Київський національний торговельно-економічний університет
Кафедра інженерії програмного забезпечення та кібербезпеки

ВИПУСКНИЙ КВАЛІФІКАЦІЙНИЙ ПРОЕКТ

на тему:

«Розробка системи захисту інформації бізнес-процесів»

Студента 2м курсу, 6з групи, спеціальності 121 «Інженерія програмного забезпечення», спеціалізації «Інженерія програмного забезпечення» _____ підпис студента — Чернігівського Івана Андрійовича

Науковий керівник кандидат технічних наук, доцент _____ підпис керівника — Сашньова Мар'яна Василівна

Гарант освітньої програми Доктор технічних наук, професор кафедри інженерії програмного забезпечення та кібербезпеки _____ підпис керівника — Криворучко Олена Володимирівна.

КИЇВ – 2020

Київський національний торговельно-економічний університет

Факультет інформаційних технологій
Кафедра інженерії програмного забезпечення та кібербезпеки
Освітній ступінь магістр
Спеціальність 121 «Інженерія програмного забезпечення»

Затверджую
Зав. кафедри інженерії програмного забезпечення та кібербезпеки
Криворучко О. В.
«8» листопада 2019 р.

Завдання
на випускний кваліфікаційний проект студентові
Чернігівському Івану Андрійовичу
(прізвище, ім'я, по батькові)

1. Тема випускного кваліфікаційного проекту «Розробка системи захисту інформації бізнес-процесів»

Затверджена наказом ректора від «24» грудня 2019 р. № 4440

2. Строк здачі студентом закінченої проекту 01 грудня 2020

3. Цільова установка та вихідні дані до проекту

Мета проекту – створення інструменту, для забезпечення захисту важливих файлів.

Об'єкт дослідження – бізнес-процеси на підприємстві, критичні дані, шкідливе ПЗ (програмне забезпечення).

Предмет дослідження – властивості критичних даних на підприємстві та шкідливого ПЗ.

4. Консультанти проекту із зазначенням розділів, які консультують:

Розділ	Консультант (прізвище, ініціали)	Підпис, дата	
		Завдання видав	Завдання прийняв

5. Зміст випускного кваліфікаційного проекту (перелік питань за кожним розділом)

ВСТУП

РОЗДІЛ 1. ДОСЛІДЖЕННЯ СИТУАЦІЇ НА ПІДПРИЄМСТВІ ТА РИНКУ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ

1.1. Визначення інформації, що потребує захисту, та її поточний стан

1.2. Поточний стан ринку програмного забезпечення

1.3. Технічне завдання на розробку програмного забезпечення

1.4. Висновки до розділу 1

РОЗДІЛ 2. ХАРАКТЕРИСТИКА ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ ДЛЯ ЗАХИСТУ ІНФОРМАЦІЇ НА ПІДПРИЄМСТВІ

2.1. Опис процедури появи можливих загроз для звітності підприємства

2.2. Етапи проектування алгоритмів для програмного забезпечення

2.3. Висновки до розділу 2

РОЗДІЛ 3. РОЗРОБКА ПРОГРАМИ ДЛЯ ЗАХИСТУ ІНФОРМАЦІЇ БІЗНЕС-ПРОЦЕСІВ НА ПІДПРИЄМСТВІ

3.1. Інтерфейс програмного модулю

3.2. Опис програмного модулю

3.3. Висновки до розділу 3

ВИСНОВКИ ТА ПРОПОЗИЦІЇ

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

ДОДАТКИ

6. Календарний план виконання проекту

№ пор.	Назва етапів випускного кваліфікаційного проекту	Строк виконання етапів проекту	
		за планом	фактично
1	2	3	4
1.	Вибір теми випускного кваліфікаційного проект	20.09.2019	20.09.2019
2.	Розробка та затвердження завдання на проект магістра	08.11.2019	08.11.2019
3.	Вступ та перелік літературних джерел	24.01.2020	24.01.2020
4.	Наукова стаття	01.09.2020	01.09.2020
5.	Технічне завдання	28.02.2020	28.02.2020
6.	Розділ 1. Дослідження ситуації на підприємстві та ринку програмного забезпечення	25.06.2020	25.06.2020
7.	Розділ 2. Характеристика програмного забезпечення для захисту інформації на підприємстві	07.09.2020	07.09.2020
8.	Розділ 3. Розробка програми для захисту інформації бізнес-процесів на підприємстві	19.10.2020	19.10.2020
9.	Програма та методика тестування	21.10.2020	21.10.2020
10.	Керівництво користувача	23.10.2020	23.10.2020
11.	Висновки та пропозиції	30.10.2020	30.10.2020
12.	Здача випускного кваліфікаційного проекту на кафедру (перша перевірка)	05.11.2020	05.11.2020
13.	Підготовка автореферату та презентації доповіді	05.11.2020	05.11.2020
14.	Попередній захист випускного кваліфікаційного проекту	25.11.2020-27.11.2020	25.11.2020-27.11.2020
15.	Зовнішнє рецензування випускного кваліфікаційного проекту	01.12.2020	01.12.2020
16.	Підготовка до публічного захисту випускного кваліфікаційного проекту	10.12.2020-11.12.2020	

7. Дата видачі завдання «8» листопада 2019 р.

8. Науковий керівник випускного кваліфікаційного проекту Сашньова М.В.

(прізвище, ініціали, підпис)

9. Гарант освітньої програми Криворучко О.В.

(прізвище, ініціали, підпис)

10. Завдання прийняв до виконання студент Чернігівський І.А.

(прізвище, ініціали, підпис)

11. Відгук керівника випускного кваліфікаційного проекту

_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____

Науковий керівник випускного кваліфікаційного проекту

_____

(підпис, дата)

Відмітка про попередній захист _____Сашньова М.В._____

(ПІБ, підпис, дата)

12. Висновок про випускний кваліфікаційний проект

Випускний кваліфікаційний проект студента _Чернігівського І.А._____

(прізвище, ініціали)

може бути допущена до захисту екзаменаційній комісії.

Гарант освітньої програми _____Криворучко О. В._____

(прізвище, ініціали, підпис)

Завідувач кафедри _____Криворучко О. В._____

(підпис, прізвище, ініціали)

«_____»_____20___ р.

АНОТАЦІЯ

Відповідно до мети дослідження робота присвячена розробці програми для захисту від троянів, що дозволить уникнути ризиків у випадках несправності антивірусного програмного забезпечення.

В результаті порівняльного аналізу аналогічних рішень визначено вагомі недоліки подібних програм, що були прийняті до уваги та усунені у нашій розробці.

Розробка виконана у середовищі розробки NanoVB6. Обрана мова програмування VB6 та cmd.

Готовий програмний комплекс VARAN було успішно протестовано відповідно до функціональних вимог.

Ключові слова: антивірус, вірус, ПК, Windows

ABSTRACT

In accordance with the purpose of the study, the work is devoted to the development of a program for protection against Trojans, which will avoid risks in cases of malfunction of anti-virus software.

As a result of comparative analysis of similar solutions, significant shortcomings of such programs were identified, which were taken into account and eliminated in our development.

The development was performed in the development environment of NanoVB6. Selected programming language VB6 and cmd.

The ready-made VARAN software package was successfully tested in accordance with the functional requirements.

Keywords: antivirus, virus, PC, Windows

Зміст

ВСТУП 4

РОЗДІЛ 1. ДОСЛІДЖЕННЯ СИТУАЦІЇ НА ПІДПРИЄМСТВІ ТА РИНКУ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ 6

1.1. Визначення інформації, що потребує захисту, та її поточний стан 6

1.2. Поточний стан ринку програмного забезпечення 16

1.3. Технічне завдання на розробку програмного забезпечення 19

1.4. Висновки до розділу 1 ..... **Ошибка! Закладка не определена.**

РОЗДІЛ 2. ХАРАКТЕРИСТИКАПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ ДЛЯ ЗАХИСТУ ІНФОРМАЦІЇ НА ПІДПРИЄМСТВІ 20

2.1. Опис процедури появи можливих загроздля звітності підприємства 20

2.2. Етапи проектування алгоритмів для програмного забезпечення 22

2.3. Висновки до розділу 2 26

РОЗДІЛ 3. РОЗРОБКА ПРОГРАМИ ДЛЯ ЗАХИСТУ ІНФОРМАЦІЇ БІЗНЕС-ПРОЦЕСІВ НА ПІДПРИЄМСТВІ 27

3.1. Інтерфейс програмного модулю 27

3.2. Опис програмного модулю 30

3.3. Висновки до розділу 3 38

ВИСНОВКИ ТА ПРОПОЗИЦІЇ 39

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ 40

ДОДАТКИ 44

ВСТУП

В сучасних умовах виникнення нових технічних та електронних засобів, які становлять небезпеку витоку інформації, спричиняє проблему захисту інформаційних ресурсів. Інформаційна безпека характеризується ступенем стійкості як до впровадження, так і до вилучення інформації, захищеності від випадкових чи навмисних природних або штучних впливів.

Проблема інформаційної безпеки розглядається у трьох основних аспектах: захист інформації; контроль за національним інформаційним простором; достатнє інформаційне забезпечення державних і недержавних органів, громадських, приватних організацій. Рівень захисту визначають для кожного певного виду інформації окремо. Для вирішення цієї проблеми необхідна система заходів, головною метою якої є захист від несанкціонованого доступу, наслідком якого може бути втрата, модифікація і витік інформації [11].

Актуальність досліджуваної теми зумовлена стрімким ростом за останні чотири роки шкідливого програмного забезпечення, що зумовлює блокування інформації при виконанні бізнес-процесів на підприємствах для малого та середнього бізнесу (за статистичними даними приріст складає 6000%).

Згідно з дослідженням лабораторії комп'ютерної криміналістики Group-IB «Програми-вимагачі: новітні методи атак шифрувальників», кількість атак вірусів-шифрувальників в 2019 року порівняно з попереднім роком зросла на 40%. Розмір середнього необхідного викупу також серйозно збільшився. Найбільші суми вимагають шифрувальники сімейства Ryuk, DoppelPaymer і REvil – їх одноразові вимоги про викуп досягали $800тис.

У дослідженні повідомляється, що цілі шахраїв змістилися в корпоративний сектор, оскільки тактики та інструменти операторів шифрувальників еволюціонували до складних технік, які раніше відрізняли в першу чергу хакерські APT-групи. Жертвами виявилися муніципалітети, корпорації, медичні установи, а середній розмір необхідного викупу зріс з $ 8000 в 2018 р., до $ 84 000в 2019 р. [25].

Оскільки стандартні засоби захисту (наприклад, антивіруси загального призначення) не можуть впоратися із задачею захисту файлів, потрібен новий спеціалізований інструмент, що буде захищати дані від даної загрози.

Метою дослідження є створення інструменту, для забезпечення захисту важливих файлів.

Об'єктом дослідження є бізнес-процеси на підприємстві, критичні дані, шкідливе ПЗ (програмне забезпечення)

Предметом дослідження є властивості критичних даних на підприємстві та шкідливого ПЗ (програмного забезпечення).

Задачі дослідження:

- Визначити типову поведінку шкідливого ПЗ;
- визначити типові недоліки антивірусних рішень;
- проаналізувати роботу спеціалізованих захисних рішень, вдосконалити їх методи;
- розробити більш дієве ПЗ для захисту бізнес-процесів щодо поточних рішень в контексті ефективності нейтралізації загроз.

Наукова новизна дослідження полягає в тому, що створений алгоритм може працювати майже в нежиттєздатних умовах для інших рішень, та є більш ефективним у порівнянні з іншими рішеннями.

