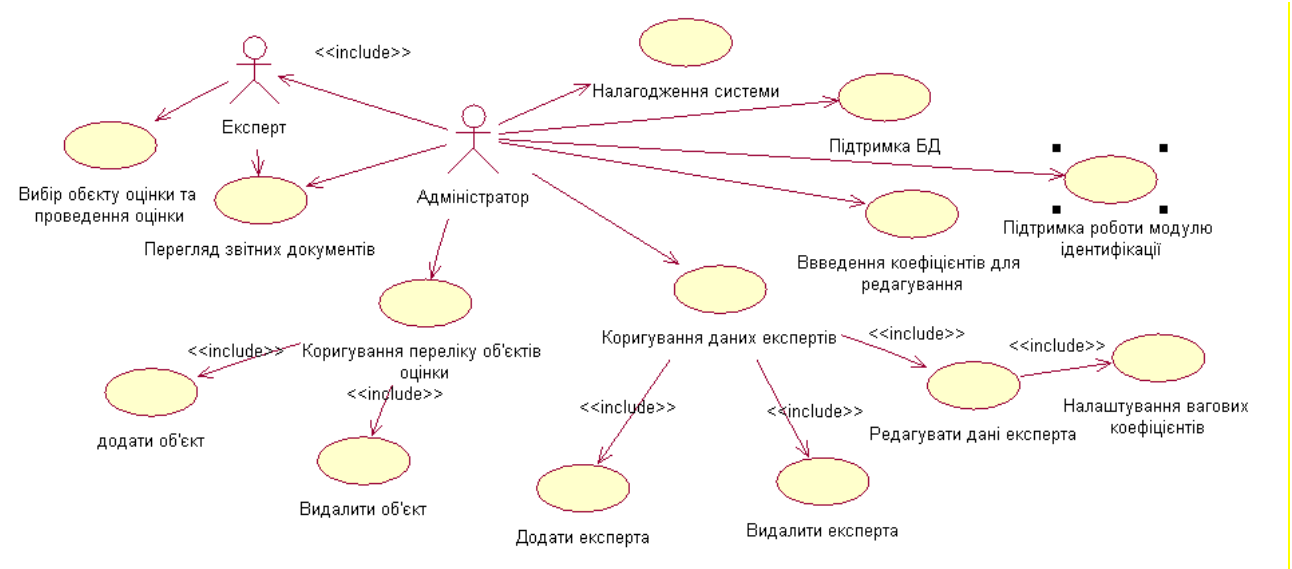
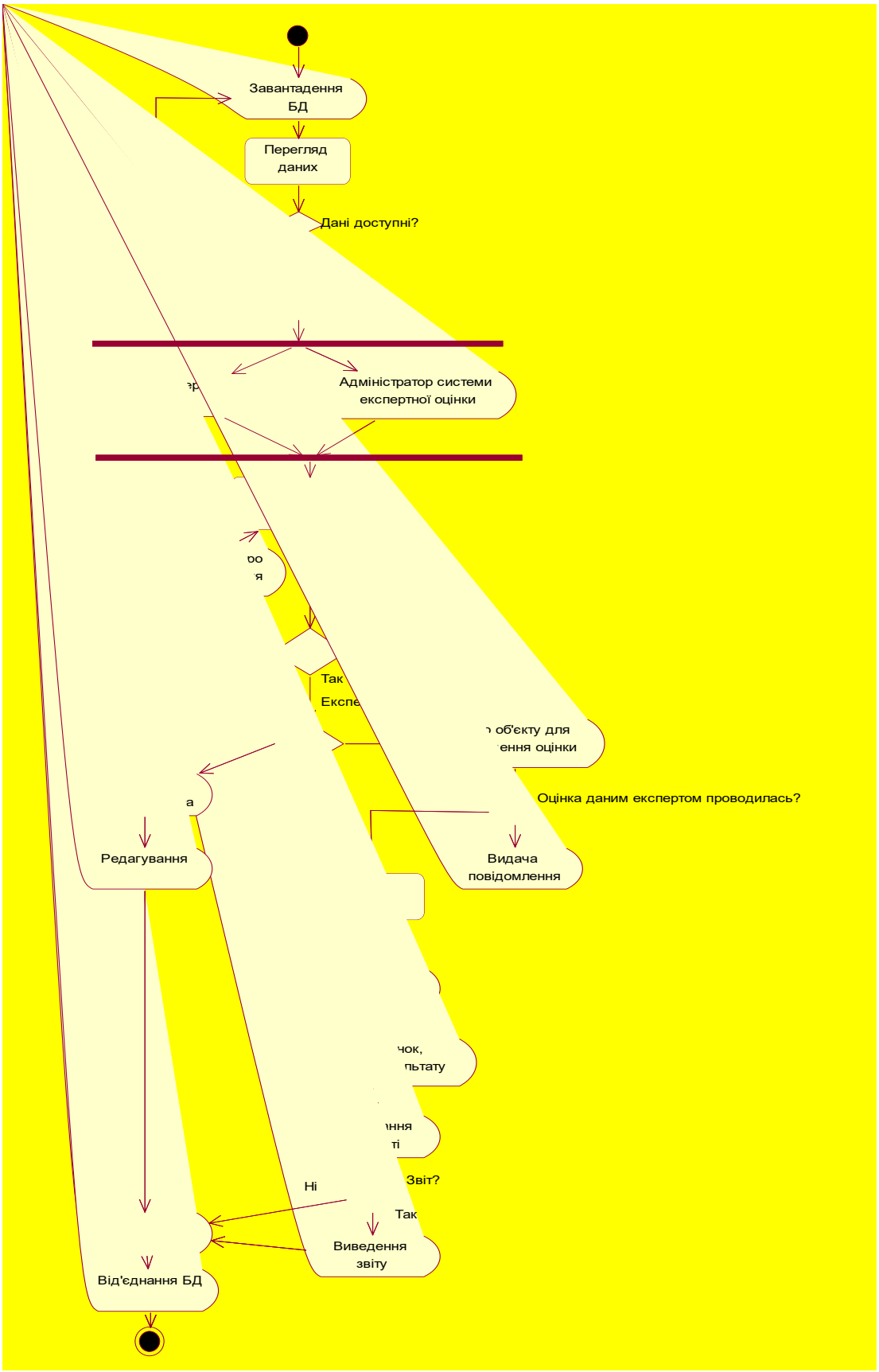


Рисунок 2.2 – Графік використання заданої системи у вигляді діаграми

Графік активності ІС у вигляді діаграми представлений на рисунку 2.3. Початковим кроком роботи з ІС є ввімкнення системи.