Методи дослідження:

Синтез, аналіз, експеримент

РОЗДІЛ 1.
ДОСЛІДЖЕННЯ СИТУАЦІЇ НА ПІДПРИЄМСТВІ ТА РИНКУ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ

1.1. Визначення інформації, що потребує захисту, та її поточний стан

Аналіз законодавчої бази [17; 18; 20; 21; 22] дозволив виділити певні терміни, необхідні для викладу матеріалу, які ми будемо використовувати у подальшому дослідженні:

- *Документ*– матеріальний носій, що містить інформацію, основними функціями якого є її збереження та передачу у часі та просторі;
- *захист інформації* – сукупність правових, адміністративних, організаційних, технічних та інших заходів, що забезпечують збереження, цілісність інформації та належний порядок доступу до неї; сукупність методів і засобів, що забезпечують цілісність, конфіденційність і доступність інформації за умов впливу на неї загроз природного або штучного характеру, реалізація яких може призвести до завдання шкоди власникам і користувачам інформації;
- *інформація* –будь-які відомості та/або дані, які можуть бути збережені на матеріальних носіях або відображені в електронному вигляді;
- *суб'єкт владних повноважень*– орган державної влади, орган місцевого самоврядування, інший суб'єкт, що здійснює владні управлінські функції відповідно до законодавства, у тому числі на виконання делегованих повноважень.

- *безпека об'єкта критичної інфраструктури* – стан захищеності об'єкта критичної інфраструктури, за якого забезпечується функціональність і безперервність його роботи та/або можливість надання ним основних послуг;
- *власник* та/або керівник об'єкта *критичної інфраструктури* (далі – оператор основних послуг) – державний орган, підприємство, установа, організація будь-якої форми власності, юридична та/або фізична особа, якому/якій на правах власності, оренди або на інших законних підставах належить об'єкт критичної інфраструктури або який/яка відповідає за його поточне функціонування;
- *життєво важливі послуги та функції* (далі – основні послуги) – послуги, які надаються, та функції, що виконуються, операторами основних послуг, збої та переривання у наданні (виконанні) яких призводять до негативних наслідків для населення, суспільства, соціально-економічного стану та національної безпеки і оборони України;
- *захист об'єктів критичної інформаційної інфраструктури*– організаційні, нормативно-правові, інженерно-технічні та інші заходи, спрямовані на забезпечення безпеки об'єктів критичної інформаційної інфраструктури;
- *ідентифікація об'єкта критичної інформаційної інфраструктури* – процедура віднесення об'єкта інформаційної інфраструктури до об'єктів критичної інформаційної інфраструктури;
- *критична інформаційна інфраструктура* – сукупність об'єктів критичної інформаційної інфраструктури;
- *акт несанкціонованого втручання* – діяння, що створило загрозу безпечному функціонуванню об'єкта критичної інфраструктури та призвело до одного або декількох з таких наслідків: порушило його безперервність і стійкість; створило реальні чи потенційні загрози національній безпеці;

- *безпека критичної інфраструктури*– стан захищеності критичної інфраструктури, за якого забезпечується функціональність, безперервність роботи, цілісність і стійкість критичної інфраструктури;
- *захист критичної інфраструктури* – всі види діяльності, спрямовані на своєчасне виявлення, запобігання і нейтралізацію загроз безпеці об'єктів критичної інфраструктури, а також мінімізацію та ліквідацію наслідків у разі їх реалізації;
- *кризова ситуація* – порушення або загроза порушення штатного режиму функціонування критичної інфраструктури чи окремого її об'єкта, реагування на яке потребує залучення додаткових сил і ресурсів;
- *критична інфраструктура* – сукупність об'єктів, які є стратегічно важливими для економіки і національної безпеки, порушення функціонування яких може завдати шкоди життєво важливим національним інтересам;
- *об'єкт критичної інфраструктури* – визначений у встановленому законодавством порядку складовий елемент критичної інфраструктури, функціональність, безперервність, цілісність і стійкість якого забезпечують реалізацію життєво важливих національних інтересів;
- *оператор критичної інфраструктури*– державний орган, підприємство, установа, організація, юридична та/або фізична особа, якому/якій на правах власності, оренди або на інших законних підставах належать об'єкти критичної інфраструктури та який/яка відповідає за їх поточне функціонування;
- *охорона об'єктів критичної інфраструктури* – комплекс режимних, інженерних, інженерно-технічних та інших заходів, які організовуються і проводяться суб'єктами державної системи захисту критичної інфраструктури з метою запобігання та/або недопущення чи припинення

протиправних дій (чи актів несанкціонованого втручання) на об'єктах критичної інфраструктури;

- *рівень критичності* – відносна міра важливості об'єктів критичної інфраструктури, якою враховується вплив раптового припинення функціонування або функціонального збою на безпеку постачання, забезпечення суспільства важливими товарами і послугами;
- *режим функціонування критичної інфраструктури* – визначені умови та вимоги до функціонування критичної інфраструктури залежно від стану і динаміки розвитку ситуації (штатний режим функціонування; режим запобігання виникнення кризової ситуації; режим функціонування в кризовій ситуації; режим відновлення);
- *стійкість критичної інфраструктури*– стан критичної інфраструктури, за якого забезпечується її спроможність функціонувати у штатному режимі, адаптуватися до умов, що постійно змінюються, протистояти та швидко відновлюватися після впливу загроз будь-якого виду.
- *інформація про інцидент кібербезпеки* – відомості про обставини кіберінциденту, зокрема про те, які об’єкти кіберзахисту і за яких умов зазнали кібератаки, які з них успішно виявлені, нейтралізовані, яким запобігли за допомогою яких засобів кіберзахисту, у тому числі з використанням яких індикаторів кіберзагроз;
- *інцидент кібербезпеки* (далі – кіберінцидент) – подія або ряд несприятливих подій ненавмисного характеру (природного, технічного, технологічного, помилкового, у тому числі внаслідок дії людського фактора) та/або таких, що мають ознаки можливої (потенційної) кібератаки, які становлять загрозу безпеці систем електронних комунікацій, систем управління технологічними процесами, створюють імовірність порушення штатного режиму функціонування таких систем (у тому числі зриву та/або блокування роботи

системи, та/або несанкціонованого управління її ресурсами), ставлять під загрозу безпеку (захищеність) електронних інформаційних ресурсів;

- *кібератака* – спрямовані (навмисні) дії в кіберпросторі, які здійснюються за допомогою засобів електронних комунікацій (включаючи інформаційно-комунікаційні технології, програмні, програмно-апаратні засоби, інші технічні та технологічні засоби і обладнання) та спрямовані на досягнення однієї або сукупності таких цілей: порушення конфіденційності, цілісності, доступності електронних інформаційних ресурсів, що обробляються (передаються, зберігаються) в комунікаційних та/або технологічних системах, отримання несанкціонованого доступу до таких ресурсів; порушення безпеки, сталого, надійного та штатного режиму функціонування комунікаційних та/або технологічних систем; використання комунікаційної системи, її ресурсів та засобів електронних комунікацій для здійснення кібератак на інші об'єкти кіберзахисту;
- *кібербезпека* – захищеність життєво важливих інтересів людини і громадянина, суспільства та держави під час використання кіберпростору, за якої забезпечуються сталий розвиток інформаційного суспільства та цифрового комунікативного середовища, своєчасне виявлення, запобігання і нейтралізація реальних і потенційних загроз національній безпеці України у кіберпросторі;
- *кіберзагроза* – наявні та потенційно можливі явища і чинники, що створюють небезпеку життєво важливим національним інтересам України у кіберпросторі, справляють негативний вплив на стан кібербезпеки держави, кібербезпеку та кіберзахист її об'єктів;

- *кіберзахист* – сукупність організаційних, правових, інженерно-технічних заходів, а також заходів криптографічного та технічного захисту інформації, спрямованих на запобігання кіберінцидентам, виявлення та захист від кібератак, ліквідацію їх наслідків, відновлення сталості і надійності функціонування комунікаційних, технологічних систем;
- *кіберзлочин* (комп'ютерний злочин) – суспільно небезпечне винне діяння у кіберпросторі та/або з його використанням, відповідальність за яке передбачена законом України про кримінальну відповідальність та/або яке визнано злочином міжнародними договорами України;
- *кіберзлочинність* – сукупність кіберзлочинів [17].

Досліджувані ПЗ та бізнес-процеси підприємства покликані здійснювати захист та максимально зменшити шкоду від кібератак.

Багато користувачів постраждали від троянів-шифрувальників, як на комп'ютерній так і на мобільній ОС, антивіруси детектували загрози лише після того, як ПК користувачів були заражені, як наслідок – неможливість відновити файли та близько 10тис модифікацій троянів.

Тому виникла потреба у новому продукті, який би виявляв загрозу за відповідними діями ще до її старту та шкідливої діяльності миттєво захищаючи файли.

Захист інформації ведеться для підтримки таких властивостей інформації як:

Цілісність – неможливість модифікації інформації неавторизованим користувачем.

Конфіденційність – інформація не може бути отримана неавторизованим користувачем.

Доступність – полягає в тому, що авторизований користувач може використовувати інформацію відповідно до правил, встановлених політикою безпеки не очікуючи довше заданого (прийнятного) інтервалу часу [18].

Загроза, що виникає стосовно інформації під час кібератаки може бути спрямована як на її цілісність, так і на конфіденційність та доступність.

Відповідно до властивостей інформації виділяють такі загрози її безпеці:

- *загрози цілісності*:
  - знищення;
  - модифікація;
- *загрози доступності*:
  - блокування;
  - знищення;
- *загрози конфіденційності*:
  - несанкціонований доступ (НСД);
  - витік;
  - розголошення [18].

Аспекти захисту інформації також розподілені за властивостями інформації: для збереження **конфіденційності** інформації здійснюється захист від несанкціонованого ознайомлення з інформацією. Для збереження **цілісності** інформації –захист інформації від несанкціонованої модифікації. Для обмеження **доступності** інформації відбувається захист (забезпечення) доступу до інформації, а також можливості її використання. Доступність забезпечується як підтриманням систем в робочому стані так і завдяки способам, які дозволяють швидко відновити втрачену чи пошкоджену інформацію [19].

Види захисту інформації

Кожен вид захисту інформації забезпечує окремі аспекти інформаційної безпеки:

Технічний – забезпечує обмеження доступу до носія повідомлення апаратно-технічними засобами (антивіруси, фаєрволи, маршрутизатори, токіни, смарт-карти тощо):

- попередження блокування ;
- попередження витоку по технічним каналам;

Інженерний – попереджує руйнування носія внаслідок навмисних дій або природного впливу інженерно-технічними засобами (сюди відносять обмежуючі конструкції, охоронно-пожежна сигналізація).

Криптографічний – попереджує доступ за допомогою математичних перетворень повідомлення (ІП):

- попередження несанкціонованої модифікації ;
- попередження несанкціонованого розголошення [17].

Організаційний – попередження доступу на об'єкт інформаційної діяльності сторонніх осіб за допомогою організаційних заходів (правила розмежування доступу).

В нашому дослідженні пропонуємо використати технічний вид захисту інформації для забезпечення захисту бізнес-процесів. Відповідно, відбувається захист самого змісту інформації.

За змістом інформація поділяється на такі види: інформація про фізичну особу; інформація довідково-енциклопедичного характеру; інформація про стан довкілля (екологічна інформація);інформація про товар (роботу, послугу);науково-технічна інформація; податкова інформація; правова інформація; статистична інформація; соціологічна інформація; інші види інформації.

Наше дослідження спрямоване на захист інформації про юридичну особу, товар та іншу супровідну інформацію та унеможливити доступ до неї [17; 20].

За порядком доступу інформація поділяється на відкриту інформацію та інформацію з обмеженим доступом. Будь-яка інформація є відкритою, крім тієї, що віднесена законом до інформації з обмеженим доступом.

Інформація з обмеженим доступом має наступні характеристики: - інформація з обмеженим доступом є конфіденційна, таємна та службова інформація. Відповідно, конфіденційною є інформація про фізичну особу, а також інформація, доступ до якої обмежено фізичною або юридичною особою, крім суб'єктів владних повноважень [17; 22].

Конфіденційна інформація може поширюватися за бажанням (згодою) відповідної особи у визначеному нею порядку відповідно до передбачених нею умов, а також в інших випадках, визначених законом.

Відносини, пов’язані з правовим режимом конфіденційної інформації, регулюються законом. Порядок віднесення інформації до таємної або службової, а також порядок доступу до неї регулюються законами. До інформації з обмеженим доступом не можуть бути віднесені такі відомості:

1) про стан довкілля, якість харчових продуктів і предметів побуту;

2) про аварії, катастрофи, небезпечні природні явища та інші надзвичайні ситуації, що сталися або можуть статися і загрожують безпеці людей;

3) про стан здоров’я населення, його життєвий рівень, включаючи харчування, одяг, житло, медичне обслуговування та соціальне забезпечення, а також про соціально-демографічні показники, стан правопорядку, освіти і культури населення;

4) про факти порушення прав і свобод людини, включаючи інформацію, що міститься в архівних документах колишніх радянських органів державної безпеки, пов'язаних з політичними репресіями, Голодомором 1932-1933 років в Україні та іншими злочинами, вчиненими представниками комуністичного та/або націонал-соціалістичного (нацистського) тоталітарних режимів;

5) про незаконні дії органів державної влади, органів місцевого самоврядування, їх посадових та службових осіб;

6) інші відомості, доступ до яких не може бути обмежено відповідно до законів та міжнародних договорів України, згода на обов'язковість яких надана Верховною Радою України. Порушення законодавства України про інформацію тягне за собою дисциплінарну, цивільно-правову, адміністративну або кримінальну відповідальність згідно із законами України [17; 22]. Існують випадки, коли інформація з обмеженим доступом може бути поширена, якщо вона є суспільно необхідною, тобто є предметом суспільного інтересу, і право громадськості знати цю інформацію переважає потенційну шкоду від її поширення. Предметом суспільного інтересу вважається інформація, яка свідчить про загрозу державному суверенітету, територіальній цілісності України; забезпечує реалізацію конституційних прав, свобод і обов'язків; свідчить про можливість порушення прав людини, введення громадськості в оману, шкідливі екологічні та інші негативні наслідки діяльності (бездіяльності) фізичних або юридичних осіб тощо [20; 21].

Інформація про підприємства та установи є інформацією з обмеженим доступом і, як правило, власник бажає максимально захистити її і не допустити її поширення в тому числі інформацію суспільного інтересу. Проте, як показує практика, підприємці не вживають адекватних заходів для забезпечення кібербезпеки. Інколи це стосується також і об'єктів критичної інфраструктури.

Об'є́кти крити́чної інфраструкту́ри – підприємства та установи (незалежно від форми власності) таких галузей, як енергетика, хімічна промисловість, транспорт, банки та фінанси, інформаційні технології та телекомунікації (електронні комунікації), продовольство, охорона здоров'я, комунальне господарство, що є стратегічно важливими для функціонування економіки і безпеки держави, суспільства та населення, виведення з ладу або руйнування яких може мати вплив на національну безпеку і оборону, природне середовище, призвести до значних матеріальних та фінансових збитків, людських жертв [19; 20; 21].

Закон України «Про основні засади забезпечення кібербезпеки України» використовує термін «*критично важливі об'єкти інфраструктури*», визначаючи їх як юридичні особи, діяльність яких безпосередньо пов'язана з технологічними процесами та/або наданням послуг, що мають велике значення для економіки та промисловості, функціонування суспільства та безпеки населення, виведення з ладу або порушення функціонування яких може справити негативний вплив на стан національної безпеки і оборони України, навколишнього природного середовища, заподіяти майнову шкоду та/або становити загрозу для життя і здоров'я людей [22].

Для оцінки критичності об'єкта інформаційної інфраструктури оператор основних послуг використовує такі критерії:

- необхідність об'єкта інформаційної інфраструктури як для стійкого та безперервного функціонування об'єкта критичної інфраструктури, так і для надання ним основних послуг;

- кібератака, кіберінцидент, інцидент з інформаційної безпеки на об'єкті інформаційної інфраструктури істотно впливає на безперервність та стійкість надання об'єктом критичної інфраструктури основних послуг;

- у разі порушення безперервності та стійкості надання основних послуг об'єктом інформаційної інфраструктури відсутній альтернативний об'єкт (спосіб) для їх надання [22].

Об'єкти інформаційної інфраструктури, що відповідають всім трьом критеріям, визначаються оператором основних послуг як об'єкти критичної інформаційної інфраструктури. При цьому категорія критичності об'єкта критичної інформаційної інфраструктури встановлюється за категорією критичності об'єкта критичної інфраструктури.

Таким чином, інформація, що потребує захисту на підприємстві – інформація з обмеженим доступом що охороняється законом, є необхідною для стійкого та безперервного функціонування підприємства, може бути об'єктом кібератак.

1.2. Поточний стан ринку програмного забезпечення

На сьогоднішній день існує значна кількість антивірусного ПЗ – більше п'ятдесяти одиниць, але послуги по захисту файлів від шкідливого шифрувального ПЗ надають лишекілька компаній, пропоновані ними продукти Cybereason RansomFree, Malwarebytes Anti-Ransomware, AppCheck, Avast_free_antivirus_anti_ransom, Kaspersky Anti-Ransomware, види послуг, що надаються вказаними продуктами, спосіб їх розповсюдження та інформацію щодо потенційних клієнтів, з якими компанії хотіли б співпрацювати,подано у таблиці 1.1.

Таблиця 1.1.

Програми для захисту від троянів-шифрувальників

Продукт фірми	Послуги	Розмір(МБ)	Способи реклами	Клієнти
Cybereason RansomFree (безкоштовний)	Блокує віруси	4	Інтернет	Користувачі, корпоративні компанії
Malwarebytes Anti-Ransomware (безкоштовний)	Блокує віруси	60	Інтернет	Корпоративні компанії і користувачі
AppCheck (безкоштовний з обмеженою функціональністю / платний з повною функціональністю)	Блокує віруси	7	Інтернет	Користувачі
Avast_free_antivirus_anti_ransom (безкоштовний)	Блокує віруси	7	Інтернет	Користувачі
Kaspersky Anti-Ransomware (платний)	Блокує віруси	30	Інтернет, пошта	Корпоративні компанії

Як бачимо з таблиці, вказані продукти виконують однакові послуги – блокують віруси, але відрізняються за спрямованістю на користувачів, розміром та за ціною.

Незважаючи на те, що ці програмні продукти позиціонують себе як найкращий спосіб 100% захисту від всіх існуючих і невідомих загроз, вони мають певні суттєві недоліки, що представлені в таблиці 1.2.

Таблиця 1.2.

Переваги та недоліки спеціалізованого захисного ПЗ

Продукт фірми	Переваги	Недоліки
Cybereason RansomFree	Може знаходити ще невідомі загрози, безкоштовний для кожного, кращий на ринку	Ця програма – аналізатор поведінки, тому спрацьовує після 2-3 секунд роботи вірусів
Malwarebytes Anti-Ransomware	Висока ефективність на тестах	Потрібен інтернет, захищає всього від 3х різних вірусів
AppCheck	Має 3 ступені захисту, включає бекап файлів	Платний, тільки для win7 sp1, захищає всього 46 типів файлів
Avast_free_antivirus_anti_ransom	Може розшифровувати файли	Не може захистити від сучасних вірусів, тільки розшифровувати існуючі (21 штука)
Kaspersky Anti-Ransomware	Має свою лабораторію, орієнтований на припинення епідемій	Працює лише по сигнатурам, тільки для приватних підприємств з повною інформацією

Отже, зважаючи на вищевикладене, робимо висновок про те, що сучасні пропоновані різними фірмами антивіруси не забезпечують необхідний рівень захисту інформації з обмеженим доступом, тому існує необхідність створення нового інструменту, який міг би усунути всі недоліки сучасних програм для захисту файлів.

1.3. Технічне завдання на розробку програмного забезпечення

Нами було обрано такий перелік необхідних якостей для ПЗдля роботи в екстремальних умовах і вичерпності ресурсів:

1. Здатний захищати дані від троянів без підключення до Інтернету.
2. Не потребує оновлення сигнатурних баз – він їх не використовує, зробивши більший акцент на проактивний захист.
3. Не потребує встановлення на ПК.
4. Займає дуже мало місця на диску (<100КБ), не потребує бекапів.
5. Встановлюється тільки на комп'ютери під управлінням Microsoft Windows – подібних ОС.
6. Здатний працювати без встановлення зайвих компонентів на всіх без винятку розрядних ОС.
7. Має дуже малий ступінь використання системних ресурсів, та після повногоналаштування зовсім не навантажує систему та не висить у пам'яті.
8. Захищає файли ефективніше ніж інші продукти – миттєво і непомітно.

1.4. Висновки до розділу 1

Отже, ми розібрали які види інформації бувають, можливі критичні дані на підприємстві, сучасні захисні рішення, їх переваги та недоліки, визначили яким повинно бути ідеальне ПЗ для захисту файлів.

РОЗДІЛ 2.
ХАРАКТЕРИСТИКА ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ ДЛЯ ЗАХИСТУ ІНФОРМАЦІЇ НА ПІДПРИЄМСТВІ

2.1. Опис процедури появи можливих загроз для звітності підприємства

Основні загрози, з якими може стикнутися підприємство – віруси-шифрувальники, віруси-шпигуни, віруси-віддаленого доступу, що впливають на працездатність підприємства та можуть спричинити значні збитки. Оскільки втрату працездатності підприємства та його банкрутство може спричинити тільки перший тип вірусів – віруси-шифрувальники, його і буде розглянуто у нашому дослідженні.

Зазвичай вірус шифрує популярні типи користувацьких файлів: документи, таблиці, бази даних бухгалтерських програм, фотографії, тощо. Розшифровку, зазвичай, пропонують виконати за гроші– переказати необхідну суму на мобільний телефон або біткоїн-гаманець. Варто зазначити, що дія інших вірусів також не передбачає відновлення втрачених файлів, проте існує алгоритм спроби їх відновлення. Натомість, віруси-шифрувальники, безповоротно руйнують файли, не допускаючи можливості їх відновлення [23].

Проаналізувавши кілька екземплярів вірусів-шифрувальників, можна визначити типовішкідливі дії більшості вірусів-шифрувальників та етапи їх проникнення у закриту мережу [24; 27].

Етапи:

1) Розвідка корпоративної мережі, отримання всієї необхідної інформації для зараження.

2) Створення / модифікація вірусу і векторів атак в залежності від мережі.

3) Завантаження вірусу на комп'ютери корпоративних користувачів – таргетована фішингова поштова розсилка (рахунок фактура, договори контрагентів, ухвала суду тощо) з шкідливим вкладенням (.doc .pdf чи .exe), zero-day у комп'ютерній системі, заражені носії інформації чи підкуплені співробітники.

4) Запуск вірусу в обхід захисних систем (автоматично чи за допомогою користувача).

5) Знищення слідів проникнення, резервних копій даних, залишення повідомлення для керівництва компанії.

Це всі етапи для коштовних таргетованих атак, але в більшості випадків етапи 1,2 та 5 не виконуються. Фішингова розсилка націлена не на конкретну компанію а на всі можливі, тому знищення слідів проникнення не є ефективним, що дозволяє швидко зреагувати на кіберінцедент і локалізувати загрозу.

Проте, якщо відбулося проникнення вірусу в пам'ять комп'ютера і вірус зміг отримати можливість керування, його наявність можна ідентифікувати за наступними типовими діями [24; 25].