Зм	Арк	№ докум	Підпис	Дата	КІК.КР.Б-125-09-ПЗ	Арк 34

Рисунок 2.3 – Графік активності ІС оцінки кіберзагроз у вигляді діаграми

Важливим етапом є підключення БД. Якщо все зроблено вірно, наступним кроком буде завантаження інтерфейсу з опцією вибору користувача. Наступний етап – введення логіну та паролю у діалоговому вікні. Далі, якщо все виконано вірно, кожен користувач отримає індивідуальне робоче вікно. Також, важливо не забути про збереження даних як тільки будуть проведені всі маніпуляції з системою. Фінальний крок: потрібно від'єднати базу даних та вийти з ІС оцінки кіберзагроз.

Був побудований графік використання даної системи, а також графік її активності – у вигляді діаграм.

2.3 Вибір програмного засобу для реалізації ІС

Для створення інформаційної системи оберемо веб-орієнтовану реалізацію. Отже, для вибору стеку розробки проведемо порівняльний аналіз основних мов бек-енду PHP та ASP.Net.

PHP означає препроцесор гіпертексту (раніше він використовувався для позначення особистої домашньої сторінки), і це мова програмування загального призначення, це означає, що з його допомогою можна писати велику кількість додатків, що мають різні домени. PHP був розроблений в першу чергу для створення веб-сайтів, тобто для цілей веб-розробки.

PHP також відома як мова сценаріїв на стороні сервера і тому в основному використовувався для створення статичних веб-сторінок або протилежних динамічним. PHP не обмежується їх розробкою, він також використовується

для розробки веб-додатків. Але є одна заковика, і це факт, що сценарії PHP можна зрозуміти і працювати з ними, тільки якщо на сервері є PHP. І якщо до цих сценаріїв звертаються клієнтські комп'ютери, то все, що потрібно, - це веб-браузер і нічого більше.

Кодування заповнене тегами PHP, а всі розширення закінчуються на '.php'. Давайте дізнаємося більше про мову сценаріїв. Функції мови сценаріїв аналогічні функціям сценаріїв, вони містять список інструкцій, які інтерпретуються при виконанні програми. Це в основному використовується для виконання звичайних завдань програми. Сценарії інтерпретуються відповідно до серверів, будь то на стороні сервера або на стороні клієнта. І, як було сказано раніше, PHP є серверною мовою. Але його можна розмістити в HTML-сторінках.

Це ще не все, що його можна використовувати в поєднанні з веб-системами, які є або шаблонними, або системами управління контентом. PHP також корисний, коли справа стосується роботи з веб-фреймворками. Є багато переваг використання PHP, але ми розглянемо їх під час порівняння з asp.net від компанії-розробника dot net.

ASP.NET

Простіше кажучи, це фреймворк для веб-додатків. І той, який є відкритим вихідним кодом, що означає, що користувачі можуть переглядати програмне забезпечення, вносити в нього зміни і ділитися ним з ким завгодно. Він був розроблений постачальником послуг з розробки програмного забезпечення Microsoft.

Основна мета цього - надати платформу для створення динамічних веб-сайтів разом з додатками і послугами. Оскільки він розроблений компанією-розробником dot net, він може бути написаний тільки на мовах програмування

.NET. Крім того, йому дев’ятнадцять років, що запустився в січні 2002 року, і воін все ще дуже ефективний з точки зору продуктивності.

Він підтримує всі новітні операційні системи: Windows, Linux, а також macOS. Ця структура веб-додатків створюється за допомогою Common Language Runtime. Компанія-розробник dot net надає структуру, яку можна використовувати для створення найрізноманітніших додатків, наприклад консольних, веб-додатків і т. Д. Але послуги розробки asp.net вигідні тільки тоді, коли справа стосується розробки веб-додатків і сервісів. Ось чому він відомий як підмножина .NET Framework. Фреймворк asp.net в основному призначений для роботи з HTTP. І це також дуже зручно для інтеграції Javascript, HTML і CSS.

Чим ASP.NET краще?

Є багато причин, за якими робота зі службами розробки ASP.NET вигідна. Деякі з них згадані нижче:

Це розширена платформа: платформа asp.net розширює платформу .NET. Він оснащений деякими інструментами та бібліотеками, яких немає в попередніх фреймворках. Розширення MVC і Editor - це деякі з веб-шаблонів, для яких існують певні бібліотеки. Ці бібліотеки включені в структуру asp.net.

Продуктивність: коли справа доходить до продуктивності, asp.net виявляється краще, ніж його конкуренти.

Кодування: він підтримує написання бекенд-коду для всіх типів логіки на C #. А також для доступу до даних.

PHP	ASP.NET
Гнучка розробка програмного забезпечення	створено Microsoft

Легко для новачків	Підтримує всі мови .NET
Кросплатформеність	Кросплатформеність
Оснащений розширеними функціями	Можливості можуть бути додані і видалені
Зв'язок з усіма різними базами даних	Висока надійність, першокласна продуктивність
серверна мова	відкрите джерело
низька продуктивність	Складні сторінки, проблеми з продуктивністю
Неможливо управляти великою кількістю додатків	недостатня абстракція

Враховуючи, що для даної інформаційної системи висока надійність є головним критерієм для вибору інструментарію, отже зупинимо свій вибір на ASP.Net.

3.ПРОГРАМНА РЕАЛІЗАЦІЯ ІНФОРМАЦІЙНОЇ СИСТЕМИ ОЦІНКИ КІБЕРЗАГРОЗ

3.1. Розробка структури системи

На даному етапі кваліфікаційної роботи сформовано та проаналізовано задачі, які повинна виконувати інформаційної системи оцінки кіберзагроз щодо оцінки захищеності логістичної мережі підприємства. Запропоновано загальний алгоритм роботи системи підтримки прийняття рішень експерта з інформаційної безпеки щодо оцінки захищеності інформаційно-телекомунікаційної системи та реаліовано БД системи. Для реалізації системи обрано архитектурний паттерн MVC, на якому грунтується ASP.Net MVC.

MVC - це архітектурний принцип, згідно з яким веб-додаток видаляє компоненти Model View Controller. За цією моделлю додатків, користувацького інтерфейсу та взаємодії з користувачем, розділеним таким чином, для модифікації одного з компонентів, що відображає мінімальний вплив на інші. Таке розділення спрощує управління окремими приватними додатками, що сприяє їх розробці, зміні та тестуванню.

Дизайн, керований доменом (DDD) - набір принципів і схем, що допомагають розробникам створювати витончені системи об'єктів. При правильному застосуванні оновлення створюється створення програмних абстракцій, які називаються моделями предметних областей. У ці моделі входить сложна бізнес-логіка, що впливає на зміну між реальними умовами використання продуктів і кодами. DDD не є якоюсь або конкретною технологією чи методологією. Це набір правил, що дозволяють приймати

правильні проектні рішення. Даний підхід дозволяє значно прискорити процес проектування програмного забезпечення у незнаній предметній області.

Підхід DDD корисний у ситуації, коли розробник не є спеціалістом у галузі розробленого продукту. До прикладу: програміст не може знати всі області, в яких потрібно створити ПО (банківське діло, металургія, вираження бананів), але не за допомогою правильних презентаційних структур, за допомогою проблемно-орієнтованого підходу, може без зусиль запровадити додаток, основуючись на ключових моментах та знаннях робочої області.

Також в кваліфікаційні роботі реалузовано БД даних системи, схема якої навелена на рис.3.1:

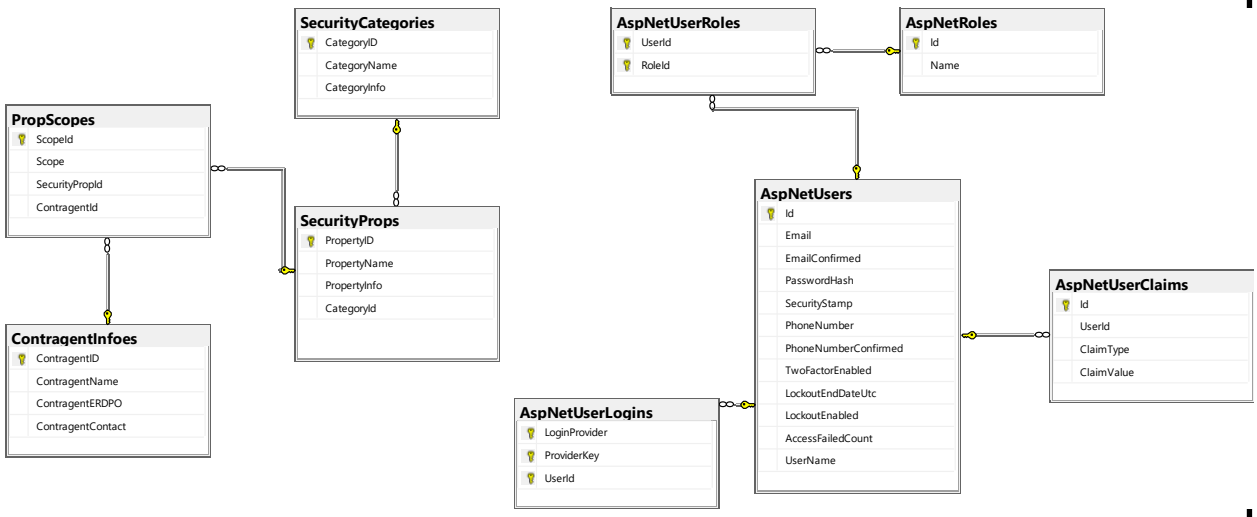


Рисунок 3.1

При вході в інформаційну систему експертів відбувається запит їх логіну та паролю і після успішної процедури ідентифікації завантажується його дані та експерт може проводити процедуру оцінювання. Після проведення оцінювання відбувається формування експертного висновку. Далі проводиться зберігання даних та пропонується вихід із системи оцінювання.

3.2 Інтерфейс інформаційної системи оцінки кіберзагроз

Вікно реєстрації нового експерта представлено на рисунку 3.2 і містить наступні поля:

– поле введення імені експерта – логіну;

– поле введення паролю експерта;

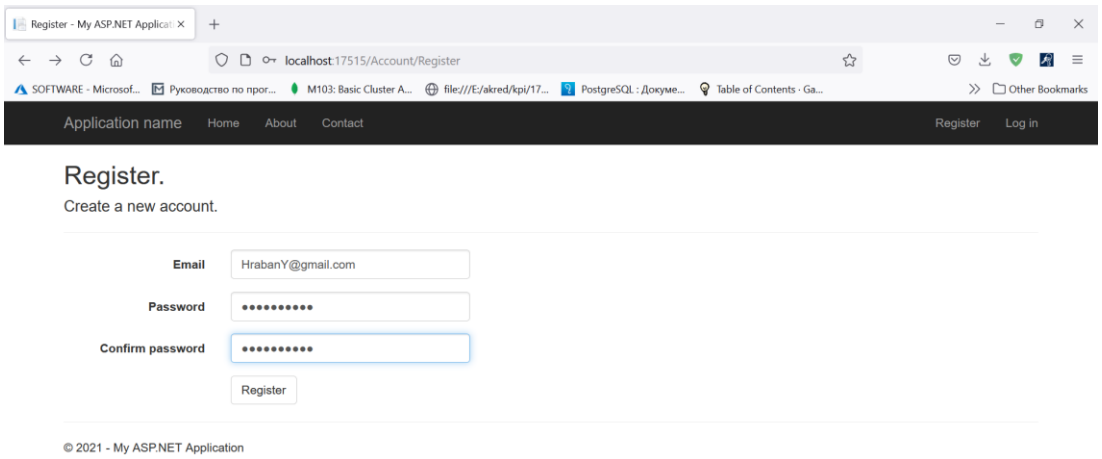


Рисунок 3.2

Після реєстрації експерта-користувача на його поштову адресу приходить запит на підтвердження, про що в браузері з’являється відповідне повідомлення.