Типові дії вірусів наступні:

1. Отримати можливість запуститися в оперативній пам'яті комп'ютера.
2. Шукати файли по масці(офісні документи, бази даних тощо).
3. Шифрувати файли випадковим ключом AES а ключ шифрувати за RSA (деякі мають вшитий ключ у своєму коді і реалізують нестійкі самописні алгоритми шифрування, проте вони не є об'єктом нашого дослідження і розглядатися не будуть).
4. Знищити тіньові копії, видалити оригінали, затерти диск нулями.

5. Залишити в кожній із папок записку з викупом, змінити шпалери на робочому столі.

6. Самоліквідуватися або висіти у системі і чекати появи нових файлів, щоб їх зашифрувати.

Оскільки сучасні антивіруси в основному працюють за сигнатурами, і в їх задачу входить детектування і знищення шкідливого ПЗ на етапі проникнення – якщо вірус зможе запуститися в пам'яті то машина буде заражена незалежно від антивіруса який на ній встановлений.Тобто існує необхідність сформувати такий алгоритм, щоб для типового шкідливого ПЗ він був найефективнішим щодо захисту від вірусу.

2.2. Етапи проектування алгоритмів для програмного забезпечення

Оскільки на етапи проникнення в мережу можуть вплинути лише системи виявлення вторгнень та грамотний ІТ-відділ компанії, з кваліфікованими фахівцями, це досить дорого обійдеться компанії. Такі витрати можуть дозволити собі лише великі корпорації, натомість представники середнього та малого бізнесу будуть потерпати від таких атак, не маючи фінансової можливості їм протистояти. По-перше, представники середнього та малого бізнесу в більшості своїй не знають про існування різноманітних вірусів і алгоритм протистояння їм, по-друге, ставши жертвами подібних атак, все одно не діють за запропонованим алгоритмом уникнення наслідків та наступних атак і зниження збитків від них.

Перша і друга причина мають в своїй основі недостатні фінансові ресурси а також несприйняття високого рівня загрози для найму висококваліфікованих ІТ-спеціалістів.Тому нам необхідно сфокусуватися на створенні захисного ПЗ, доступного для представників середнього та малого бізнесу. Для більш чіткого розуміння процедури розробки такого ПЗ, нам необхідно безпосередньо зосередитись на розумінні роботи шкідливого ПЗ [25; 26].

У підрозділі 2.1. наведено типові дії вірусів, зважаючи на послідовність дій яких, можливо розробити наступне:

1. Не дати можливості вірусу запуститися – в реальному часі моніторити дампи пам'яті та знаходити підозрілий код у відкритому вигляді.

2. Зробити так, щоб вірус не зміг знайти потрібні файли і самовидалився – перехоплювати системні запити на читання / запис файлів і оцінювати їх легітимність за складною евристикою, використовувати системні права доступу.

3. Знайти ключ або зламати алгоритм – використовуючи технології реверс-інжинірингу знайти ключ у коді віруса, атакувати механізм генерації ключів зробивши алгоритм нестійким, що допоможе розшифрувати файли без знання ключа.

4. Відслідковувати аномальну активність запису на диск та затирання файлів – перехоплювати системні виклики.

5. Парадоксально, проте є факт існування таких «антивірусів» що сигнатурно детектують текст записки івидаляють саму записку замість віруса. Як результат – заражений комп'ютер і вже безповоротно зіпсовані файли,тому що видалені записки унеможливлюють процес відновлення файлів запланованим способом. В такому випадку, знайшовши такі записки, їх варто зберегти.

6. Можна залишити без змін, оскільки хоч вірус і ліквідований – він залишився у поштовому вкладені, де його можливо ретельно проаналізувати та дослідити.

Говорячи про знаходження ключа або злам алгоритму, маємо використати такі дефініції як *криптографія,* яка здійснює пошук, дослідження і розробку математичних методів перетворення інформації, основою яких є шифрування, та *криптоаналіз*, який досліджує можливості розшифровки інформації, що власне і є криптоаналітичною атакою. Криптографічні системи забезпечують високу стійкість зашифрованих даних за рахунок підтримки режиму таємності криптографічного ключа.

Однак, на практиці будь-який шифр, який використовується в тій чи іншій криптосистемі, піддається розкриттю з визначеною трудомісткістю, у зв'язку з цим виникає необхідність оцінки криптостійкості шифрів, які застосовуються в криптографічних каналах [10; 12].

До поширених алгоритмів шифрування належать: TEA\XXTEA\Raiden, 3DES, IDEA, Магма, які поступово виводять з обігу на користь більш стійких: блокові шифри Camelia, Twofish, Serpent, Blowfish, CAST, Mars, MISTY1, Калина; поточні шифри Salsa20, ChaCha20, SOSEMANUK, Trivium та асиметричні шифри RSA, ECDSA, Rabin, Elgamal. Частіше використовуваним є AES (Advanced Encryption Standard) за його швидкість. Найбільш поширеними шифрами, які використовують віруси, є: XOR,TEA, Blowfish, AES, RSA, Elgamal. У нашому дослідженні, орієнтуючись на існуючі алгоритми шифрування, пропонуємо розглянути наступні види криптоаналітичних атак [12].

На блокові шифри можливе здійснення таких атак: на основі лише шифротексту, на основі відкритих текстів і відповідних шифротекстів, на основі підібраного відкритого тексту, на основі адаптивно підібраного відкритого тексту, на основі підібраного шифротексту, на основі підібраного ключа, атака зі зв'язаним ключем, частотний аналіз, диференціальний криптоаналіз, лінійний криптоаналіз, алгебраїчний XLS криптоаналіз, інтегральний криптоаналіз, інтерполяційна атака, усічений диференційний криптоаналіз, сдвигова атака, атака бумерангом, неможливий диференційний криптоаналіз. Хеш-функції вразливі до кореляційних атак, пошуку першого та другого прообразів, знаходження колізії, атак «днів народження». Для асиметричних шифрів небезпечними є:частотний аналіз та MItM-атака. Атаки для всіх типів шифрів: за часом, по стороннім каналам, енергоспоживання, «холодного перезапуску», компроміс «час-пам'ять», атака при збоях програмного і технічного забезпечення, атака на генератор псевдо-випадкових чисел (ГПВЧ), атака внесенням змін, «бандитський» криптоаналіз, перебір за словником та повний перебір [12].

Суттєво зауважити, що проти вищезгаданих типів атак існує велике обмеження для їх практичного використання на комп'ютерах користувачів, оскільки захист від вірусів такого типу передбачає атаку на генератор псевдо-випадкових чисел, то всі запропоновані генератором ключі будуть нестійкими. Зважаючи на те, що операція з шифрування/розшифрування даних є дуже важливою для збереження цілісності та автентичності інформації, то все, що буде задіяне в роботі користувача (робота сайтів у браузері, безпосередньо бухгалтерські програми тощо), буде нестійким та під загрозою зламу. В свою чергу, це означає, що комп'ютер користувача знаходиться під більшою загрозою, ніж виникла б під час появи шифрувальників, оскільки передача даних з ПК користувача відбувається щодня. Враховуючи вищесказане, вважаємо недоцільним використовувати такий метод захисту від шифрувальників через його високу енерговитратність та шкідливість.

Варто зазначити, що усі ці дії мають певні недоліки: вони дуже складні у реалізації та обслуговуванні, займають багато пам'яті та системних ресурсів ПК при цьому не даючи гарантовано миттєвого результату – зазвичай потрібно 3-5 секунд щоб спрацювала евристика, а це 300 зашифрованих файлів без інструкцій AES-NI(з ними рахунок іде як 4Гб на кожну секунду роботи). Таким чином за кілька секунд маємо 20 Гб зашифрованих даних, серед яких будуть критично важливі для роботи підприємства файли. Важливо, що система щоразу пропонує надокучливі запити на підтвердження дій як от: «Чи дійсно ви хочете записати / відкрити цей файл?». Зважаючи на те, що антивірусом будуть перехоплюватися усі системні виклики – користувач отримає дуже багато подібних запитів і швидше прийме рішення про видалення такої системи, поки вона встигне ідентифікувати та знешкодити хоча б один вірус [14].

Постає питання про здійснення такого захисту, що не буде дуже коштовним і не буде займати значну кількість ресурсів ПК та водночас буде ефективнішим за існуючі рішення. Знайти таке рішення допомогла битва вірусів за системні ресурси, під час проведення експерименту.

Після того, як в ізольованому і контрольованому просторі були запущені одномоментно 2 екземпляри вірусів різного сімейства – файли встигли заразитися лише одним. При повторному проведенні експерименту (вже даючи необхідні ресурси обом вірусам) результат залишився той самий – після блокування файлів одним типом вірусу, вони вже не могли повторно зашифруватися іншими, але лише в тому випадку, якщо вірус змінював їх розширення на своє.

Провівши остаточний експеримент, змінивши вручну розширення документів та запустивши відомий вірус, було виявлено що змінені таким чином файли залишилися непошкодженими(на відміну від інших немодифікованих файлів), а отже, вони стали захищеними від вірусу.

Отже, для всіх вірусів-шифрувальників які діють за описаними «типовими» діями, надійним захистом стає зміна розширень файлів, тому що за таких умов вірус не знаходить файли для шифрування і самоліквідується.

2.3. Висновки до розділу 2

Було розглянуто етапи проведення кібератак, типові дії вірусів, дані можливі рекомендації для протидії та знайдено ефективне рішення, що повністю відповідає технічному завданню та є ефективнішим за існуючі програми по ефективності. Іноді складні проблеми мають занадто просте рішення.

РОЗДІЛ 3.
РОЗРОБКА ПРОГРАМИ ДЛЯ ЗАХИСТУ ІНФОРМАЦІЇ БІЗНЕС-ПРОЦЕСІВ НА ПІДПРИЄМСТВІ

3.1. Інтерфейс програмного модулю

Аналіз наукових досліджень щодо ведення облікової документації на підприємстві демонструє, що науковціприділяли увагу питаннямщодо бухгалтерського фінансового обліку та звітності підприємства (А.В. Алексеєва, Ф.Ф. Бутинець, Г.П. Голубнича, С.М. Гольцова,Т.Г. Мельник,Г.В. Уманців, А.П. Шаповалова)[1; 3; 7; 9]. Ведення підприємницької діяльності на міжнародному рівні піднімає питання трансформації звітності підприємства за міжнародними стандартами (С.Ф. Голов,В.М. Костюченко, О.М. Кулага) [4; 5; 6]. У контексті ведення та збереження облікової документації підприємства, в полі зору науковців постало питання безпеки соціально-економічних процесів у кіберпросторі та необхідність захисту інформації бізнес-процесів на підприємстві (К.В. Безверхий,Т.В. Бочуля,Е.М. Кучер, С.Л. Рзаєва) [2; 8].

Таким чином, звітність підприємства, що іключає в себе баланс та фінансові результати, а також інформація про грошові потоки та бізнес-процеси на підприємстві є критично важливими даними, які потребують високого рівня захисту [15; 16].

Для захисту інформації бізнес-процесів на підприємстві ми пропонуємо програмну утиліту *VARAN*, яка, на нашу думку, надає необхідний захист і відповідає вимогам, зазначеним в другому розділі. Встановлений і запущений антивірус *VARAN* має наступний вигляд та демонструє на екрані інтерфейс,

як наведено на рисунку 3.1. Ми прагнули створити максимально простий інтерфейс програми, щоб уникнути непорозумінь та невірних налаштувань з боку користувача. Тому запропопонували вибір мови та індикатор роботи програми [10].

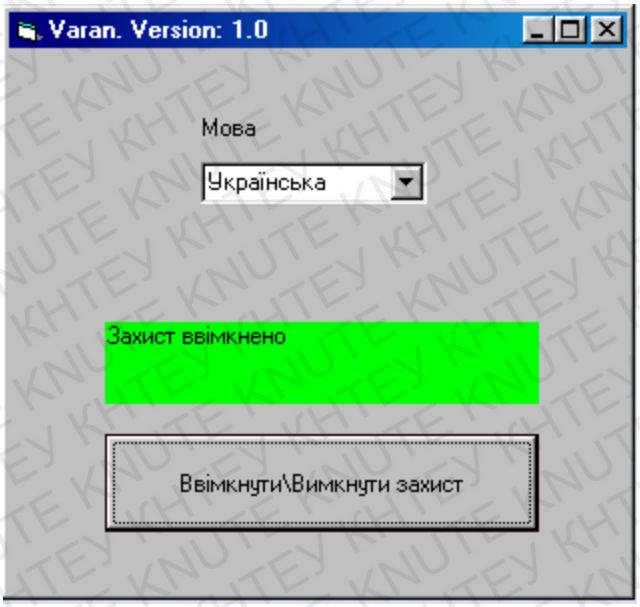

Рис. 3.1. Звичайний інтерфейс користувача, інформація про стан захисту

На рисунку 3.2 продемонстровано повідомлення програми *VARAN* про вимкнення захисту на комп'ютері користувача. Вважаємо повідомлення чітким та інформативним за рахунок використання загальноприйнятого знаку «вимкнено».

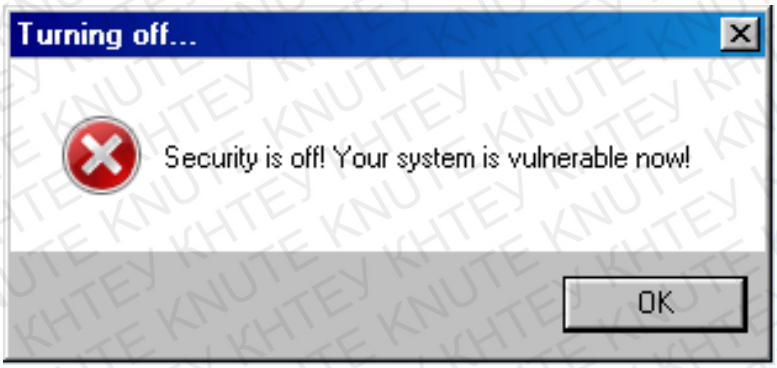

Рис. 3.2. Повідомлення програми *VARAN* про вимкнення захисту.

Окрім повідомлення програми, на екрані з’являється інтерфейс, що демострує стан програми на комп’ютері користувача просто і зрозуміло, як наведено на рисунку 3.3.

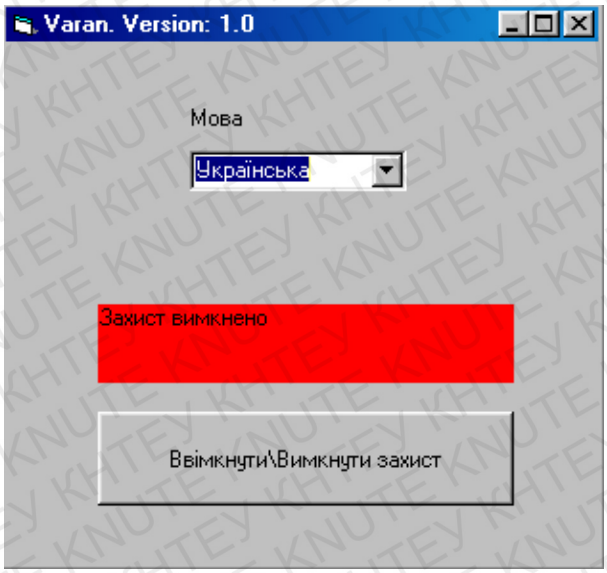

Рис. 3.3.Захист вимкнено.

Для отримання більш детальної інформації щодо роботи програми адміністратором пропонуємо скористатися командною строчкою та побачити консольний інтерфейс, як наведено на рисунку 3.4.

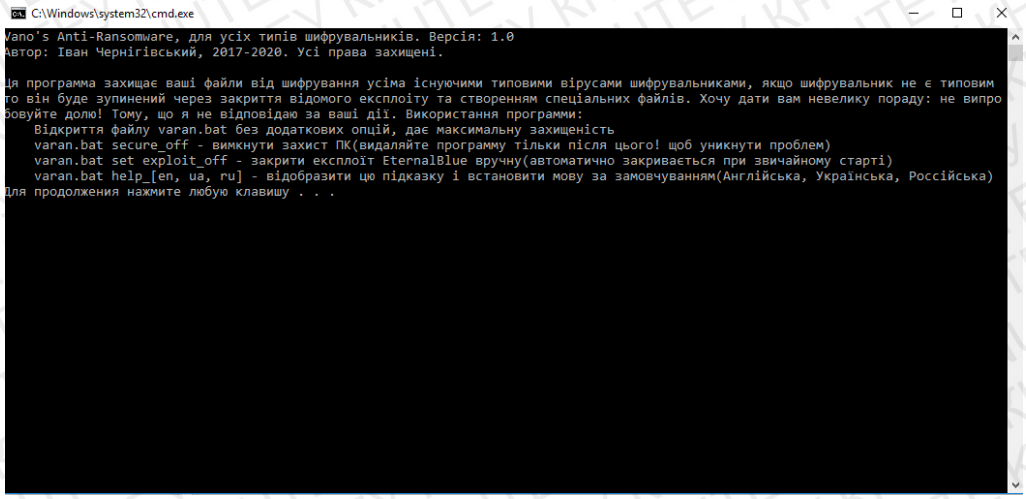

Рисунок 3.4.Консольний інтерфейс.

Кожна програма зазвичай має свої унікальні іконки та логотипи, наші можливі варіанти логотипу програми *VARAN* представлені на рисунках 3.5 і 3.6

Рис. 3.5. Кольоровий логотип

Рис. 3.6. Чорно-білий варіант

3.2.Опис програмного модулю

Проаналізувавши наукові джерела щодо безпечної взаємодії користувача та ПК, звертаємо увагу на кіберфізичну систему (КФС / CPS), в якій механізм контролюється за допомогою комп'ютерних алгоритмів. У кіберфізичних системах фізичні та програмні компоненти тісно взаємопов'язані, здатні діяти на різних просторово-часових масштабах, виявляти численні чіткі поведінкові модальності та взаємодіяти один з одним способами, що можуть змінюватися залежно від контексту. Приклади CPS включають: хмарну сітку, автономні автомобільні системи, медичний моніторинг, системи промислового управління, системи робототехніки та автопілоти [13].

CPS передбачає трансдисциплінарні підходи, злиття теорії кібернетики, мехатроніки, науки про дизайн та процеси. Керування процесом часто називають вбудованими системами. У вбудованих системах акцент робиться більше на обчислювальні елементи та менше на інтенсивний зв'язок між обчислювальними та фізичними елементами. CPS також схожий з інтернетом речей (IoT),

що має ту саму базову архітектуру; тим не менш, CPS представляє більш високу комбінацію та координацію між фізичними та обчислювальними елементами. Попередників кіберфізичних систем можна знайти в таких різноманітних сферах як аерокосмічна, автомобільна, хімічна, цивільна інфраструктура, енергетика, охорона здоров'я, виробництво, транспорт, розваги та у побутовій техніці [13].

Концепція створення багаторівневої CPS має таку структуру у такій послідовності: класифікація загрози / атаки; формування критеріїв захисту; створення багаторівневої CPS. CPS – це визначення політики безпеки, модель CPS – це вибір методів оцінки захисту стану CPS. Класифікація загроз / атак: погрози з боку особливості атаки за кінцевим результатом, метод класифікації загроз STRIDE за категоріями (підміна об'єктів, зміна даних, заперечення авторства, розголошення інформації, відмова від послуги, збільшення привілеїв) – створення моделі загроз «Інформація / CPS – джерела загроз – способи загроз реалізація». Критерії захисту інформації в CPS: архітектура конфіденційності, цілісності, доступності; спостережливість; гарантії. Формулювання завдань безпеки спрямовані на протидію загрозам безпеці та дотриманню політики безпеки в галузі інформації та комунікаційних систем через розробку складної системи інформаційної безпеки, яка працює на виявлення, блокування та нейтралізацію інформаційних загроз [13]. Опис CPS за методом STRIDE подано в таблиці 3.1.

Таблиця 3.1.

Комплексна система безпеки CPS: технологія захисту

Структура CPS	Загрози: метод STRIDE		Захисні технології	Захисні профілі	Нормативно-правове забезпечення
CS: iPhone	S	• соціальна інженерія; • заміна підписаного програмного забезпечення; • заміна об'єктів	• сертифікація програми; • спосіб завантаження надійних пристроїв; • сертифікація прошивки SHSH	• Біометричні механізми для перевірки Профіль захистуV1.3 (2008.11.07); • профіль захисту для мобільних пристроїв: Основи V 2.0 (2014.09.17); • Програмне забезпечення Soft-Захист Профайл (ASPP) Розширений пакет: Файл	• NIST Special Публікація 800-164.2012. Вказівки щодо апаратної безпеки в мобільному пристрої (тяга); • NIST Special Публікація 800-124. 2013. Керівні принципи для Управління безпекою мобільних пристроїв, Пристрої в підприємстві; • Урядова мобільна та бездротова база безпеки 2013 рік
	T	• модифікація кодів доступу; • отримання повного доступу до файлової системи (Jailbreak); • несанкціонований запуск, плата за знищення даних	• кодування захисту; • сертифікати системи експлуатації; • низькорівневе шифрування AES-256;		
	R	• заміна цифрової довідки / підпису; • маскування шкідливого програмного забезпечення; • несанкціоновані покупки через програми;	• технологія фіксації дій користувачів • батьківський контроль; • дактилоскопічний датчик		

CS: iPhone	I	• несанкціонований віддалений доступ; • соціальна інженерія; • самовільне виконання програмне забезпечення	• SSL / VPN; • дистанційне блокування пристрою • APM ніколи не виконується	Шифрування: Пом'якшення ризику розкриття інформації про конфіденційні дані Система V1.0(2014.11.10); • профіль захисту для програми, Повнодискове шифрування V1.1 (2014.03.31)	• Мобільний-Пристрій обчислювальної техніки (MCD) Стандарти та Керівні принципи. Обов'язковова Довідка для ADS Глава 545 2014
	D	• експлоїти системи ядра, в загрузчику (0x24000 Segment Overflow, usb_control_ msg(0xA1, 1) Exploit); • експлуатує на рівні ядра системи (IOSurfaceKernelExploit) • несанкціонований запуск функції блокування на пристрої	• сертифікація AppleRoot; • спосіб завантаження надійних пристроїв • Пісочниця Apple		
	E	• соціальна інженерія; • заміна цифрового сертифікату / підпису; • використання вразливостей операційної системи	• періодичне оновлення операційної системи та програм • шифрування файлів (алгоритм AES); • поетапна аутентифікація		

CS: Wi-Fi	S	• маскування під інший вузол; • заміна пристроїв (атака man-in-the-middle); • атаки на паролі доступу;	• технологія аутентифікації перевірки об'єктів; • приховування внутрішніх адрес (шлюз сеансу) • технологія обмеження доступу	• Захист брандмауера Профіль V3.0(2015.06.12); • Загальні критерії Schutzprofil (Захист профілю). Schutzprofil 1: Anforderun-genan DenNetzkonnektor V3.2.1 (2015.04.28); • профіль захисту для клієнтів IPsec Віртуальна Приватна мережа (VPN) V1.4 (2013.10.21)	• IEEE Std. 802.11; •ДСТУ ISO / IEC7498-3: 2004. Інформаційні технології – Взаємозв'язок відкритих систем – Основна довідка Модель: Назви та адресація; • ISO / IEC 27033-3: 2010. Інформаційні технології. Прийоми безпеки. Мережа безпеки. Довідкова мережа сценаріїв. Загрози, методики дизайну і контролю питання; • ISO / IEC 27033-4: 2014. Інформація технології. Мережева безпека
	T	• несанкціонована конфігурація маскування; • самовільне очищення логів; • несанкціоноване використання ресурсів мережі	• обмеження доступу до журналів; • віддалене зберігання файлів журналів; • ідентифікація користувача та аутентифікація		
	R	• перехват пакетів; • соціальна інженерія; • несанкціонований збір інформації про мережу	• шифрування даних; • IPSEC; • VPN		
	I	• DoS\ DDoS атаки; • відключення елементів мережі; • обструктивність	• фільтр пакетів; • брандмауер; • обмеження доступу до мережевих елементів		
	D	• несанкціонований доступ до налаштування обладнання; • аналіз посадової особи адміністративні дані; • несанкціоновані зміни /підміна доступу дозволи	• ідентифікація сеансів учасників; • обмеження доступу до обладнання налаштування; • фіксація зміни налаштувань		