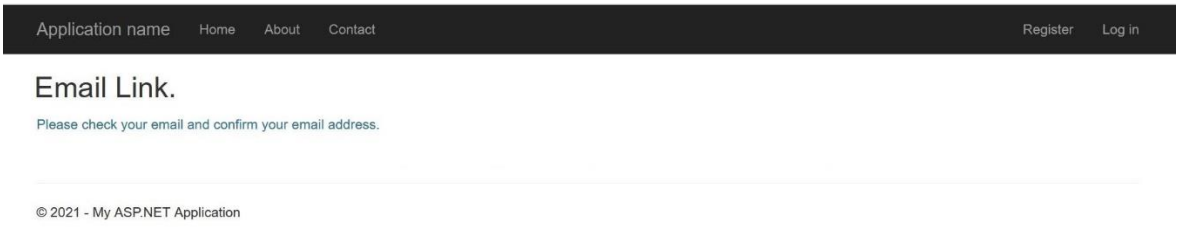


Рисунок 3.3

Якщо користувач переходить за відповідним лінком відображується повідомлення про успішну реєстрацію.

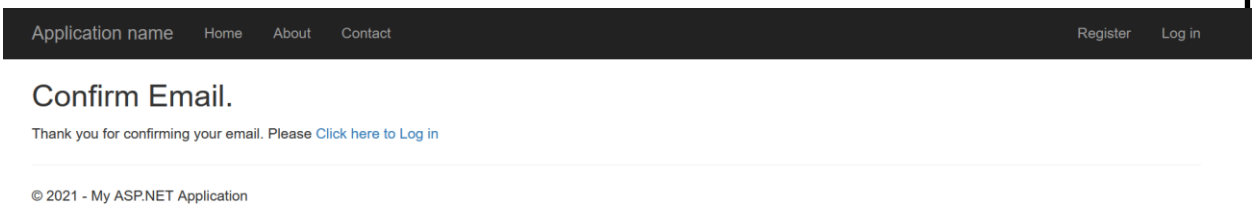


Рисунок 3.4

Після реєстрації експерта у системі відбувається процедури авторизації, рисунок 3.6. Необхідним є заповнення представлених полів.

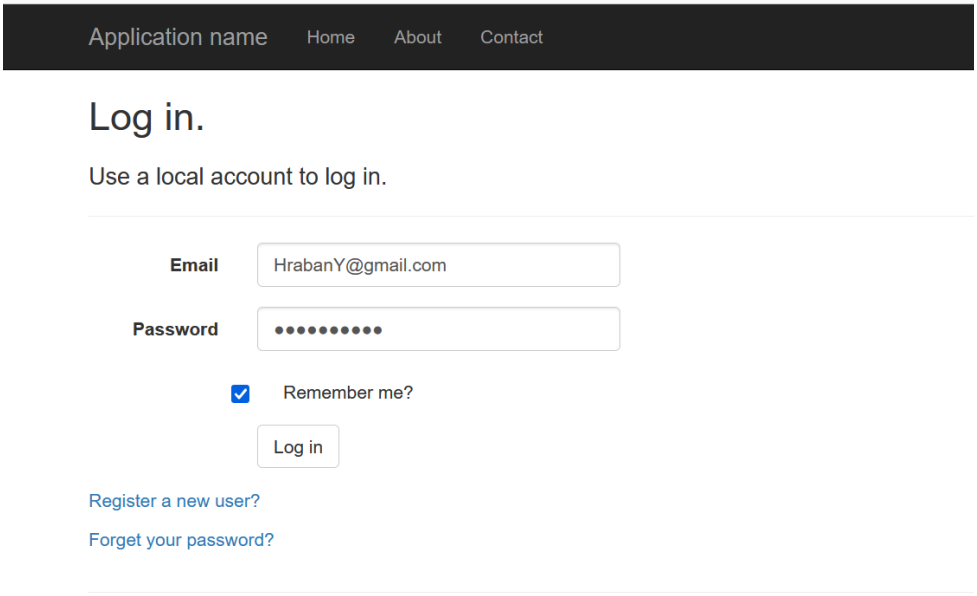


Рисунок 3.5

На головній сторінці (Home Page) наводиться перелік контрагентів, що належать до логістичної мережі підприємства. Даний додаток дозволяє редагувати існуючих та додавати нових учасників логістичної мережі, до яких буде застосовано модель аналізу заходів безпеки.

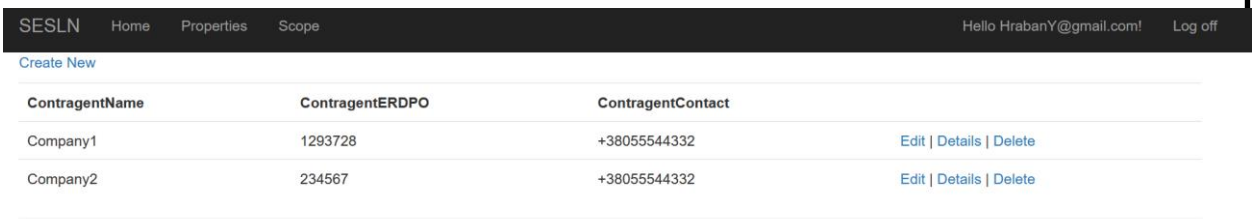


Рисунок 3.6

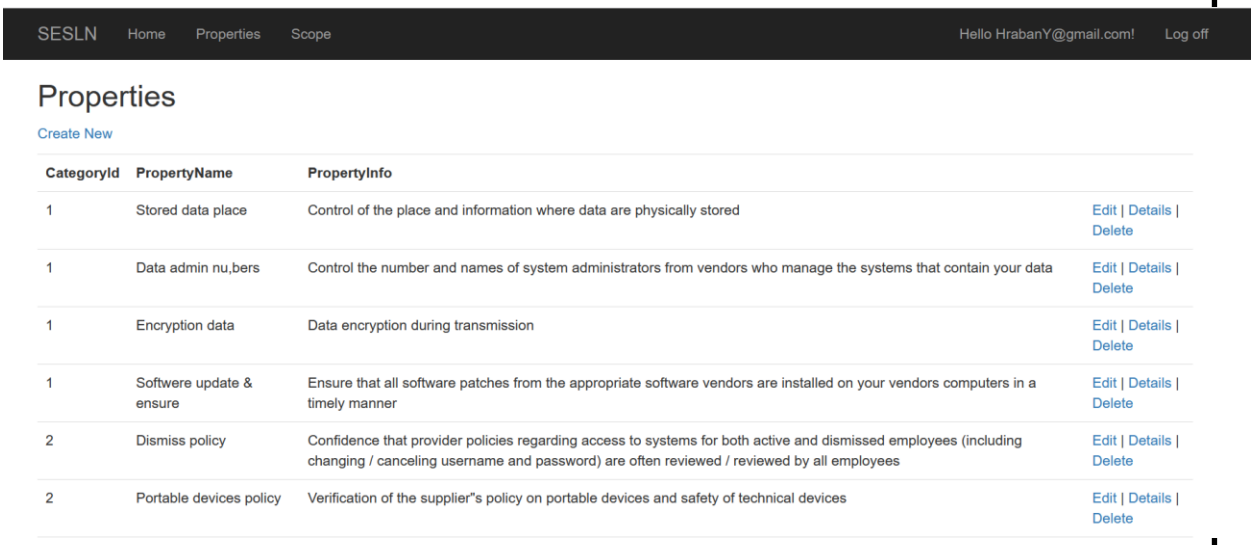
Оцінка наявності складової захисту учасника логістичної мережі та її продуктивності та ефективності відбувається за наступними категоріями, рисунок 3.8:

– контроль даних постачальника ();

– своєчасність оновлення програмного сервісного програмного забезпечення, антивірусів та політики безпеки;

– заходи резервування даних та можливості відновлення даних.

Загальний перелік можливих властивостей за якими відбуваєтсья оцінювання наведено на рисунку 3.7. За необхідності даний перелік може бути розширено, що не вплине на адекватність моделі та коректність розрахунків.



CategoryId	PropertyName	PropertyInfo	
1	Stored data place	Control of the place and information where data are physically stored	Edit | Details | Delete
1	Data admin nu,bers	Control the number and names of system administrators from vendors who manage the systems that contain your data	Edit | Details | Delete
1	Encryption data	Data encryption during transmission	Edit | Details | Delete
1	Softwere update & ensure	Ensure that all software patches from the appropriate software vendors are installed on your vendors computers in a timely manner	Edit | Details | Delete
2	Dismiss policy	Confidence that provider policies regarding access to systems for both active and dismissed employees (including changing / canceling username and password) are often reviewed / reviewed by all employees	Edit | Details | Delete
2	Portable devices policy	Verification of the supplier"s policy on portable devices and safety of technical devices	Edit | Details | Delete

Рисунок 3.7

На вкладці Scope оцінювання експерту пропонується оцінити стан кіберзахисту одного з контрагентів логістичного ланцюга. Оцінки виставляються в тих межах, які представлено напроти кожного поля виставлення оцінки.

SESLN Home Properties Scope Hello HrabanY@gmail.com! Log off

Scope

Create New

ContragentName	PropertyName	PropertyInfo	Scope	
Company1	Stored data place	Control of the place and information where data are physically stored	1	Edit | Details | Delete
Company1	Data admin nu,bers	Control the number and names of system administrators from vendors who manage the systems that contain your data	2	Edit | Details | Delete
Company1	Encryption data	Data encryption during transmission	2	Edit | Details | Delete
Company1	Softwere update & ensure	Ensure that all software patches from the appropriate software vendors are installed on your vendors computers in a timely manner	1	Edit | Details | Delete
Company1	Dismiss policy	Confidence that provider policies regarding access to systems for both active and dismissed employees (including changing / canceling username and password) are often reviewed / reviewed by all employees	3	Edit | Details | Delete
Company1	Portable devices policy	Verification of the supplier"s policy on portable devices and safety of technical devices	3	Edit | Details | Delete
Company1	Security & monitoring network	Verification of the provider of wireless network security procedures and monitoring capabilities	1	Edit | Details | Delete

Рисунок 3.8

Після заповнення всіх форм по виставленню балів можна переходити до формування висновку. Так як розрахунковий модуль системи вже порахував орієнтовну експертну оцінку, формується висновок встановленого зразку, рисунок 3.9.

Результат представляється у вигляді рейтингового показника – визначений в балах. В залежності від набраної кількості балів виводиться висновок щодо захищеності ІКС та її рівня захищеності, рисунок 3.10.

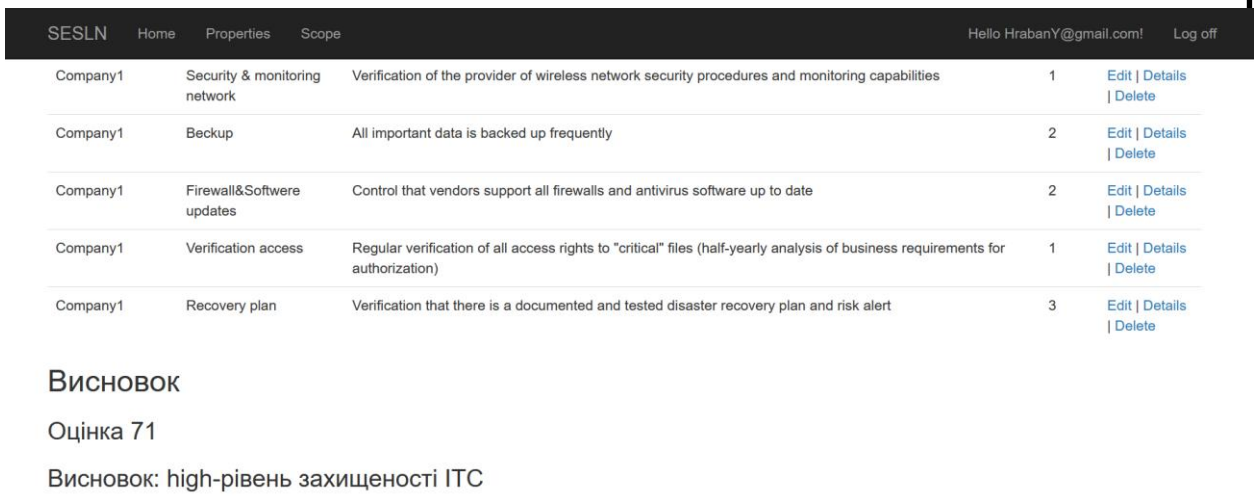


Рисунок 3.9

Представлений інтерфейс програмного продукту має зручний вигляд та простий у користування. Ряд запобіжних заходів дозволяє отримати коректно заповнені форми оцінювання з відсутніми пустими полями, рисунок 3.10

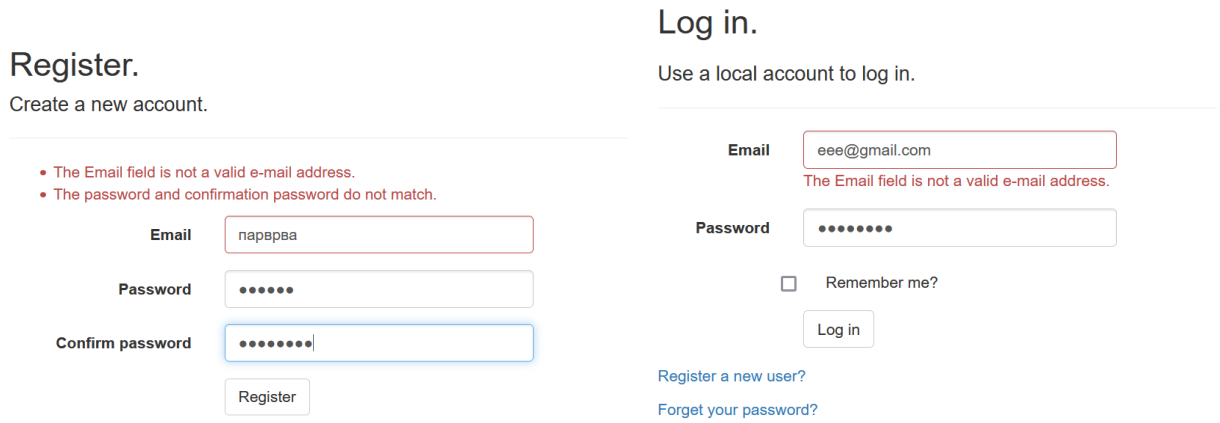


Рисунок 3.10 – Вигляд службових повідомлень

Розроблений інтерфейс програмного продукту є досить простим у користуванні, що не вимагає додаткових витрат на навчання персоналу та інформативним щодо проведених оцінок. Додатково слід зазначити наявність

запобіжних засобів, які обмежують повторне оцінювання об’єкту та коригування своїх даних експертами.

ВИСНОВКИ

Проведені дослідження дали нам змогу визначити особливості та засоби протидій кіберзагрозам у сучасних реаліях життя. Були також описані та проаналізовані основні загрози підприємствам. Були визначені особливості кібератак. Також, розібрані деякі засоби протидії несанкціонованим діям.

Була проведена розробка алгоритмів функціонування системи, а саме запропоновано загальний алгоритм роботи інформаійної системи оцінки кіберзагроз, реалізовано БД системи та розрахунковий модуль. Інтерфейс користувача є гнучким та забезпечує контроль коректності введення даних. Приведено детальний опис інтерфейсної частини програмного продукту.

Було представлено проектування ІС оцінки кіберзагроз, запропоновано структуру системи до складу якої входять користувачі, функції системи, накопичувач інформації по запитах, базу даних, ядро системи, статичні звіти, інтерфейси користувачів. Розроблено та представлено діаграму активності та використання ІС оцінки кіберзагроз. Проведено вибір програмного засобу для реалізації запропонованої системи.

1. Стратегія національної безпеки Украї-ни : Указ Президента України від 26.05.2015 No 287/2015 [Електронний ресурс]. – Режим доступу : http://zakon4.rada.gov.ua/laws/show/287/2015.2. Дорожня карта Партнерства у сфері страте-гічних комунікацій між Радою національної без-пеки і оборони України та Міжнародним секре-таріатом НАТО [Електронний ресурс]. – Режим доступу : http://mfa.gov.ua/mediafiles/sites/nato/files/Roadmap_Ukr.pdf.3. Стратегія кібербезпеки України : Указ Пре-зидента України від 15.03.2016 No 96/2016 [Електро-нний ресурс]. – Режим доступу : http://zakon3.rada.gov.ua/laws/show/96/2016.4. Шеломенцев В.П. Правове забезпечення систе-ми кібернетичної безпеки України та основні напря-ми її удосконалення / В.П. Шеломенцев // Боротьба з організованою злочинністю і корупцією (теорія і практика). – 2012. – Вип. 1. – С. 312–320.5. Лікан В.А. Стратегічні комунікації : [словник] / В.А. Ліпкан, Т.В. Попова ; за заг. ред. В.А. Ліпкана. – К. : О.С. Ліпкан, 2016. – 416 с.6. Ліпкан В.А. Консолідація інформаційного законодавства України : [монографія] / В.А. Ліп-кан, М.І. Дімчогло ; за заг. ред. В.А. Ліпкана. – К. : О.С. Ліпкан, 2014. – 416 с.7. Ліпкан В.А. Інкорпорація інформаційного за-конодавства України : [монографія] / В.А. Ліпкан, К.П. Череповський ; за заг. ред. В.А. Ліпкана. – К. : О.С. Ліпкан, 2014. – 408 с.8. Мандзюк О.А. Стан та перспективи розвитку правового режиму податкової інформації в Україні : [монографія] / О.А. Мандзюк. – К. : Дорадо-Друк, 2015. – 192 с.9. Баскаков В. Тенденції адміністративної відпо-відальності у сфері інформаційної безпеки / В. Бас-каков, О. Стоєцький // Актуальні проблеми право-охоронної діяльності : матеріали наук.-практ. конф. (Київ, 20 груд. 2010 р.). – К., 2010. – С. 64–66. 10. Дімчогло М.І. Консолідація інформаційного законодавства як напрям боротьби з тероризмом / М.І. Дімчогло // Інформаційні технології боротьби з тероризмом : матеріали наук.-практ. конференції. – К., 2012. – С. 22–24.11. Залізняк В.А. Інформаційна безпека як інсти-тут інформаційного права України / В.А. Залізняк // Актуальні проблеми зміцнення державності і націо-нальної єдності України : матеріали наук.-практ. кон-ференції. – К., 2010. – С. 46–48.12. Збінський Є.Ф. Захист податкової таємниці як складова інформаційної безпеки / Є.Ф. Збінський // Ім-перативи розвитку цивілізації. – 2015. – No 2. – С. 84–85.13. Рудник Л.І. Право на доступ до інформації : дис. ... канд. юрид. наук : спец. 12.00.07 «Адміністративне пра-во і процес; фінансове право; інформаційне право» / Л.І. Рудник ; Національний університет біоресурсів і природокористування України. – К., 2015. – 247 с.14. Логінов О.В. Гносеологічний аспект управлін-ня інформаційною безпекою України / О.В. Логінов // Науковий вісник Юридичної академії МВС Украї-ни. – Дніпропетровськ, 2004. – No 2. – С. 153–161.15. Максименко Ю.Є. Міжнародно-правові та європейські засади забезпечення безпеки інформа-ційного суспільства / Ю.Є. Максименко // Акту-альні проблеми забезпечення національної безпеки України : матеріали наук.-прак. конф. (м. Київ, 6 груд. 2005 р.) / Київський націон. ун-т внутр. справ. – К., 2005. – С. 58–66.16. Стоєцький О.В. Адміністративна відпові-дальність за порушення у сфері інформаційної безпе-ки України : автореф. дис. ... канд. юрид. наук : спец. 12.00.07 «Адміністративне право і процес; фінансове право; інформаційне право» / О.В. Стоєцький ; Запо-різький нац. ун-т. – Запоріжжя, 2013. – 19 с.17. Татарникова К.Г. Засади комплексної кодифі-кації законодавства про інформацію / К.Г. Татарни-кова // Проблеми державного будівництва в Україні : матеріали XVIII Міжнар. наук.-практ. конф. профе-сорсько-викладацького складу «Україна в Євроінте-граційних процесах» (м. Київ, 16–17 лют. 2013 р.). – К., 2013. – Вип. 21. – Т. 1. – С. 226–229.18. Череповський К.П. Елементи структуризації міжнародного інформаційного права / К.П. Черепов-ський // Правові та політичні проблеми сучасності : матеріали наук.-практ. конференції. – К., 2012. – С. 40–44.19. Шепета О.В. Адміністративно-правові засади технічного захисту інформації : автореф. дис. ... канд. юрид. наук : спец. 12.00.07 «Адміністративне право і процес; фінансове право; інформаційне право» / О.В. Шепета ; Нац. ун-т Держ. податк. служби Украї-ни. – Ірпінь, 2011. – 25 с.20. Арістова І.В. Державна інформаційна полі-тика та її реалізація в діяльності органів внутрішніх справ України: організаційно-правові засади : дис. ... докт. юрид. наук : 12.00.07 «Адміністративне пра-во і процес; фінансове право; інформаційне право» / І.В. Арістова. – Х., 2002. – 476 с.21. Арістова І.В. Державна інформаційна полі-тика: організаційно-правові аспекти : [монографія] / І.В. Арістова ; за заг. ред. О.М. Бандурки. – Х. : Вид-во Ун-ту внутр. справ, 2000. – 368 с.22. Цимбалюк В.С. Інформаційне право (основи теорії і практики) : [монографія] / В.С. Цимбалюк. – К. : Освіта України, 2010. – 388 с.23. Основи інформаційного права України : [навч. посібн.] / [В.С. Цимбалюк, В.Д. Гавловський, В.В. Гри-ценко та ін.] ; за ред. М.Я. Швеця, Р.А. Калюжного та П.В. Мельника. – К. : Знання, 2004. – 274 с.