	E	• несанкціонована конфігурація маскування; • самовільне очищення колод; • несанкціоноване використання мережевих ресурсів	• обмеження доступу до журналів; • віддалене зберігання файлів журналів; • ідентифікація користувача та аутентифікація		
CS: Bluetooth	S	• підміна пристроїв (атака man-in-the-middle); • підміна користувача; • перехват кодів доступу	• ідентифікація обладнання; • аутентифікація прав користувача • шифрування кодів доступу	• видача сертифікатів та управління Компонентами Профіль захистуV1.5 (2011.09.09); • профіль захисту для мережевих пристроїв V1.1 (2012.06.08); • Мережевий пристрій Профіль захисту (NDPP) Розширений пакет: SIP-сервер V1.1 (2014.11.05); • Загальні критерії Профіль захисту. Криптографічний модуль, Рівень безпеки «низький» V1.01b(2009.02.27)	• IEEE 802.15.1; •НДТЗІ2,5-004-99. Критерії для оцінювання інформаційної безпеки в комп'ютерних системах від несанкціонованого доступу; •ДСТУ3043-95 Інформація технології. Телеобробка даних та комп'ютерних мереж. Умови та Визначення; • ISO / IEC 27033-5: 2013. Інформаційні технології. Прийоми безпеки. Мережева безпека
	T	• самовільна зміна командування; • неправильне представлення; • помилки в потоці даних;	• хешування; • шумоізоляційне кодування; • преемуляція		
	R	• маскування несанкціонованих дій як помилки; • самовільне використання облікових даних • самовільне використання / зміна послуги	• обмеження доступу до облікових даних та послуги; • реєстрація подій; • автентифікація користувача		
	I	• перехоплення потоку даних; • перехоплення кодів доступу; • несанкціонований доступ до облікового запису інформації	• шифрування даних; • Одноразовий пароль аутентифікації; • ідентифікація пристроїв		
	D	• обструктивність; • відключення обладнання;	• динамічна зміна частоти; • обмеження доступу до обладнання		

Продовження таблиці 3.1.

	E	• заміна пристроїв (атака man-in-the-middle); • заміна користувача • перехоплення кодів доступу	• ідентифікація обладнання; • аутентифікація, авторизація користувача • шифрування кодів доступу		
PS: Sensors	T	• модифікація дисплея	• механізм контролю вимірювання	• Виявлення вторгнень Системний датчик Профіль захисту V1.3 (2007.07.25)	• IEEE 2700-2014 Стандартні для датчика параметри продуктивності та їх визначення; • IEC 62047-Серія. Частина 1-22. Мікро-електромеханічний пристрій – MEMS
	D	• відключення електроенергії; • перевищення порогу; • відмова обладнання	• дублювання датчика; • аварійне відключення датчика; • самодіагностика		

Як бачимо з таблиці 3.1, існує велика кількість різноманітних загроз кіберфізичним системам як на апаратному так і на системному рівнях. Для повного адекватного захисту інформаційного забезпечення потрібно мати значні матеріальні та людські ресурси, які будуть задіяні у виконанні вищевказаних задач. Проблема захисту від таргетованих атак залишається відкритою. Оскільки ми в нашому дослідженні орієнтуємось на потреби малого та середнього бізнесу, пропонуємо мінімально затратний варіант, який дозволить відбити частину типових кібератак та захистить файли користувача.

Загальна характеристика інформаційного забезпечення: створена та пропонована для використання програма *VARAN* відноситься до класу утиліт, що виконують захисні рішення. Написана мовою програмування VB6 та cmd, використовує технології.NET, та COM-об'єкти. Вищевказані мови були обрані для забезпечення найбільшої сумісності між версіями Windows без встановлення додаткових пакетів.

А також з метою максимально зменшити розмір основного файлу програми, що виконується. Дана програма повинна знаходитись на жорсткому диску чи твердотільному накопичувачі [10].

Було використано компілятори NanoVB6 з надлаштуванням NativeCode для прямого використання процесорних інструкцій, що в теорії, зменшує розмір файлу і збільшує швидкість його дії.

Утиліта *VARAN* змінює розширення відомих файлів і робить відповідні записи у системному реєстрі, щоб користувач міг відкривати захищені файли як зазвичай, не помічаючи різниці між захищеним та незахищеним файлом. А це, в свою чергу, не буде перешкоджати його звичайній роботі з ПК.

Також він закриває вразливості EternalBlue & DoublePulsar ,що використовують протокол SMB, шляхом внесення відповідних змін до файерволу і системного реестру. Та створює відповідні файли-індикатори для Petya Ransomware, щоб він самоліквідувався на зараженій системі. [11; 14].

Оскільки база даних необхідна лише для вимкнення захисту та налаштувань мови, зважаючи на те, що її копія знаходиться у системному реєстрі, а мову можна вибрати заново, звичайні захисні рішення доступу до баз даних (токени автентифікації), хеш-суми для контроля цілісності інформації та паролі доступу використовувати не доцільно. Для збереження налаштувань програми та зменшення розміру бази, було прийнято рішення зберігати налаштування у текстовому вигляді як структуровану базу даних «змінна – значення», записи і доступ до баз даних проводиться без автентифікації та з режимом читання/ запису напряму.

Запропонована програма *VARAN* не потребує використання автоматизованих систем збору і передачі інформації тому що є недоцільним підключення автоматизованої системи збору і передачі інформації до такої програми, оскільки таку систему необхідно підключити до всього комп'ютера. Натомість, якщо є така можливість із самого початку, то встановлення програми *VARAN* не є необхідним, оскільки підприємство вже забезпечено штатом працівників і необхідними інструментами для протистояння (кіберзахисту) зовнішнім загрозам [12].

3.3. Висновки до розділу 3

Таким чином, можемо зазначити, що нам вдалося розробити програму під назвою *VARAN*, яка дає більш ефективний захиств порівнянні з існуючими антивірусами для роботи в ОС Windowsta є зручною у використанні, оскільки максимально непомітна для користувача.

ВИСНОВКИ ТА ПРОПОЗИЦІЇ

Розроблена програма *VARAN* для захисту інформації бізнес-процесів на підприємств і дає більш ефективний захист в порівнянні з існуючими антивірусами для роботи в ОС Windows та є зручною у використанні, оскільки максимально непомітна для користувача.

Подальших наукових та практичних розвідок потребує робота над покращенням евристики антивірусу.

На дану тематику були опубліковані **тези** “Innovative Information Technology in Banking System” 16th All-Ukrainian Scientific and Practical Conference for Students and Cadets, 2017; “Information Security as a Component of National Security” Cadet’s VIIInter academic Scientific and Practical Conference in foreign languages “Modern Tools Used for Information Security Fostering (international experience)”, 2018; “Проблеми створення і вдосконалення шифрів від криптоаналітичних атак” у Всеукраїнській науково-практичній конференції “Безпека соціально-економічних процесів в кіберпросторі” 2019; “Data protection ensuring by cryptographic attack ciphers’ improving” Cadet’s VIIIInter academic Scientific and Practical Conference in foreign languages “Modern Tools Used for Information Security Fostering (international experience)”, 2019;«Політика конфіденційності сучасних популярних сервісів. Privacy Policy of Popular Modern Services» «Сучасні механізми забезпечення інформаційної безпеки (зарубіжний досвід)» IX Міжвузівської курсантської науково-практичної конференції іноземними мовами, 2020; та наукова **стаття** «Теоретичні аспекти створення комплексних систем захисту інформації», 2020.

					КНТЕУ 121 06з-18.МР		
Зм.	*Аркуш*	*№ докум.*	*Підпис*	*Дата*			
Зав. каф.		Криворучко О.В.		30.10.20	Розробка системи захисту інформації бізнес-процесів	*Стадія*	*Аркуш*	*Аркушів*
Керівник		Сашньова М.В.		30.10.20		*ВП*	*39*	*43*
Гарант		Криворучко О.В.		30.10.20		*Факультет інформаційних технологій 2м курс, 6з група*		
Розробив		Чернігівський І.А.		30.10.20	*Висновки та пропозиції*			

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Алексеєва А. В. Звітність підприємства: навч. посіб. для студ. вищ. навч. закл. / А. В. Алексеєва, А. П. Шаповалова, Г. В. Уманців; [Міністерство освіти і науки України; Київський національний торговельно-економічний університет]. – К. :Центр учбової літератури,2013. – 367 с.

2. Безверхий К. В. Інформаційний комплекс облікової системи та звітність в Україні: моногр. / К. В. Безверхий, Т. В. Бочуля. – К.: Центр учбової літератури, 2014. – 184 с.

3. Бутинець Ф. Ф. Бухгалтерський фінансовий облік: підруч. для студ. спец «Облік і аудит» вищ. навч. закл. / Ф. Ф. Бутинець. – Житомир: ПП «Рута», 2009. – 912с.

4. Голов С. Ф. Бухгалтерський облік в Україні: аналіз стану та перспективи розвитку: моногр. / С. Ф. Голов. – К.: Центр учбової літ., 2007. – 522 с.

5. Голов С. Ф. Бухгалтерський облік та фінансова звітність за міжнародними стандартами / С. Ф. Голов, В. М. Костюченко. – Х.: Фактор, 2013. – 1072 с.

6. Голов С. Ф. Трансформація фінансової звітності українських підприємств у фінансову звітність за міжнародними стандартами / С.Ф. Голов, В.М. Костюченко, О.М. Кулага. – К.: ФПБАУ, 2013. – 268 с.

7. Голубнича Г. П. Звітність підприємства: навч. посіб. для студ. вищ. навч. закл. / Г. П. Голубнича, Т. Г. Мельник. – К.: Київський університет, 2012. – 575с.

					КНТЕУ 121 06з-18.МР		
Зм.	*Аркуш*	*№ докум.*	*Підпис*	*Дата*			
Зав. каф.		Криворучко О.В.		24.01.20	Розробка системи захисту інформації бізнес-процесів	*Стадія*	*Аркуш*	*Аркушів*
Керівник		Сашньова М.В.		24.01.20		*СВД*	*40*	*43*
Гарант		Криворучко О.В.		24.01.20				
Розробив		Чернігівський І.А.		24.01.20	*Список використаних джерел*	*Факультет інформаційних технологій 2м курс, 6з група*		

8. Кучер Е.М.Information technology in the fight against cybercrime: журнал Безпека соціально-економічних процесів в кіберпросторі / Е.М. Кучер, С.Л.Рзаєва. – К.: Київ. нац. торг.-екон. ун-т, 2019. – С. 140 – 141.

9. Гольцова С. М. Звітність підприємств (фінансова, статистична, консолі дована та до фондів соціального та пенсійного страхування): навч. посіб. / С.М. Гольцова. К. : Центр учбової літ., 2008. – 155 с.

10. Чернігівський І.А. Проблеми створення і вдосконалення шифрів від криптоаналітичних атак / І.А. Чернігівський // Безпека соціально-економічних процесів в кіберпросторі : матеріали Всеукр. наук.-практ. конф. – К. : Київ. нац. торг.-екон. ун-т, 2019. – С. 234 – 235.