24. Цимбалюк В.С. Інформаційне право: концеп-туальні положення до кодифікації інформаційного за-конодавства / В.С. Цимбалюк. – К. : Освіта України, 2011. – 426 с.25. Цимбалюк В.С. Концепція кодифікації законо-давства України про інформацію / В.С. Цимбалюк // Інформаційні технології в глобальному управління : матеріали Міжнародної науково-практичної конфе-ренції (м. Київ, 29.10.2011). – К. : ФОП Ліпкан О.С., 2011. – С. 73–91.26. Сопілко І.В. Інформаційні загрози та безпе-ка сучасного українського суспільства / І.В. Сопілко [Електронний ресурс]. – Режим доступу : http://jrnl.nau.edu.ua/index.php/UV/article/viewFile/8181/9770.27. «Віртуальний ворог»: як захистити бізнес від кібератак? [Електронний ресурс]. – Режим доступу : http://www.polukr.net/uk/blog/2016/08/virtualnyj-voroh-jak-zahistiti-biznes-vid-kiberatak/.28. Баровська А.В. Функціональний аналіз сфери стратегічних комунікацій / А.В. Баровська, Д.В. Дубов // Стратегічні пріоритети. – 2016. – No 4 (41). – С. 105–112.29. Проект Стратегії забезпечення кібернетич-ної безпеки України [Електронний ресурс]. – Режим доступу : http://www.niss.gov.ua/public/File/2013_nauk_an_rozrobku/kiberstrateg.pdf.30. Великий тлумачний словник сучасної україн-ської мови / укл. О. Єрошенко. – Донецьк : ТОВ «Гло-рія Трейд», 2012. – 864 с.31. Розширення термінології сучасного кіберп-ростору / [В.В. Куцаєв, Є.О. Живило, С.П. Срібний, Ю.О. Черниш] [Електронний ресурс]. – Режим досту-пу : mino.esrae.ru/pdf/2014/3Sm/1387.doc.32. Про Доктрину інформаційної безпеки України : Указ Президента України від 08.07.2009 [Електро-нний ресурс]. – Режим доступу : http://zakon4.rada.gov.ua/laws/show/514/2009.33. Мінін Д.С. Підходи до визначення по-няття «кібербезпека» / Д.С. Мінін [Електронний ресурс]. – Режим доступу : http://istfak.org.ua/tendentsii-rozvytku-suchasnoi-systemy-mizhnarodnykh-vidnosyn-ta-svitovoho-politychnoho-protsesu/185-heopolitychna-dumka-ta-heostratehichni-protsesy-v-khkhi-st/971-pidkhody-do-vyznachennya-ponyattya-kiberbezpeka.34. Рудник Л.І. Право на доступ до інформації : дис. ... канд. юрид. наук : спец. 12.00.07 «Адміністративне пра-во і процес; фінансове право; інформаційне право» / Л.І. Рудник ; Національний університет біоресурсів і природокористування України. – К., 2015. – 247 с.35. Діордіца І.В. Інформаційні інтервенції як загроза кібернетичній безпеці / І.В. Діордіца [Електронний ре-сурс]. – Режим доступу : http://goal-int.org/informacijni-intervencii-yak-zagroza-kibernetichnij-bezpeci/.36. Єрмоленко В. Голландський референдум про Україну: 5 сценаріїв / В. Єрмоленко [Електронний ре-сурс]. – Режим доступу : URL: http://www.hromadske.tv/world/gollandskii–referendum-pro-ukrayinu-5-stsenariyiv.37. Про рішення Ради національної безпеки і оборони України «Про Стратегію національної безпеки України» : Указ Президента України від 06.05.2015 [Електронний ресурс]. – Режим доступу : http://zakon3.rada.gov.ua/laws/show/287/2015.38. Зелена книга з питань захисту критичної інф-раструктури в Україні : зб. матеріалів міжнар. експерт. нарад / упоряд. Д.С. Бірюков, С.І. Кондратов ; за заг. ред. О.М. Суходолі. – К. : НІСД, 2015. – 176 с.39. Турчинов вимагає швидкої реакції на кіберза-грози, 7 жовтня 2016 р. [Електронний ресурс]. – Режим доступу : http://www.newsru.ua/ukraine/07oct2016/turchinovkiber.html.40. Климчук О.О. Роль і місце спецслужб та правоохоронних органів провідних країн світу в на-ціональних системах кібербезпеки / О.О. Климчук, Н.А. Ткачук // Інформаційна безпека людини, сус-пільства, держави. – 2015. – No 3. – С. 75–83.41. Мінін Д.С. Підходи до визначення понят-тя «кібербезпека» / Д.С. Мінін // [Електронний ресурс]. – Режим доступу : http://istfak.org.ua/tendentsii-rozvytku-suchasnoi-systemy-mizhnarodnykh-vidnosyn-ta-svitovoho-politychnoho-protsesu/185-heopolitychna-dumka-ta-heostratehichni-protsesy-v-khkhi-st/971-pidkhody-do-vyznachennya-ponyattya-kiberbezpeka.42. Кіберзагрози і кібербезпека: чи здатні фахівці протистояти хакерам? 19.09.2016 [Електронний ре-сурс]. – Режим доступу : http://ukr.obozrevatel.com/news/34918-kiberzagrozi-i-kiberbezpeka-chi-zdatni-fahivtsi-protistoyati-hakeram.htm.43. SWIFT попередила світові банки про високу кіберзагрозу [Електронний ресурс]. – Режим доступу : http://www.depo.ua/ukr/svit/swift-poperedila-svitovi-banki-pro-visoku-kiberzagrozu-13122016123500.44. Сенатори США від обох партій виступили із заявою щодо російських кібератак, 12 грудня 2016 р. [Електронний ресурс]. – Режим доступу : http://www.pravda.com.ua/news/2016/12/12/7129541.45. Countering Information Warfare Act of 2016 [Електронний ресурс]. – Режим доступу : https://www.congress.gov/bill/114th–congress/senatebill/2692/text.46. Спецслужби США: Росія – кіберзагро-за усій життєво важливій

інфраструктурі Штатів, 05.01.2017 [Електронний ресурс]. – Режим доступу : http://zik.ua/news/2017/01/05/spetssluzhby_ssha_rosiya__kiberzagroza_usiy_zhyttievo_vazhlyviy_infrastrukturi_1021403.47. Розвідка США назвала Росію голов-ною кіберзагрозою, 05.01.2017 [Електронний ре-сурс]. – Режим доступу : http://www.pravda.com.ua/news/2017/01/5/7131747.48. Російська кіберзагроза, 26 вересня 2016 р. [Електронний ресурс]. – Режим доступу : http://www.radiosvoboda.org/a/28014684.html.49. Європейський парламент ухвалив резолюцію щодо протидії російській пропаганді, 23.11.2016 [Елек-тронний ресурс]. – Режим доступу : http://glavcom.ua/news/jevropeyskiy-parlament-uhvaliv-rezolyuciyu-shchodo-protidiji-rosiyskiy-propagandi-384228.html.50. Порошенко закликав США «бути вели-кими знову», 19.01.2017 [Електронний ресурс]. – Режим доступу : http://www.pravda.com.ua/news/2017/01/19/7132837.51. У Міноборони анонсували створення Центру реагування на кіберзагрози, 30.11.2016 [Електронний ресурс]. – Режим доступу : http://www.unian.ua/society/1653082-u-minoboroni-anonsuvali-stvorennya-tsentru-reaguvannya-na-kiberzagrozi.html.52. НБУ і НАБУ створять центр реагування на кіберзагрози в банківській системі, 04.10.2016 [Елек-тронний ресурс]. – Режим доступу : http://wz.lviv.ua/news/184233-nbu-i-nabu-stvoriat-tsentr-reahuvannia-na-kiberzahrozy-v-bankivskii-systemi.53. Сучасні тренди кібербезпекової політики: ви-сновки для України [Електронний ресурс]. – Режим доступу : http://www.niss.gov.ua/articles/294

M. Blackmer. Attacking the Weakest Link in theSupply Chain — Cisco Blog изд. — 2017. — Режимдоступа:https://blogs.cisco.com/security/attacking-the-weakest-link-in-the-supply-chain?dtid=osscdc000283.2.P. Moorhead. That Time Of Year Again: CiscoSystems Releases Its Annual Cybersecurity Report —Forbes изд. — 2018. — Режим доступа:https://www.forbes.com/sites/patrickmoorhead/2018/.3.Cyber-security risks in the supply chain — Cert-ukизд. — 2015. — Режим доступа:https://www.cert.gov.uk/wp-content/uploads/2015/02/Cyber-security-risks-in-the-supply-chain.pdf.4.R. WAUGH. The terrifying rise of cyber crime:Your computer is currently being targeted bycriminal gangs looking to harvest your personaldetails and steal your money. — Mail Online изд. —2013. — Режим доступа:https://www.dailymail.co.uk/home/moslive/article-2260221/Cyber-crime-Your-currently-targeted-criminal-gangs-looking-steal-money.html.5.ISO/IEC 27001:2013, Information technology – Security Techniques – Information securitymanagement systems – Requirements — ISO изд. —2013. — Режим доступа:https://www.iso.org/isoiec-27001-information-security.html.6.ISO/IEC 28001:2007, Security management systemsfor the supply chain – Best practices forimplementing supply chain security, assessmentsand plans – Requirements and guidance. — ISOизд. — 2007. — Режим доступа:https://www.iso.org/standard/45654.html.7.E. Florio. The Unexpected Attack Vector:SoftwareUpdaters — RSAConferenceизд. — 2017. — Режим доступа:https://www.rsaconference.com/videos/the-unexpected-attack-vector-software-updaters