11. Чернігівський І.Інформаційна безпека як складова національної безпеки Information Security as a Component of National Security / Іван Чернігівський // Сучасні механізми забезпечення інформаційної безпеки (зарубіжний досвід) : матеріали VII Міжвузівської курсантської науково-практичної конференції іноземними мовами (англійська, німецька, французька, східно-європейські мови): реферативний збірник. – Київ : Нац. акад. СБУ, 2019. – С. 273–275.

12. Чернігівський І. Забезпечення захисту даних шляхом удосконалення шифрів від криптоаналітичних атак. Data protection ensuring by cryptographic attack ciphers' improving / Іван Чернігівський // Сучасні механізми забезпечення інформаційної безпеки (зарубіжний досвід) : матеріали VIII Міжвузівської курсантської науково-практичної конференції іноземними мовами (англійська, німецька, французька, польська, словацька, чеська, румунська, російська, арабська та перська) : збірник. – Київ : Нац. акад. СБУ, 2020. – С. 416 – 419.

13. Чернігівський І.А. Теоретичні аспекти створення комплексних систем захисту інформації / І.А. Чернігівський // Вісник КНТЕУ, 2020. – С.

14. Chernigivskiy Ivan Innovative Information Technology in Banking System" /Ivan Chernigivskiy // Economic and Legal Development of Ukraine under Conditions of Post-Industrial Society: 16th All-Ukrainian Scientific and Practical Conference for Students and Cadets. – Irpin : University of State Fiscal Service of Ukrane, 2017. – P. 98 – 99.

Інтернет-ресурси

15. Управління звітністю, різноманітні види звітів[Електронний ресурс].– Режим доступу: https://businessviews.com.ua/ru/strategies/id/zvit-pro-upravlinnja-1860/

16. Системи управління підприємствами[Електронний ресурс].– Режим доступу: https://pidruchniki.com/1055070253526/menedzhment/sistemi_upravlinnya_pidpruemstvamu.

17. Закон України «Про Інформацію» [Електронний ресурс].– Режим доступу: https://zakon.rada.gov.ua/laws/show/2657-12#Text

18. Захист інформації [Електронний ресурс].– Режим доступу: https://uk.wikipedia.org/wiki/%D0%97%D0%B0%D1%85%D0%B8%D1%81%D1%82_%D1%96%D0%BD%D1%84%D0%BE%D1%80%D0%BC%D0%B0%D1%86%D1%96%D1%97

19. Об'єкти_критичної_інфраструктури [Електронний ресурс].– Режим доступу: https://uk.wikipedia.org/wiki/%D0%9E%D0%B1%27%D1%94%D0%BA%D1%82%D0%B8_%D0%BA%D1%80%D0%B8%D1%82%D0%B8%D1%87%D0%BD%D0%BE%D1%97_%D1%96%D0%BD%D1%84%D1%80%D0%B0%D1%81%D1%82%D1%80%D1%83%D0%BA%D1%82%D1%83%D1%80%D0%B8

20. Деякі питання об'єктів критичної інформаційної інфраструктури[Електронний ресурс].– Режим доступу: https://zakon.rada.gov.ua/laws/show/943-2020-%D0%BF#Text

21. Закон України «Про критичну інфраструктуру та її захист» [Електронний ресурс].– Режим доступу: http://search.ligazakon.ua/l_doc2.nsf/link1/JH7YW00A.html

22. Закон України «Про основні засади забезпечення кібербезпеки України» [Електронний ресурс].– Режим доступу: https://zakon.rada.gov.ua/laws/show/2163-19#Text

23. Как работают вирусы шифровальщики и как от них защититься [Електронний ресурс].– Режим доступу: https://tech-geek.ru/how-ransomware-works/

24. Анализ одной из модификаций шифровальщика VaultCrypt [Електронний ресурс].– Режим доступу: https://habr.com/ru/post/266077/

25. Вирусы-вымогатели_(шифровальщики)_Ransomware [Електронний ресурс].– Режим доступу: https://www.tadviser.ru/index.php/%D0%A1%D1%82%D0%B0%D1%82%D1%8C%D1%8F:%D0%92%D0%B8%D1%80%D1%83%D1%81%D1%8B-%D0%B2%D1%8B%D0%BC%D0%BE%D0%B3%D0%B0%D1%82%D0%B5%D0%BB%D0%B8_(%D1%88%D0%B8%D1%84%D1%80%D0%BE%D0%B2%D0%B0%D0%BB%D1%8C%D1%89%D0%B8%D0%BA%D0%B8)_Ransomware#CovidLock_.28.D0.B2.D0.B8.D1.80.D1.83.D1.81-.D0.B2.D1.8B.D0.BC.D0.BE.D0.B3.D0.B0.D1.82.D0.B5.D0.BB.D1.8C.29

26. Противодействие вирусам-шифровальщикам часть 1 [Електронний ресурс].– Режим доступу: https://www.osp.ru/winitpro/2016/12/13051097

27. Как мы защищались от шифровальщика, и сколько это нам стоило [Електронний ресурс].– Режим доступу: https://www.olly.ru/blog/kak-my-zashchishchalis-ot-shifrovalshchika-i-skolko-eto-nam-stoilo/

ДОДАТКИ

Додаток А

Лістинг програмного коду

GUI Form1.frm

```
VERSION 5.00
Begin VB.Form Form1
   Caption         =   "Varan. Version: 1.0"
   ClientHeight    =   4065
   ClientLeft      =   7245
   ClientTop       =   4245
   ClientWidth     =   4635
   LinkTopic       =   "Form1"
   ScaleHeight     =   4065
   ScaleWidth      =   4635
   Begin VB.ComboBox Combo1
      Height          =   315
      Left            =   1440
      TabIndex        =   2
      Text            =   "Русский"
      Top             =   840
      Width           =   1695
   End
   Begin VB.CommandButton Command1
      Caption         =   "Выключить\Включить защиту"
      Height          =   735
      Left            =   720
      Style           =   1  'Graphical
      TabIndex        =   1
      Top             =   2880
      Width           =   3255
   End
   Begin VB.Label Label2
      Caption         =   "Язык"
      Height          =   255
      Left            =   1440
      TabIndex        =   3
      Top             =   480
      Width           =   1695
   End
   Begin VB.Label Label1
      Caption         =   "Защита отключена!"
      Height          =   615
      Left            =   720
      TabIndex        =   0
      Top             =   2040
      Width           =   3255
   End
End
Attribute VB_Name = "Form1"
Attribute VB_GlobalNameSpace = False
Attribute VB_Creatable = False
Attribute VB_PredeclaredId = True
```

```
Attribute VB_Exposed = False
Private Sub Combo1_Click()
Select Case Combo1.ListIndex
            Case 0
                Command1.Caption = "Выключить\Включить защиту"
                Label2.Caption = "Язык"
                If (Label1.Caption = "Security off") Or (Label1.Caption =
"Защита отключена!") Or (Label1.Caption = "Захист вимкнено") Then
                Label1.Caption = "Защита отключена!"
                Else
                Label1.Caption = "Защита включена"
                End If
            Case 1
                Command1.Caption = "Ввімкнути\Вимкнути захист"
                Label2.Caption = "Мова"
                If (Label1.Caption = "Security off") Or (Label1.Caption =
"Защита отключена!") Or (Label1.Caption = "Захист вимкнено") Then
                Label1.Caption = "Захист вимкнено"
                Else
                Label1.Caption = "Захист ввімкнено"
                End If
            Case 2
                Command1.Caption = "Enable\Disable Security"
                Label2.Caption = "Language"
                If (Label1.Caption = "Security off") Or (Label1.Caption =
"Защита отключена!") Or (Label1.Caption = "Захист вимкнено") Then
                Label1.Caption = "Security off"
                Else
                Label1.Caption = "Security on"
                End If
        End Select
End Sub

Private Sub Command1_Click()
Select Case Label1.Caption
            Case "Защита включена"
                Label1.Caption = "Защита отключена!"
                Label1.BackColor = vbRed
                GoTo Security_OFF
            Case "Защита отключена!"
                Label1.Caption = "Защита включена"
                Label1.BackColor = vbGreen
                GoTo Security_ON
        End Select

        Select Case Label1.Caption
            Case "Security on"
                Label1.Caption = "Security off"
                Label1.BackColor = vbRed
                GoTo Security_OFF
            Case "Security off"
                Label1.Caption = "Security on"
                Label1.BackColor = vbGreen
                GoTo Security_ON
        End Select
```

```
        Select Case Label1.Caption
            Case "Захист ввімкнено"
                Label1.Caption = "Захист вимкнено"
                Label1.BackColor = vbRed
                GoTo Security_OFF
            Case "Захист вимкнено"
                Label1.Caption = "Захист ввімкнено"
                Label1.BackColor = vbGreen
                GoTo Security_ON
        End Select
Security_ON:
Shell "cmd.exe /c console.bat", vbHide
MsgBox "Security is turning on and adjust, please wait some minutes",
vbInformation, "Turning on..."
Exit Sub
Security_OFF:
Shell "cmd.exe /c console.bat secure_off", vbHide
MsgBox "Security is off! Your system is vulnerable now!", vbCritical,
"Turning off..."
Exit Sub
End Sub


Private Sub Form_Load()
Select Case Label1.Caption
            Case "Защита отключена!"
                Label1.Caption = "Защита отключена!"
                Label1.BackColor = vbRed
            Case "Защита включена"
                Label1.Caption = "Защита включена"
                Label1.BackColor = vbGreen
        End Select
Combo1.AddItem ("Русский")
Combo1.AddItem ("Українська")
Combo1.AddItem ("English")
End Sub
```

GUI Project1.vbp

```
Type=Exe
Reference=*\G{00020430-0000-0000-C000-
000000000046}#2.0#0#..\..\..\..\Windows\system32\stdole2.tlb#OLE Automation
Reference=*\G{420B2830-E718-11CF-893D-
00A0C9054228}#1.0#0#..\..\..\..\Windows\system32\scrrun.dll#Microsoft
Scripting Runtime
Reference=*\G{565783C6-CB41-11D1-8B02-
00600806D9B6}#1.2#0#..\..\..\..\Windows\system32\wbem\wbemdisp.TLB#Microsof
t WMI Scripting V1.2 Library
Form=Form1.frm
Startup="Form1"
Command32=""
Name="Project1"
HelpContextID="0"
CompatibleMode="0"
MajorVer=1
MinorVer=0
RevisionVer=0
AutoIncrementVer=0
ServerSupportFiles=0
VersionCompanyName="None"
CompilationType=0
OptimizationType=0
FavorPentiumPro(tm)=0
CodeViewDebugInfo=0
NoAliasing=0
BoundsCheck=0
OverflowCheck=0
FlPointCheck=0
FDIVCheck=0
UnroundedFP=0
StartMode=0
Unattended=0
Retained=0
ThreadPerObject=0
MaxNumberOfThreads=1
```

GUI Project1.vbw

```
Form1 = 116, 76, 897, 534, C, 129, 65, 945, 565, C
```

CLI console.bat

```
@Echo off
set /p lang=<"%~dp0\ActiveFolder\language.txt"
reg add HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced /v HideFileExt /t REG_DWORD /d 1 /f
taskkill /f /im explorer.exe
start explorer.exe
cd "%~dp0\ActiveFolder\"
cls
chcp 1251 >nul
goto greet_%lang%
:greet_en
echo Vano's Anti-Ransomware, for all types of ransomware. Version: 1.0
echo Author: Ivan Chernihovskiy, 2017. All rights are reserved.
echo.
:greet_ua
echo Vano's Anti-Ransomware, для усіх типів шифрувальників. Версія: 1.0
echo Автор: Іван Чернігівський, 2017. Усі права захищені.
echo.
:greet_ru
echoVano'sAnti-Ransomware, для всех типов шифровальщиков. Версия: 1.0
echo Автор: Иван Черниговский, 2017. Все права защищены.
echo.

goto %1
set ext=extentions.txt
set table=table.txt
```

```
goto start
:secure_off
set secure=off
set ext=table.txt
set table=ext.txt
goto replace
:start
set masiv=abcdefghijklmnopqrstuvwxyz-ABCDEFGHIJKLMNOPQRSTUVWXYZ_1234567890@#$+
set count=0

find /i "01001" computer_setings.nfo
if %errorlevel% == 1 set exploit_off=1
if %2 == exploit_off set exploit_off=1
if %exploit_off% == 1 goto Ethernal_Blue
goto set_rnd

:Eternal_Blue
rem For old modification of "Petya ransomware"-type, that use exploit Eternal Blue
echo 01001>>computer_setings.nfo
echo.>C:\Windows\perfc
echo.>C:\Windows\perfc.dll
attrib +r C:\Windows\perfc
attrib +r C:\Windows\perfc.dll
sc.exe config lanmanworkstation depend=bowser/mrxsmb20/nsi
sc.exe config mrxsmb10 start=disabled
```

reg add HKLM\SYSTEM\CurrentControlSet\Services\LanmanServer\Parameters /v SMB1 /t REG_DWORD /d 0 /f

reg add HKLM\SYSTEM\CurrentControlSet\services\mrxsmb10 /v Start /t REG_DWORD /d 4 /f

reg add HKLM\SYSTEM\CurrentControlSet\Services\LanmanWorkstation /v DependOnService /t REG_MULTI_SZ /d Bowser\0 MRxSmb20\0 NSI\0 /f

netsh advfirewall firewall add rule name="Block_TCP-135" dir=in action=block protocol=tcp localport=135

netsh advfirewall firewall add rule name="Block_TCP-137" dir=in action=block protocol=tcp localport=137

netsh advfirewall firewall add rule name="Block_TCP-138" dir=in action=block protocol=tcp localport=138

netsh advfirewall firewall add rule name="Block_TCP-139" dir=in action=block protocol=tcp localport=139

netsh advfirewall firewall add rule name="Block_TCP-445" dir=in action= blockprotocol=tcp localport=445

netsh advfirewall firewall add rule name="Block_TCP-1024" dir=in action=block protocol=tcp localport=1024

netsh advfirewall firewall add rule name="Block_TCP-1025" dir=in action=block protocol=tcp localport=1025

netsh advfirewall firewall add rule name="Block_TCP-1026" dir=in action=block protocol=tcp localport=1026

netsh advfirewall firewall add rule name="Block_TCP-1027" dir=in action=block protocol=tcp localport=1027

netsh advfirewall firewall add rule name="Block_TCP-1028" dir=in action=block protocol=tcp localport=1028

netsh advfirewall firewall add rule name="Block_TCP-1029" dir=in action=block protocol=tcp localport=1029

```
netsh advfirewall firewall add rule name="Block_TCP-1030" dir=in action=block protocol=tcp localport=1030
netsh advfirewall firewall add rule name="Block_TCP-1031" dir=in action=block protocol=tcp localport=1031
netsh advfirewall firewall add rule name="Block_TCP-1032" dir=in action=block protocol=tcp localport=1032
netsh advfirewall firewall add rule name="Block_TCP-1033" dir=in action=block protocol=tcp localport=1033
netsh advfirewall firewall add rule name="Block_TCP-1034" dir=in action=block protocol=tcp localport=1034
netsh advfirewall firewall add rule name="Block_TCP-1035" dir=in action=block protocol=tcp localport=1035
netsh advfirewall firewall add rule name="Block_TCP-5000" dir=in action=block protocol=tcp localport=5000

:set_rnd
set /a rnd1=1+(68-2)*%random%/32768
ping -n 2 127.0.0.1
set /a rnd2=1+(68-2)*%random%/32768
ping -n 2 127.0.0.1
set /a rnd3=1+(68-2)*%random%/32768
ping -n 2 127.0.0.1
set /a rnd4=1+(68-2)*%random%/32768
ping -n 2 127.0.0.1
set /a rnd5=1+(68-2)*%random%/32768
ping -n 2 127.0.0.1
set /a rnd6=1+(68-2)*%random%/32768
```

```
Call set
symbols=.%masiv:~0,%rnd1%%%masiv:~0,%rnd2%%%masiv:~0,%rnd3%%%masiv:
~0,%rnd4%%%masiv:~0,%rnd5%%%masiv:~0,%rnd6%%
find /i %symbols% table.txt
if %errorlevel% == 1 echo %symbols%>>table.txt&goto count
goto set_rnd
:count
set /a count+=1
if %count% == 405 goto replace
goto set_rnd
:replace
for /f %%a "delims=;" in (%ext%) do (
for /f %%b "delims=;" in (%table%) do (
for %%c in (A B C D E F G H I J K L M N O P Q R S T U V W X Y Z) do call
:protect %%c
:protect
dir /B "%1:\"&& for /r "%1:\" %%d in (%%a) do (RENAME "%%d"
"%%~nxd.%%b")
echo assoc %%b=%%a>>replacement_table.bat")
)
if "%secure%" == "off" goto final
replacement_table.bat
ping -n 2 127.0.0.1
:final
del replacement_table.bat /q
chcp 1251 >nul
goto result_%lang%
:result_ru
```

```
if "%secure%" == "off" msg * Защита отключена&del computer_setings.nfo /q&exit
msg * Защита включена
echo 1010011 1001111 1010011>>computer_setings.nfo
exit
:result_ua
if "%secure%" == "off" msg * Захист вимкнено&del computer_setings.nfo /q&exit
msg * Захист ввімкнено
echo 1010011 1001111 1010011>>computer_setings.nfo
exit
:result_en
if "%secure%" == "off" msg * Security is off&del computer_setings.nfo /q&exit
msg * Security is on
echo 1010011 1001111 1010011>>computer_setings.nfo
exit

:help_en
echo en>language.txt
cls
echo Vano's Anti-Ransomware, for all types of ransomware. Version: 1.0
echo Author: Ivan Chernihivskiy, 2017. All rights are reserved.
echo.
echo This programm protect your files from encryption of all existing viruses type-ransomware that was made before 15.11.2017, if ransomware not-typical it will stopped by closing exploit-kit and special zero-files. I have simple recomendation for you: do not test fate! Because I don't have any responsable of your activity. Usage programm:
```

```
echo     Open varan.bat without options to have maximum security
echo     varan.bat secure_off - turn off the security of your PC(delete programm only after this! to avoid problems)
echo     varan.bat set exploit_off - disable exploit EternalBlue manualy(exist as default start)
echo     varan.bat help_^[en, ua, ru^] - display this help and set defolt language(English, Ukrainian, Russian)
pause
exit
:help_ua
echo ua>language.txt
cls
chcp 1251>nul
echo Vano's Anti-Ransomware, для усіх типів шифрувальників. Версія: 1.0
echo Автор: Іван Чернігівський, 2017. Усі права захищені.
echo.
echo Ця программа захищає ваші файли від шифрування усіма існуючими типовими вірусами шифрувальниками які були створені до 15.11.2017, якщо шифрувальник не є типовим то він буде зупинений через закриття експлоіту та створенням спеціальних файлів. Хочу дати вам невелику пораду: не випробовуйте долю! Тому, що я не відповідаю за ваші дії. Використання программи:
echo     Відкриття файлу varan.bat без додаткових опцій, дає максимальну захищеність
echovaran.batsecure_off - вимкнути захист ПК(видаляйте программу тільки після цього! щоб уникнути проблем)
echovaran.batsetexploit_off - закрити експлоїт EternalBlueвручну(автоматично закривається при звичайному старті)
```

echovaran.bathelp_^[en, ua, ru^] - відобразити цю підказку і встановити мову за замовчуванням(Англійська, Українська, Россійська)

pause

exit

:help_ru

echoru>language.txt

cls

chcp 1251>nul

echoVano'sAnti-Ransomware, для всех типов шифровальщиков. Версия: 1.0

echo Автор: Иван Черниговский, 2017. Все права защищены.

echo.

echo Эта программа защищает ваши файлы от шифрования всеми существующими вирусами шифровальщиками которые были созданы до 15.11.2017, если шифрователь не типичный то он будет остановлен закрытием эксплоита и специальными файлами-пустышками. У меня есть для вас простая рекомендация: не испытывайте судьбу! Потому что я не несу ответственности за ваши действия. Использование программы:

echo Открытие varan.bat без единой опции даёт вам максимальную защищённость

echovaran.batsecure_off - выключить защиту для этого ПК(удаляйте программу только после этого! чтобы избежать проблем)

echovaran.batsetexploit_off - отключить экслоит EternalBluевручную(отключается при обычном старте)

echovaran.bathelp_^[en, ua, ru^] - отображает эту подсказку на определённом языке, и устанавливает его по умолчанию(Английский, Украинский, Русский)

pause

exit

Додаток Е

CLI back.bat

```
@Echo off
reg add
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\Ad
vanced /v HideFileExt  /t REG_DWORD /d 0 /f
taskkill  /f /im explorer.exe
start explorer.exe
```

Додаток З

База даних розширень файлів ext.txt

.doc.docx.xls.xlsx.ppt.pptx.pst.ost.msg.eml.vsd.vsdx.csv.rtf.123.wks.wk1.pdf.dwg.onetoc2.snt.jpeg.jpg.docb.docm.dot.dotm.dotx.xlsm.xlsb.xlw.xlt.xlm.xlc.xltx.xltm.xlsb.xla.xlam.xll.xlw.pptm.pot.pps.ppsm.ppsx.ppam.potx.potm.pub.bdr.ols.pbr.prv.pubhtml.pubmhtml.puz.wiz.ps.wps.caq.mph.wbk.xps.gfx.edb.hwp.602.sxi.sti.sldx.sldm.sldm.vdi.vmdk.vmx.gpg.aes.ARC.PAQ.bz2.tbk.bak.tar.tgz.gz.7z.rar.zip.backup.iso.vcd.bmp.png.gif.raw.cgm.tif.tiff.nef.psd.ai.svg.djvu.m4u.m3u.mid.wma.flv.3g2.mkv.3gp.mp4.mov.avi.asf.mpeg.vob.mpg.wmv.fla.swf.wav.mp3.sh.class.jar.java.r.rb.rbw.asp.jsp.brd.sch.dch.dip

.pl.vb.vbp.vbw.frm.vbs.vbe.vba.ps1.cmd.js.jse.asm.h.reg.pas.cpp.c.cs.htm.html.ico.mid.ttf.esv.plt.prf.exp.tpl.lnx.svg.str.cat.drp.dpr.dpk.dfm.sb.py.pyc.pyd.pyo.pyw.swift.go.pp.inc.pl.pm.t.pod.php.phtml.php3.php4.php5.php7.phps.m.mm.scala.sc.ada.css.hs.lhs.lua.f.for.f90.f95.sb2.sprite.sprite2.cbl.cob.cpy.suo.sln.ldf.mdf.ibd.myi.myd.frm.odb.dbf.db.mdb.accdb.accde.accdt.accdr.sql.sqlitedb.sqlite3.asc.lay6.lay.mml.sxm.otg.odg.uop.std.sxd.otp.odp.wb2.slk.dif.stc.sxc.ots.ods.3dm.max.3ds.uot.stw.sxw.ott.odt.pem.p12.csr.crt.key.pfx.der.cer.eps.lic.one.p7b.p7c.pef.ptx.rdp.srw.uti.x3f.xpx.gfx.mus.WS.rpm.gba.qif.msg.eml.app.apk.pck.sk.zs2.zbk.1c.cf.cfu.dt.epf.erf.1cd.log.lgf.lgp.elf.cdn.mxl.efd.mft.grs.geo.st.pff.vrp.pff